TRANSPAC4 DISTRIBUTED DENIAL OF SERVICE (DDOS) DETECTION AND MITIGATION PROJECT SUMMARY

Lead: Hans Addleman
Additional Staff: AJ Ragusa, Dan Doyle, CJ Kloote, and Doug Southworth
Indiana University
January 19, 2021

SUMMARY

Routine performance analysis of R&E networks is a vital component of maintaining a high-speed, friction-free path for use by researchers and educators. In addition to standard throughput testing and route analysis, there's an increasing need to detect and mitigate malicious network traffic before it becomes a major source of network interference. As part of this effort, the efficacy of various open source tools was evaluated with the hope of finding a budget conscious, easy to implement solution that could be used to mitigate attacks on any R&E network.

INTRODUCTION

Distributed Denial of Service (DDOS) attacks continue to be a major source of disruption for many resource owners. This type of attack generally consists of an attacker compromising a number of hosts that are directed to send large amounts of data to a target system in an effort to overwhelm the target. Many types of DDOS attacks have traffic patterns that are easy to identify through the examination of packet header samples via sflow or netflow.

Our project plan was originally set out to automate the detection and mitigation of DDOS traffic as it entered the TransPAC network. TransPAC consists of multiple, trans-oceanic backbone networks, what is generally referred to as a backbone or pass-through network, and as such has not traditionally been responsible for detecting or mitigating potentially harmful traffic. Part of the potential challenge was the potential 100Gbps of traffic the TransPAC links can support.

This material is based upon work supported by the National Science Foundation (NSF) under Award #1450904

USE OF SCIPASS

The initial approach planned to leverage the SciPass tool (https://docs.globalnoc.iu.edu/sdn/scipass.html). SciPass, developed by the IU Global NOC, was an OpenFlow application designed to help network security by augmenting an OpenFlow switch with a load balancer interface to an intrusion detection system (IDS), such as Bro/Zeke (https://zeek.org/). When operating in Science DMZ mode, SciPass could use Bro to detect "good" data transfers and add bypass rules so that the traffic avoided institutional firewalls, thereby improving transfer performance and reducing load on IT infrastructure. In addition, it could match traffic patterns and block malicious network traffic at the host-level. Most tools that block bad actors work at the subnet scale, which would also block non-infected hosts along with the infected hosts in the same subnet. SciPass could, potentially, block only traffic from infected hosts participating in a DDOS attack.

We carried out some initial experiments in our software defined networking (SDN) lab consisting of a Brocade switch, a SDN controller running SciPass, and a suite of network test equipment. During the course of the experiments, a bug was found in the SciPass code that kept it from executing properly during testing. However, by this point in time, the SciPass tool was no longer supported and the experiments were put on hold.

USE OF NOZZLE

In July 2019, we met with Warrick Mitchel, the Network Architect for AARNet, at APAN. Mitchel described a new project called Nozzle that was being developed in Australia as a plugin to the Faucet SDN controller (https://faucet.nz/). Faucet is an open source SDN controller. Nozzle (https://research.csiro.au/isp/research/past-projects/project-nozzle-software-defined-enterprise-network-security/) was expected to have nearly the same functionality as SciPass in terms of being able to block host level traffic based on patterns detected by an IDS. However, Nozzle was under a highly changeable

This material is based upon work supported by the National Science Foundation (NSF) under Award #1450904

development cycle and was not yet open source, so this tool could not be used for our research.

RESCOPING TO DNS AMPLIFICATION ATTACKS

Having recognized that there were no easily available, open source tools, the team rescoped the project to focus on DNS amplification attacks. This type of attack occurs when a DNS name lookup request is sent with the source IP address falsified, which can result in multiple responses that overwhelm a target's system. The plan was to use some of the framework from the NetSage project (http://netsage.global), and to expand it to work with raw netflow data to detect and analyze potential DDOS attacks. DNS Amplification attacks, with their readily identifiable traffic patterns, were chosen as the first attack type for analysis.

One of the changes to the NetSage system was the need to use raw TransPAC netflow data instead of the standard NetSage de-identified data, where not only are flows smaller than 10 Megabyte discarded but the low-order bits of the IP address are removed before archiving. The team developed a python script to process 6 months of raw TransPAC data, identify probable pattern matches, and upload netflow records to a secure Elasticsearch database.

The team then developed a new, secure Grafana dashboard to aid the analysis process. This dashboard displays the top sources, destinations, and flow pairs by number of flows, specifically the type of small flows that are present in a DDOS attack. It also includes a panel which shows the top single destination of these small flows, along with all of the associated sources, aiding in quick identification of a potential DDOS target.

OUTCOME

We used the NetSage variant Dashboard to analyze data from April 1st, 2020 to September 30th, 2020. The dashboard showed that there were no DNS amplification attacks apparent on theTransPAC network during this period. With the tools, infrastructure, and methodology we now have in place to parse

This material is based upon work supported by the National Science Foundation (NSF) under Award #1450904

TransPAC netflow data, we can continue to look for DNS amplification attacks and possibly expand to different DDOS patterns. We will also work with the OmniSOC (https://omnisoc.iu.edu/) to find netflow data sets with known attacks to test our DDOS algorithm.

This material is based upon work supported by the National Science Foundation (NSF) under Award #1450904