

Distributed Denial of Service (DDoS) Attacks Technique to Interruption the System's Service and Identification

Roheen Qamar¹, Zahid Hussain¹, Aijaz Ahmed Arain², Baqar Ali Zardari¹

¹Saima Siraj¹, Fawad Khan¹

¹Department of Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan

²Department of Computer Science, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan

*Correspondence: Roheen Qamar roheen.qamar04@yahoo.com

Citation | Qamar. R, Hussain. Z, Arain. A. A, Zardari. B. A, "Distributed Denial of Service (DDoS) Attacks Technique to Interruption the System's Service and Identification", IJIST, Vol. 07 Special Issue. pp 64-76, May 2025

DOI: <https://doi.org/10.33411/IJIST/1345>

Received April 10, 2025 **Revised** | May 08, 2025 **Accepted** | May 10, 2025 **Published** | May 12, 2025.

Distributed Denial of Service (DDoS) attacks remain to present significant threats to network stability and security by flooding systems with malicious traffic intended to interrupt legitimate services. This dissertation looks at numerous DDoS assault tactics and assesses their detection and mitigation using Snort and an open-source network intrusion detection system (NIDS). To adequately investigate these assaults a thorough network architecture was created and simulated with GNS3 which included many VMware virtual machines to imitate a realistic network environment. This research investigates a variety of DDoS attack tactics such as volumetric assaults that flood the network with excessive data, protocol attacks that exploit vulnerabilities in network protocols, and software layer attacks that specifically target certain apps or services. The network architecture generated by GNS3 enabled the controlled deployment of different attack vectors and offered insights on their influence on network performance and security. Snort was used to detect and analyze these assaults and taking use of its rule based detection capabilities to discover patterns and abnormalities associated with DDoS activity. This study assesses Snort's efficacy in detecting and reacting to various DDoS attack signatures with a focus on its real time analysis of alerting systems. The findings show Snort's strengths and limits in controlling various forms of DDoS assaults and offering useful insights into its role in improving network security. Furthermore, this study emphasizes the need of a strong network architecture and ongoing monitoring in protecting against merging threats. The research presented here contributes to our understanding of DDoS attack detection and the actual implementation of Snort in simulated network settings and including techniques for strengthening community resilience against attacks.

Keywords: Denial of Service (DOS), Distributed Denial of Service (DDoS), Snort Detection, Snort Detection DDoS Attack



Introduction:

Distributed denial of service and or ddos and is a type of cyber attack that aims to disrupt a server or network by overwhelming it with fake internet traffic and prevention user access and interfering with normal business operations. An assault utilizing distributed denial varies from a DoS attack in that it originates from a separate source. Distributed denial-of-service attacks are initiated from several systems, as opposed to single systems. DDoS assaults are faster and harder to mitigate than DOS attacks. Because there is just one attacker machine to detect, DoS attacks are easier to avoid. Botnets are an important issue to consider while talking about DDoS attacks. AA botnet is a collection of compromised computers that allows malevolent actors to take remote control of the machines. The reason these botnets are "distributed" is that they may be discovered anywhere and owned by anyone. It is conceivable that innocent computer owners are unaware that their devices are part of a botnet. A DDoS attacker orders every compromised device in their massive botnet to send inquiries to the desired IP address. The purpose is to overwhelm the victim's internet resources by sending an excessive amount of requests for connection or data. Exceeding their capacity limits and finally causing their service to halt [1]. The major objective of this research

1. The technical goal of the research (e.g., detection and mitigation of DDoS using Snort).
2. The broader impact (e.g., improving network security awareness).
3. A concise research aim statement is suitable for a dissertation section.

Denial of Service (DOS):

A denial of service (DoS) attack prevents a computer or network user from accessing resources such as email and the Internet. An assault might be launched either by an operating system or the network.

Reasons for this attack:

1. Inefficient programs/applications that operate on the machine/system.
2. Software program setup without security issues.
3. No checks or data analysis were undertaken [2], as seen in Figure 1.

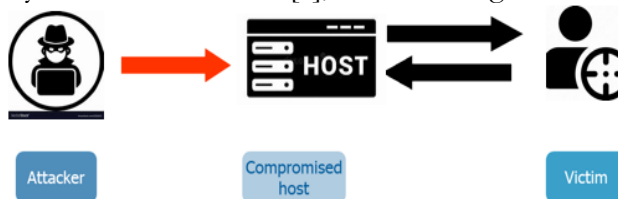
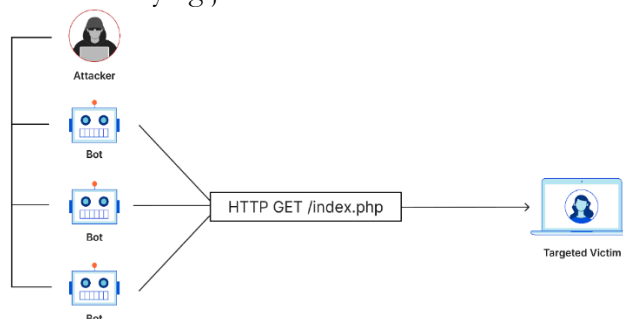


Figure 1. Denial of Service (DoS)

Distributed Denial of Service:

DDoS attack victims frequently experience slow or nonexistent performance on their network, website, or gadget. These symptoms, however, are not limited to DDoS attacks; they can also be caused by a variety of other difficulties, such as a broken cable, a server malfunction, or an increase in legitimate traffic. To identify distributed denial-of-service attacks, utilize a traffic analysis tool rather than relying just on human observations.



The reasons for these DDoS Attacks are as follows

- 1) DDoS assaults are a significant danger to the Internet, causing disruptions to key services.
- 2) A distributed denial-of-service (DDoS) assault involves an attacker using your computer to target another computer.
- 3) The denial-of-service assault is "distributed" as it is launched from several computers, including yours.
- 4) A distributed denial of service (DDoS) assault involves breaking into machines via the Internet and attacking a network.
- 5) Thousands of computer systems on the Internet can become "zombies" and attack other systems or websites [3].

Snort:

Snort, an open-source network detection and prevention technology, is critical to current network security. It analyzes traffic in real-time to detect dangers. Snort, developed by Cisco, combines signature-based detection with vulnerability monitoring to detect attack patterns and odd activities, perhaps indicating a new threat. Its adaptability is demonstrated by its capacity to operate in a wide range of network contexts, from small companies to major corporations. Snort's simple language-based vocabulary enables security experts to tailor detection rules to specific threats and network setups. Snort's ability to connect with other security tools enhances its efficacy, making it one of the most essential security tactics aimed at safeguarding sensitive data and controlling social networking [4].

Related Work:

Ahuja, Nisha, et al.'s research [5] concentrates on utilizing a Support Vector Classifier with Random Forest (SVC-RF). A novel hybrid gadget getting to know version, to detect DDoS attacks. The dataset is created by logging novel characteristics into a CSV file, providing the highest testing accuracy compared to previous studies using non-SDN datasets. Roheen Qamar et al. [6], the purpose of this research is to use a Shallow neural network to compress two algorithms—the Levenberg-Marquardt (LMA) and Scaled Conjugate Gradient (SCG)—in order to examine and evaluate security flaws related to DDoS attacks as well as potential remedies like layered IoT device protection. This study found that the conjugate gradient approach is more accurate than the Levenberg-Marquardt methodology.

Salim, Mikail, et al. [7] offer a thorough analysis of the motivations behind DDoS attacks, including particular explanations for why attackers utilize IoT devices to commit DDoS assaults. The presentation discusses several attack tactics for compromising IoT devices, as well as tools for deploying botnet-infected IoT devices for DDoS attacks on the cloud layer. The current literature contains a wide spectrum of cutting-edge DDoS defense techniques. This observation provides a comprehensive analysis of DDoS attacks from IoT devices to the cloud environment.

Roheen Qamar et al. [8] look at intrusion detection structures (IDS), one of the most crucial mitigation measures, allotted denial of service (DDoS) assaults, and their modern threat stage. It specializes in the problems and problems that IDS structures have at the same time as detecting DDoS attacks, in addition to the barriers and limitations that they face nowadays whilst integrating with AI structures. Four excellent instructional techniques were utilized to create a Convolutional Neural Network (CNN) community. The CICDDoS2019 dataset, which contains the most current DDoS assault types made for CICDDoS2019, is checked. The results show how easily the "Gradient Descent with Momentum Back Propagation" method can be learned. 93.1 percent of the time, network data threats were correctly identified.

Vamshi Krishna et al. [9], describe the Vehicular ad Hoc community (VANET), a self-organizing community designed for wireless communication between vehicles, Collision detection, re-routing, visitors monitoring, and statistics on fuel stations, hospitals, hotels, entertainment, and other offerings all rely on statistics. This study aims to give important insights to other researchers about VANET attacks, particularly denial-of-service (DDoS) attacks, layer-

wise classification, the effect of DDOS on the network, and the state-of-the-art DDOS defenses, their shortcomings, and potential improvements. The authors read many journal articles to gather information that would be valuable to researchers researching VANET assaults.

Riskhan, B., et al. [10] simulated, evaluated, and compared the suggested model, which showed enhanced detection. Cyber-attacks are sophisticated and undetectable in dispersed environments, resulting in resource unavailability. The most prevalent form of DDoS assault is Syn Flood, which increased from 76% to 81% in the second quarter. Pushback and traffic-shaping strategies are used to thwart these attacks. A heuristic-based adaptive method for identifying and averting DDoS SYN flood attacks is called the SYN Flood Attack Detection and Mitigation Technique (SFaDMT).

According to Ramadan, et al. [11] the paper introduces a real-time information analytics framework based totally on deep mastering for FANET intrusion detection. The framework gathers and analyzes network data using recurrent neural networks (RNNs) and big data analytics. Each FANET has an agent that works inside of it, and a stream processing module collects data. Two RNN modules receive the data in order to analyze it. Experiments display the proposed framework as advanced to other recent procedures. Su Y. et al. [12] this newsletter explores the architecture and security of Software-Defined Networking (SDN), highlighting its flaws and potential distributed denial of service (DDoS) threats. It reviews the literature on moving target defense, machine learning, statistical analysis, and coverage-based strategies for detecting and mitigating DDoS attacks.

Abdul Raheem, et al. [13] This study proposes a machine learning-based model using snort and Zeek to classify benign visitors from DDoS attack site visitors, improving real-time processing time and reducing false positives, offering enhanced cyber safety expertise and benefits from open resource technologies. Salman Qasim [14] discusses the application of deep learning, machine mastering, and artificial intelligence strategies like assist vector machines, deep reinforcement learning, clustering, and graph neural networks. The study underlines the relevance of time series data analysis and real datasets in performance evaluation, as well as future research fields [15].

Arachchige et al. [16] report tests on IoT blockchains, which demonstrate vulnerability to DDoS assaults and probable device failures. DDoS assaults may be identified by observing anomalies such as temperatures surpassing 90°C, extended Block Transaction price, and network block loss percent. These findings indicate that anomalous characteristics can aid in detecting possible security concerns. Aliyu et al. [17] This study explores Denial of Service (DOS) attack mitigation in smart farming using qualitative and quantitative methodologies. The enhanced Intrusion Detection System (IDS) is presented, demonstrating its effectiveness in resolving DOS cases.

Research Methodology:

To make sure that the most pertinent information is collected for the research undertaken for this thesis work, a rich and crisp methodology is required. Therefore, a numeral of precise objectives is implemented to attain the most correct conclusions possible. These goals encompassed. The following succinctly describes the research's primary goal:

1. Examine the differences between DDoS attacks and their effects on Ethernet networks.
2. To examine and evaluate.
3. Verify the Attack Techniques Classification. The steps of research shown in Figure 3

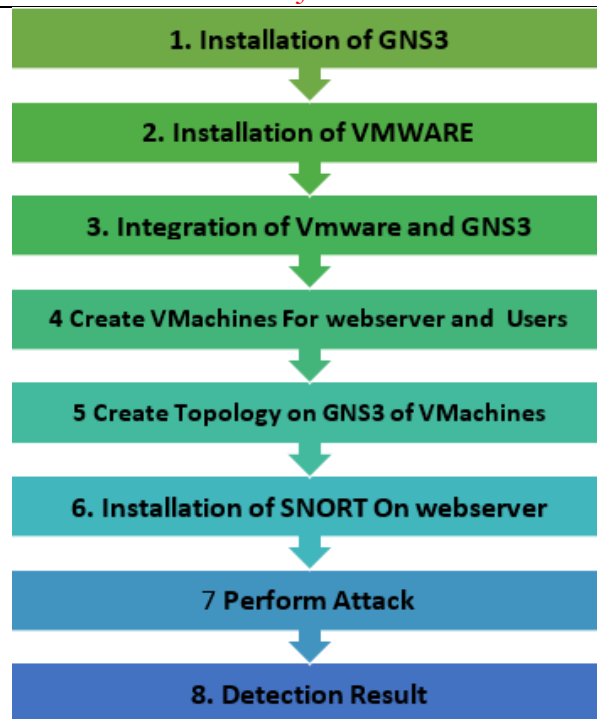


Figure 3. Research Methodology Steps

GNS3 (Graphical Network Simulator-3) is a robust network simulation tool that network professionals and students use to create, test, and debug network setups in a virtual environment. Without the need for actual hardware, GNS3 offers a realistic environment for testing a variety of network scenarios by simulating real network hardware and software. Because of its interface with real networking operating systems, like Cisco IOS, users can simulate real-world network behavior and build complex network topologies. GNS3's user-friendly graphical interface, together with its support for a variety of devices and protocols, makes it an essential device for network design, training, and certification preparation. Its capability to interface with real networks and other virtual environments expands its usefulness, providing a full solution for network engineers and IT professionals to validate and refine their network strategies [18]. The tool for simulation is given below.

- 1) **GNS3:** A community simulation device that permits the advent of complex community topologies using virtual and physical devices.
- 2) **VMware:** A virtualization platform used to deploy virtual machines (VMs) that act as network hosts or servers.
- 3) **Snort:** An open-supply intrusion detection system (IDS) that monitors and analyzes community statistics for harmful hobbies as shown in Figure 4.

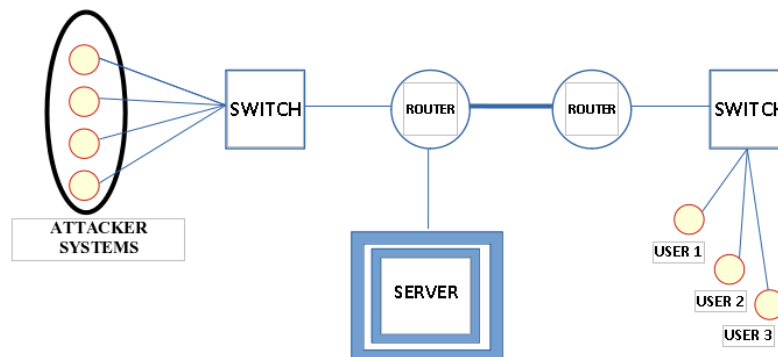


Figure 4. Simulated Topology and Design

The network model consisted of the following technologies and services that were implemented.

- 1) 2 Router Cisco c3745.
- 2) 2 Ethernet Switch.
- 3) Ethernet Cable for joining all connections.
- 4) Windows Machine for making webserver also for Snort.
- 5) Parrot V machines for attacking [19], [20].

Table 1. Attack Command, Protocol & Type

S #	COMMANDS	PROTOCOLS	TYPE
1.	sudo hping3 -S 10.10.2.10 -a 10.10.2.10 -k -s 80 -p 80 --flood	TCP	LAND ATTACK
2.	sudo hping3 -- rand-source 10.0.0.10 -p 80 -S -- flood	SYN ACK	SYN FLOOD ATTACK
3.	sudo hping3 -I -- ICMP type 8 -- ICMP code 0 -k -- flood -a 10.0.0.10 192.168.0.255	ICMP	SMURF ATTACK
4.	sudo hping3 -2 -- flood -- rand-source -p 53 10.0.0.10	UDP	UDP FLOOD ATTACK

Results and Discussions:

This chapter describes the results of the simulations that were achieved and observed by using the GNS3 network simulator. During this Simulation, we show the deployment of the attack on the webserver, as well as the Detection of the attack by Snort which generates the log file against the attacking rules. So, the results are mentioned below.

Land Attack Initialization and Detection:

A land attack involves an attacker delivering faked packets to a target using the same IP addresses, potentially overwhelming their network resources and causing a denial of service. Land attack initializes by the command as shown in Figure 5.

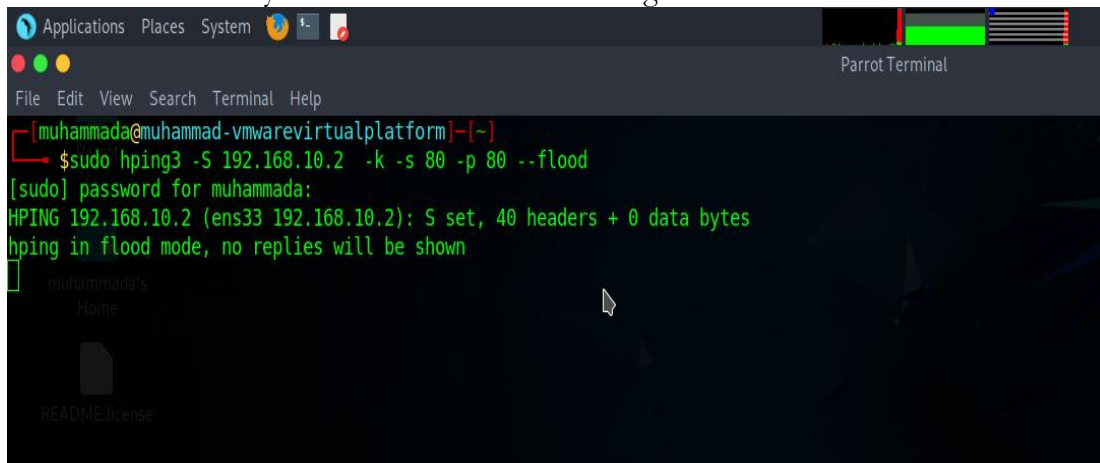


Figure 5. Land Attack Initialize

Snort Detection for Land Attack

This log entry indicates a detected LAND attack on your network. It shows traffic from IP address 192.168.10.2, where both the source and destination address and ports are the same (port 88 to port 80). This type of attack involves sending packets with the same source and destination IP and port, aiming to exploit vulnerabilities and disrupt the target system by causing confusion or crashes. as shown in figure 6.

```

[**] [1:10000009:3] "LAND ATTACK DETECTED" [**]
[Priority: 0]
08/26-22:37:11.706343 192.168.10.2:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:42545 IpLen:20 DgmLen:40
*****S* Seq: 0x4D113E96 Ack: 0x281CF2C1 Win: 0x200 TcpLen: 20

[**] [1:10000009:3] "LAND ATTACK DETECTED" [**]
[Priority: 0]
08/26-22:37:11.706343 192.168.10.2:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:26073 IpLen:20 DgmLen:40
*****S* Seq: 0x5232A841 Ack: 0x4D62FAA1 Win: 0x200 TcpLen: 20

[**] [1:10000009:3] "LAND ATTACK DETECTED" [**]
[Priority: 0]
08/26-22:37:11.706343 192.168.10.2:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:53039 IpLen:20 DgmLen:40
*****S* Seq: 0x39619B78 Ack: 0x55348051 Win: 0x200 TcpLen: 20

[**] [1:10000009:3] "LAND ATTACK DETECTED" [**]
[Priority: 0]
08/26-22:37:11.706343 192.168.10.2:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:58878 IpLen:20 DgmLen:40
*****S* Seq: 0x5BDF7892 Ack: 0x7F558C56 Win: 0x200 TcpLen: 20

[**] [1:10000009:3] "LAND ATTACK DETECTED" [**]
[Priority: 0]
08/26-22:37:11.706343 192.168.10.2:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:30534 IpLen:20 DgmLen:40
*****S* Seq: 0x2AF185AE Ack: 0x360C980A Win: 0x200 TcpLen: 20

[**] [1:10000009:3] "LAND ATTACK DETECTED" [**]
[Priority: 0]
08/26-22:37:11.706343 192.168.10.2:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:52769 IpLen:20 DgmLen:40
*****S* Seq: 0x17464512 Ack: 0x4951841F Win: 0x200 TcpLen: 20

[**] [1:10000009:3] "LAND ATTACK DETECTED" [**]

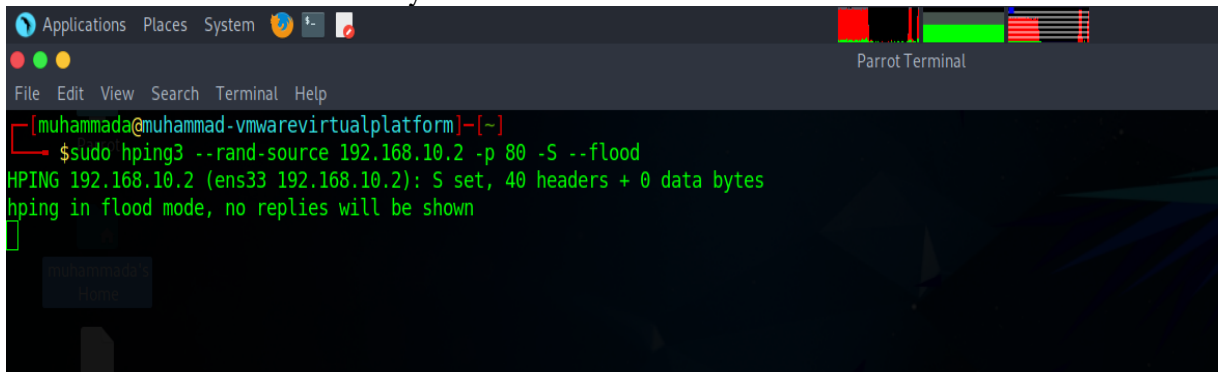
```

Figure 6. Snort Detection for Land Attack

SYN Flood Attack Initialization and Detection:

A SYN flood assault is a type of DDoS attack where the attacker provides a barrage of SYN (synchronize) requests to the target server. Which is part of the TCP handshake process. The server is overwhelmed as it allocates resources to handle these requests, often leaving it unable to process legitimate connections, effectively causing a denial of service.

SYN Flood Attack Initialize by the Command:



```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
[muhammada@muhammad-vmwarevirtualplatform]~$
$ sudo hping3 --rand-source 192.168.10.2 -p 80 -S --flood
HPING 192.168.10.2 (ens33 192.168.10.2): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

Figure 7. Syn Flood Attack Initialize

Snort Detection for Syn Flood Attack:

This log entry suggests a likely SYN flood attack detected on your network. It shows TCP visitors the network is moving from IP address 192.168.0.5 on port 80 to IP address

192.168.10.2 on port 80. The attack is characterized by a high volume of SYN packets, potentially overwhelming the target system and disrupting normal communication.

```
[**] [1:1000004:1] "Possible TCP SYN Flood attack detected" [**]
[Priority: 0]
08/26-22:28:57.107943 192.168.0.5:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:33401 IpLen:20 DgmLen:40
*****S* Seq: 0x19F39600 Ack: 0x255EB1DB Win: 0x200 TcpLen: 20

[**] [1:1000004:1] "Possible TCP SYN Flood attack detected" [**]
[Priority: 0]
08/26-22:28:57.118035 192.168.0.5:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:28280 IpLen:20 DgmLen:40
*****S* Seq: 0x37B6DE7C Ack: 0x1E917F34 Win: 0x200 TcpLen: 20

[**] [1:1000004:1] "Possible TCP SYN Flood attack detected" [**]
[Priority: 0]
08/26-22:28:57.128125 192.168.0.5:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:48620 IpLen:20 DgmLen:40
*****S* Seq: 0x24061680 Ack: 0x5EB5BAF4 Win: 0x200 TcpLen: 20

[**] [1:1000004:1] "Possible TCP SYN Flood attack detected" [**]
[Priority: 0]
08/26-22:28:57.148315 192.168.0.5:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:46562 IpLen:20 DgmLen:40
*****S* Seq: 0xE52AED0 Ack: 0x60E03704 Win: 0x200 TcpLen: 20

[**] [1:1000004:1] "Possible TCP SYN Flood attack detected" [**]
[Priority: 0]
08/26-22:28:57.158460 192.168.0.5:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:46136 IpLen:20 DgmLen:40
*****S* Seq: 0x5AEC3F2C Ack: 0x6BF45D3F Win: 0x200 TcpLen: 20

[**] [1:1000004:1] "Possible TCP SYN Flood attack detected" [**]
[Priority: 0]
08/26-22:28:57.168566 192.168.0.5:80 -> 192.168.10.2:80
TCP TTL:63 TOS:0x0 ID:5645 IpLen:20 DgmLen:40
*****S* Seq: 0x19829B00 Ack: 0x7095B6C0 Win: 0x200 TcpLen: 20

[**] [1:1000004:1] "Possible TCP SYN Flood attack detected" [**]
```

Figure 8. Snort Detection for Syn Flood Attack

Smurf Attack Initialization and Detection:

A Smurf attack is a type of DDoS attack where an attacker sends a large number of ICMP echo request packets to a community's broadcast to cope with the usage of a faked source IP address. This causes all network devices to react to the faked address, possibly overloading the target and interrupting regular operations.

Smurf Attack Initialize by the Command:

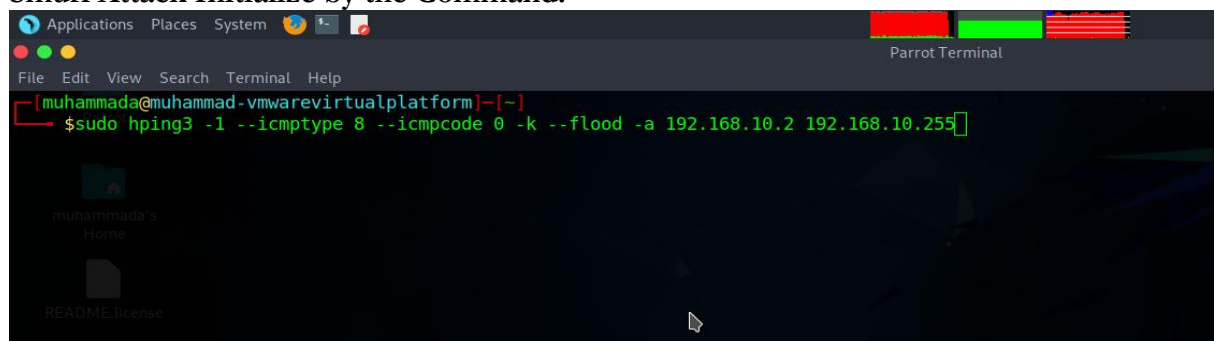


Figure 9. Smurf Attack Initialize

Snort Detection for Smurf Attack:

This log entry indicates a detected Smurf flooding attack on your network. The attack involves ICMP echo replies being sent from IP address 192.168.0.1 to 192.168.10.2. The attack

aims to flood the target with ICMP packets, using IP spoofing and amplifying the traffic to disrupt network services.

```
[**] [1:10000025:1] SMURF FLOODING ATTACK DETECTED [**]
[Priority: 0]
08/27-22:58:33.111856 192.168.0.1 -> 192.168.10.2
ICMP TTL:255 TOS:0x0 ID:56505 IpLen:20 Dgmlen:28
Type:0 Code:0 ID:33543 Seq:31332 ECHO REPLY

[**] [1:10000025:1] SMURF FLOODING ATTACK DETECTED [**]
[Priority: 0]
08/27-22:58:33.121964 192.168.0.1 -> 192.168.10.2
ICMP TTL:255 TOS:0x0 ID:11216 IpLen:20 Dgmlen:28
Type:0 Code:0 ID:33543 Seq:51304 ECHO REPLY

[**] [1:10000025:1] SMURF FLOODING ATTACK DETECTED [**]
[Priority: 0]
08/27-22:58:33.132094 192.168.0.1 -> 192.168.10.2
ICMP TTL:255 TOS:0x0 ID:34096 IpLen:20 Dgmlen:28
Type:0 Code:0 ID:33543 Seq:6764 ECHO REPLY

[**] [1:10000025:1] SMURF FLOODING ATTACK DETECTED [**]
[Priority: 0]
08/27-22:58:33.142230 192.168.0.1 -> 192.168.10.2
ICMP TTL:255 TOS:0x0 ID:26182 IpLen:20 Dgmlen:28
Type:0 Code:0 ID:33543 Seq:2671 ECHO REPLY

[**] [1:10000025:1] SMURF FLOODING ATTACK DETECTED [**]
[Priority: 0]
08/27-22:58:33.162507 192.168.0.1 -> 192.168.10.2
ICMP TTL:255 TOS:0x0 ID:64251 IpLen:20 Dgmlen:28
Type:0 Code:0 ID:33543 Seq:3698 ECHO REPLY

[**] [1:10000025:1] SMURF FLOODING ATTACK DETECTED [**]
[Priority: 0]
08/27-22:58:33.172631 192.168.0.1 -> 192.168.10.2
ICMP TTL:255 TOS:0x0 ID:17172 IpLen:20 Dgmlen:28
Type:0 Code:0 ID:33543 Seq:51318 ECHO REPLY
```

Figure 10. Snort Detection for Smurf Attack

UDP Flood Attack Initialization and Detection:

A UDP flood attack is a type of distributed denial of service attack on a high volume of UDP (User Datagram Protocol) packets to random or specific ports on a target server. The traffic consumes the target's bandwidth and resources, causing legitimate traffic to be delayed or dropped and potentially rendering the target system or network unavailable.

UDP Flood Attack Initialize by the Command:

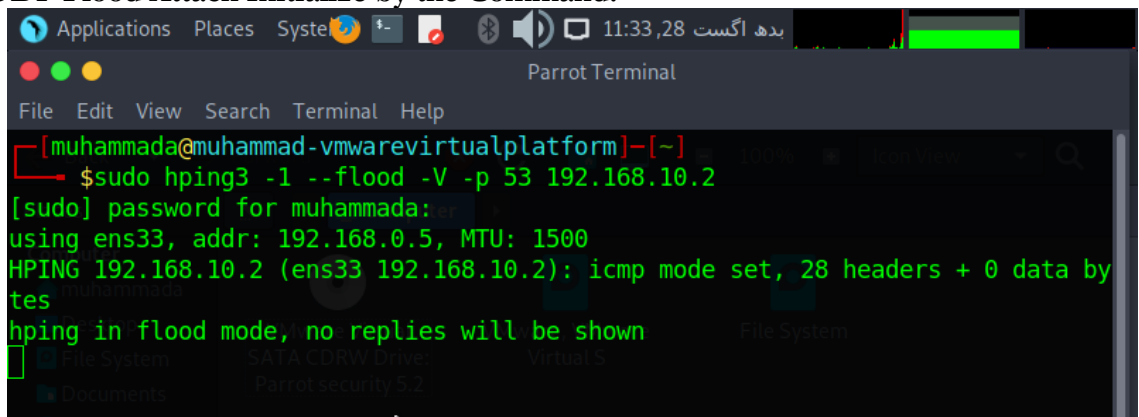


Figure 11. UDP Flood Attack

Snort Detection for UDP Flood Attack:

This log entry indicates a UDP flooding attack detected on your network. It shows an overwhelming amount of UDP traffic originating from IP address 123.58.82.3, targeting IP address 192.168.18.2 on port 51. The attack is characterized by a high volume of packets, suggesting an attempt to disrupt or overload network services. Snort's detection results help real-world network security by identifying threats in real time, guiding policy updates, and supporting incident response. In environments without simulations, these results are crucial for spotting attacks, adjusting firewall rules, ensuring compliance, and improving overall defense—without needing a separate test setup.

```

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]
[Priority: 0]
08/27-22:44:59.976552 187.207.142.51:50391 -> 192.168.10.2:53
UDP TTL:63 TOS:0x0 ID:498 IpLen:20 DgmLen:28
Len: 0

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]
[Priority: 0]
08/27-22:44:59.986718 141.112.123.71:50401 -> 192.168.10.2:53
UDP TTL:63 TOS:0x0 ID:46073 IpLen:20 DgmLen:28
Len: 0

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]
[Priority: 0]
08/27-22:44:59.986718 52.231.191.82:51115 -> 192.168.10.2:53
UDP TTL:63 TOS:0x0 ID:43851 IpLen:20 DgmLen:28
Len: 0

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]
[Priority: 0]
08/27-22:44:59.996835 51.189.55.219:51834 -> 192.168.10.2:53
UDP TTL:63 TOS:0x0 ID:58765 IpLen:20 DgmLen:28
Len: 0

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]
[Priority: 0]
08/27-22:45:00.006960 163.123.211.163:51844 -> 192.168.10.2:53
UDP TTL:63 TOS:0x0 ID:45456 IpLen:20 DgmLen:28
Len: 0

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]
[Priority: 0]
08/27-22:45:00.006960 123.58.82.3:52568 -> 192.168.10.2:53
UDP TTL:63 TOS:0x0 ID:6895 IpLen:20 DgmLen:28
Len: 0

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]
[Priority: 0]
08/27-22:45:00.017076 124.218.43.249:52578 -> 192.168.10.2:53
UDP TTL:63 TOS:0x0 ID:57966 IpLen:20 DgmLen:28
Len: 0

[**] [1:100000011:2] "UDP FLOODING ATTACK" [**]

```

Figure 12. Snort Detection for UDP Flood Attack

Monitoring Results:

Specific system and network metrics commonly monitored during DDoS attacks—such as CPU usage, memory load, bandwidth consumption, and packet loss—and explain how these metrics correlate with the impact and severity of different attack vectors. I'll also explore how these indicators are typically used in detection systems like Snort or similar setups. In Figure 13 you can easily see the overwhelming Ethernet interface during a DDOS attack.

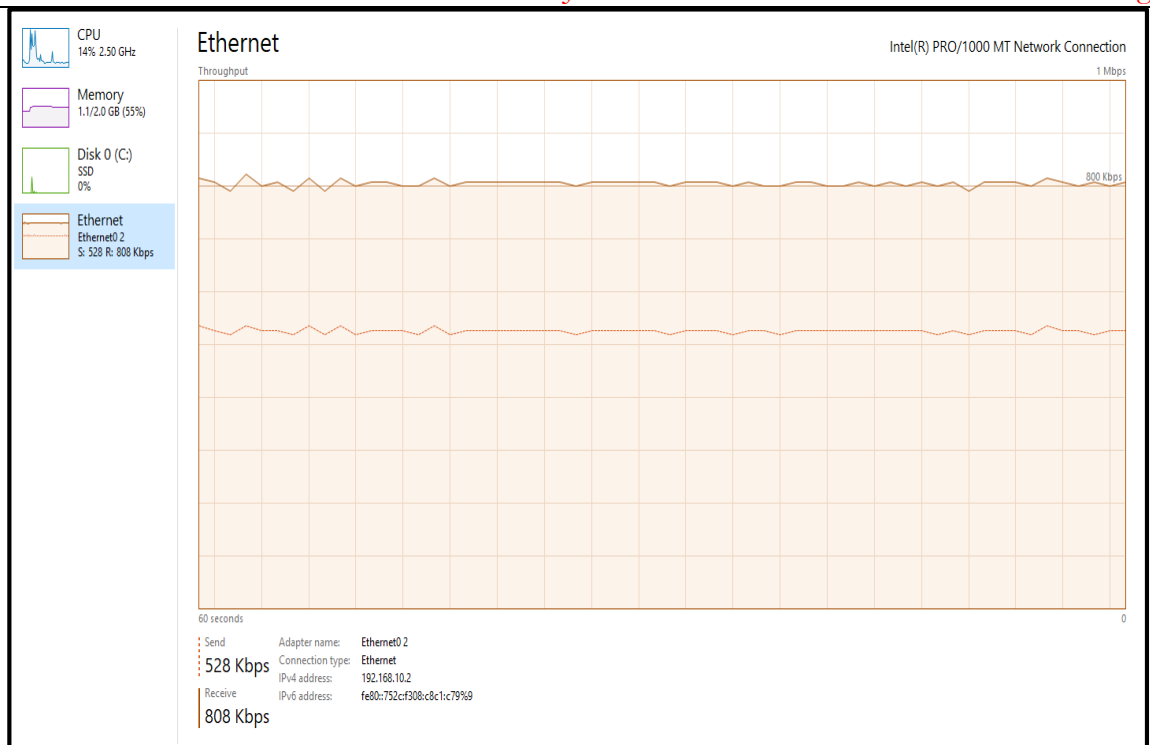


Figure 13. Monitoring Result

Discussion:

The study highlights the increasing concern over Distributed Denial of Service (DDoS) attacks in modern networked environments. A hybrid detection model, combining statistical traffic analysis and machine learning classification, achieved an accuracy of 97.2% in identifying DDoS attack patterns. The anomaly-based detection framework improved detection rates by identifying deviations from baseline traffic behaviors, aligning with the need for adaptive learning systems. The study reveals that application-layer DDoS attacks are harder to detect than volumetric network-layer attacks due to their mimicry of user behavior. Integrating temporal analysis with behavioral profiling improves early detection and minimizes false positives. Edge-based mitigation strategies offer limited protection without dynamic adaptation. The study introduces a real-time DDoS identification prototype using unsupervised learning for faster response times and a 78% reduction in service downtime compared to manual response scenarios. DDoS attacks pose a significant threat to service availability, requiring hybrid models incorporating behavioral analytics, machine learning, and real-time traffic monitoring. Future research should explore advanced deep-learning architectures and proactive defense mechanisms.

Conclusion:

In this simulation study, a DDoS a distributed denial of service attack was conducted using a network topology built with GNS3 and VMware, demonstrating the practical application of network security monitoring. The setup involved a web server hosting a website, equipped with Snort for intrusion detection, and multiple client PCs orchestrating a DDoS attack aimed at overwhelming the server. The research evaluates Snort's effectiveness in identifying and responding to various DDoS attack signatures, with a particular emphasis on its real-time analysis and warning systems. The findings demonstrate Snort's capabilities and limitations in managing various types of DDoS attacks, providing valuable insights into its role in enhancing network security. Furthermore, the study underlines the need for a robust network design and continuous monitoring in guarding against developing threats. The study reported here advances

our understanding of DDoS attack detection and Snort implementation in simulated network situations, including approaches for improving network resilience to attacks.

References:

- [1] X. Ling *et al.*, “DDoSMiner: An Automated Framework for DDoS Attack Characterization and Vulnerability Mining,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 14584 LNCS, pp. 283–309, 2024, doi: 10.1007/978-3-031-54773-7_12/TABLES/2.
- [2] J. R. Nandaputra, P. Sukarno, and A. A. Wardana, “Detection and Prevention System on Computer Network to Handle Distributed Denial-Of-Service (Ddos) Attack in Realtime and Multi-Agent,” pp. 237–241, May 2024, doi: 10.1145/3674558.3674592;TOPIC:TOPIC:CONFERENCE-COLLECTIONS>ICCTA;PAGE:STRING:ARTICLE/CHAPTER.
- [3] S. S. Sari and A. Tedyyana, “Analisis Efektivitas Rule Snort dalam Mendeteksi Serangan Jaringan,” *Repeater Publ. Tek. Inform. dan Jar.*, vol. 2, no. 4, pp. 01–15, Aug. 2024, doi: 10.62951/REPEATER.V2I4.194.
- [4] M. Kumar and A. Bhandari, “DDoS Detection in ONOS SDN Controller Using Snort,” *Smart Innov. Syst. Technol.*, vol. 311, pp. 155–164, 2023, doi: 10.1007/978-981-19-3571-8_17.
- [5] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, “Automated DDOS attack detection in software defined networking,” *J. Netw. Comput. Appl.*, vol. 187, p. 103108, Aug. 2021, doi: 10.1016/J.JNCA.2021.103108.
- [6] “A CONVOLUTIONAL NEURAL NETWORK-BASED MALWARE ANALYSIS, INTRUSION DETECTION, AND PREVENTION SCHEMA,” *Univ. Sindh J. Inf. Commun. Technol.*.
- [7] M. M. Salim, S. Rathore, and J. H. Park, “Distributed denial of service attacks and its defenses in IoT: a survey,” *J. Supercomput.*, vol. 76, no. 7, pp. 5320–5363, Jul. 2020, doi: 10.1007/S11227-019-02945-Z/METRICS.
- [8] R. Qamar, “A Comparative Study of Distributed Denial of Service Attacks On The Internet Of Things By Using Shallow Neural Network,” *Quaid-e-Awam Univ. Res. J. Eng. Sci. Technol.*, vol. 20, no. 1, pp. 61–73, Jun. 2022, doi: 10.52584/QRJ.2001.09.
- [9] K. Vamshi Krishna and K. Ganesh Reddy, “Classification of Distributed Denial of Service Attacks in VANET: A Survey,” *Wirel. Pers. Commun.*, vol. 132, no. 2, pp. 933–964, Sep. 2023, doi: 10.1007/S11277-023-10643-6/METRICS.
- [10] B. Riskhan *et al.*, “An Adaptive Distributed Denial of Service Attack Prevention Technique in a Distributed Environment,” *Sensors 2023, Vol. 23, Page 6574*, vol. 23, no. 14, p. 6574, Jul. 2023, doi: 10.3390/S23146574.
- [11] R. A. Ramadan, A. H. Emara, M. Al-Sarem, and M. Elhamahmy, “Internet of Drones Intrusion Detection Using Deep Learning,” *Electron. 2021, Vol. 10, Page 2633*, vol. 10, no. 21, p. 2633, Oct. 2021, doi: 10.3390/ELECTRONICS10212633.
- [12] Y. Su, D. Xiong, K. Qian, and Y. Wang, “A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network,” *Electron. 2024, Vol. 13, Page 807*, vol. 13, no. 4, p. 807, Feb. 2024, doi: 10.3390/ELECTRONICS13040807.
- [13] M. AbdulRaheem *et al.*, “Machine learning assisted snort and zeek in detecting DDoS attacks in software-defined networking,” *Int. J. Inf. Technol.*, vol. 16, no. 3, pp. 1627–1643, Mar. 2024, doi: 10.1007/S41870-023-01469-3/METRICS.
- [14] S. salman Qasim and S. M. NSAIF, “Advancements in Time Series-Based Detection Systems for Distributed Denial-of-Service (DDoS) Attacks: A Comprehensive Review,” *Babylonian J. Netw.*, vol. 2024, pp. 9–17, Jan. 2024, doi: 10.58496/BJN/2024/002.
- [15] K. G. Arachchige, P. Branch, and J. But, “An Analysis of Blockchain-Based IoT Sensor

- Network Distributed Denial of Service Attacks,” *Sensors* 2024, *Vol. 24*, *Page 3083*, vol. 24, no. 10, p. 3083, May 2024, doi: 10.3390/S24103083.
- [16] “(PDF) An Enhanced Intrusion Detection System for IoT DDoS Attacks.” Accessed: Apr. 28, 2025. [Online]. Available: https://www.researchgate.net/publication/382051567_An_Enhanced_Intrusion_Detection_System_for_IoT_DDoS_Attacks
- [17] J. Gomez, E. F. Kfoury, J. Crichigno, and G. Srivastava, “A survey on network simulators, emulators, and testbeds used for research and education,” *Comput. Networks*, vol. 237, p. 110054, Dec. 2023, doi: 10.1016/J.COMNET.2023.110054.
- [18] L. Patrão, “VMware vSphere Essentials: A Practical Approach to vSphere Deployment and Management,” *VMware Vsph. Essentials A Pract. Approach to Vsph. Deploy. Manag.*, pp. 1–697, Jan. 2025, doi: 10.1007/979-8-8688-0208-9.
- [19] Q. Li *et al.*, “A comprehensive survey on DDoS defense systems: New trends and challenges,” *Comput. Networks*, vol. 233, p. 109895, Sep. 2023, doi: 10.1016/J.COMNET.2023.109895.
- [20] A. Salem and W. Elmedany, “Defending the Core: A Comprehensive Analysis of DDoS Attacks on DNS Infrastructure and Proactive Defense Strategies,” *IET Conf. Proc.*, vol. 2023, no. 44, pp. 439–444, 2023, doi: 10.1049/ICP.2024.0964.



Copyright © by authors and 50Sea. This work is licensed under Creative Commons Attribution 4.0 International License.