Reviewer 1

1. What motivated you to conduct an experiment specifically on Denial of Service (DDoS) attacks based on the CDX platform? Were there any specific goals or objectives you aimed to achieve through this research?
   Response 1: Revised as per reviewer's suggestion. Refer to p.3, lines 102-114, " The Cyber Defense eXercise (CDX)... information security".

2. Can you provide more details about the configuration and setup of the virtual machines on the CDX platform? How did you ensure that the simulation accurately represented real-world DDoS attack scenarios?
   Response 2: Revised as per reviewer's suggestion. Refer to p.5-6, lines 216-228, " Figure 2 illustrates... within the platform ". and p.6-7, Figure 2-3, Table 1.

3. What criteria or indicators did you use to determine the effectiveness of the defense end (Intrusion Detection System) based on SNORT in detecting and mitigating DDoS attacks? Did you evaluate its performance in terms of accuracy, false positives, false negatives, or any other metrics?
   Response 3: Revised as per reviewer's suggestion. Refer to p.19, lines 523-528, " We evaluate …during preprocessing" and p.20, Table 6.

4. How did you analyze the traffic flow and packet patterns once the attack was detected? What methods or techniques were employed to distinguish normal network traffic from malicious DDoS attack traffic?
   Response 4: As suggested by the reviewer, please refer to p.4, lines 159-175, " In a DDoS attack ... suspicious IP address".

5. Author can read the following papers to increase the technical strength of the paper: Optimal Load Distribution for the Detection of VM-Based DDoS Attacks in the Cloud, Attack-Specific Feature Selection for Anomaly Detection in Software-Defined Networks, Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions.

   Response 5: In line with the reviewer's recommendation, we have cited the suggested papers in our study.

   1) See p.2, lines 69-73, where we mention "A dual-pronged ... distribution among VMs."
   2) Refer to p.2-3, lines 90-101, for our discussion on "Software Defined Network ... and open challenges."
   3) Refer to p.21, References [11], [16-17].

6. Can you elaborate on the role of Wireshark and PRTG at the analyzing end and monitoring end, respectively? How did these tools contribute to the identification and monitoring of DDoS attacks during the experiment?

   Response 6: As suggested by the reviewer, please refer to p.6, lines 228-238, "The ... prompt reaction ".

7. Minor editing of English language required.

   Response 7: The paper has been proofread by a native English speaker. Please review the revised document.