CSCD 434-040 Network Security

Lab 6, Examine logs - Due, February 21, 2024

February 15, 2024

Overview

You'll examine the pcap files the researchers produced when studying the Great Cannon (GC). Use the paper as your guide to find out what you should be looking for.

Find the payload

You must first find the malicious payload that is the injected javascript in `injector_traceroute.tcpdump`. Once you have found it, you'll need to make it human readable by unpacking its contents. Put the unpacked javascript in your write up. Give a brief description of what you think the javascript code is doing.

Identifying the GC

Look at the TTLs of the packets that contain the offending javascript from the task above. Create a program in python identify potential GC packets based on what you find. Use this code to tell me how many flows had their traffic hijacked by the GC and payloads returned with malicious javascript.

Additionally, tell me the correlation of TTLs across GC injected packets. Are they related, why or why not?

Examine logs from `both_sidechannel.tcpdump` and tell me if you think the GFW and GC use the same counter when selecting a TTL. Include your reasoning.

Turn in

Turn in your code as well as a README and PDF write up. Answer all questions in the sections above and include any code requested. Turn in a tarball (`yourname.tar.gz`) of your assignment.