CS5333: Firewall Assignment (Submission / Demo Deadline: May 7th, 2021)

This is a group assignment: up to 4 (four) students can submit a common answer, implement and demonstrate the system. You're expected to pick Task 4-a or 4-b as per your preference.

Task 1 (15 Points) – Creating a simple Firewall using Socket Programming

Implement a simple firewall with two network interface cards connecting to the external network (Internet) and the internal network that you secure. In the socket programing, we used read() for capturing packet. What do you do to let a packet go through the firewall from the outside to inside? In this stage, you may hardcode a simple rule set. The network topology that you use may be 3 VMs that are interconnected like {Host1 – Firewall – Host2}. Also, the mode of firewall operation maybe a router (visible) or a bridge (invisible from hosts).

Task 2 (25 points) – Extending the rule set and its operation on Firewall

Extend the supported rule set at least upto layer 4 including MAC, IPv4 IPv6, ICMP for IPv4/v6, TCP/UDP on top of the firewall developed for Task 1. Instead of hardcoding the rule set, use a better way for updating the rule set without terminating the process of Firewall. You may think of Interactive CLI, REST API or something. As the operation of rule set, "Add", "Delete", "Update" and "Show Statistics" for a rule must be implemented. Your firewall must support the aggregation of a rule set, such as prefix or the range of port numbers.

Task 3 (25 Points) – Performance examination and improvement

Assuming that you have done up to Task 2, then how do you tell the performance of your implementation? How much packet per second can your implementation handle (PPS)? Do you see any change of performance if drop or pass the packet? What happens if you have 10, 50 or 100 rules and the packets are equally matching

the filtering rules? What happens if you increase the number of matching fields in a filtering rule, say MAC address only or Prefix/Port/Proto combination? Generate the controlled or random traffic, and benchmark the system. Show the benchmarking result as the proper graph with legend, description of each axis and unit. You must clarify which traffic generator you use under what kind of configuration for collecting data.

Task 4-a (25 Points): Improving the firewall performance

Given the benchmarking result, how do you improve the firewall performance? Explain how, implement it, and benchmark it again so that you can show the evidence of betterment. Under what kind of condition does your solution work nice? Is it an almighty solution or specific to some particular situations?

Task 4-b (25 Points): Detecting attacks in the network using Firewall

Extend your firewall to detect attacks, such as DoS/DDoS, Port Scan, Cache Poisoning of unsecure protocol like ARP. Pickup at least one attack and explain what the attack is and how your firewall detects it. Then, implement the detection mechanism on your firewall. The detection mechanism must be demonstrated based on the emulated attacks in your testbed. You must clarify which traffic generator or attacking tool you use under what kind of configuration for creating the emulated attacks.

Report (10 Points): The report should be a detailed project report and self sufficient to understand what you have done. You can add screenshots to show the working of the system. All the tools, API and software used should be mentioned with reference.

Deliverables: You need to submit all your source codes and a detailed report in a single .zip file with filename as <your_roll_number>.zip.

Evaluation: All the code submitted will be checked for plagiarism. Any plagiarism issue will be dealt with as per the department plagiarism policy. The assignment will be evaluated by the TAs on a scheduled date and time. If anyone from a team does not appear for evaluation, the assignment will be treated as not submitted.

Late Submission Policy: 20 % penalty for each late day submission.

Q&A

Q1. Why should you use VMs?
A1. Because your development and demonstration should not be affected by the unavailability of LAN by any chance.

Q2. Can you use a ready-made library for GUI?
A2. Basically yes. But the function as a firewall is much more important. Reasonably working CLI will be equally appreciated.

Q3. My Firewall works only for UDP traffic. Is it acceptable?
A3. No.

Q4. Can you use any third-party API to craft a packet?
A4. No. Please stick to the real traffic using traffic generator or network benchmarking tools.

Q5. Can you use any third-party API or iptables to avoid Raw Socket programming?
A5. No. Please stick to your own code.