Journal of Engineering Sciences (Improsci)
e-ISSN: 3031-7088
p-ISSN: 3032-3452

Intrusion Prevention System to Protect Dos Attack

Arif Nurudin [1*], Ismael Mubariq [2]
[1*] Industrial Engineering, University of Muhammadiyah Cirebon, Indonesia. Email arif.nurudin@umc.ac.id
[2]Informatic Engineering, University of Muhammadiyah Cirebon, Indonesia. Email ismaelmubaruq8@gmail.com
Corresponding Author : e-mail arif.nurudin@umc.ac.id

Abstract. Data security on a network infrastructure is a very sensitive and vulnerable matter. One alternative to overcome this is to use IPS (Intrusion Prevention System) technology where the technology is a development of IDS (Intrusion Detection System) which uses Snort. In this study, IPS technology is applied using the Untangle Firewall where the Intrusion Prevention feature is available on the platform with the intention of testing the feature on the Untangle Firewall. Testing was carried out using DoS (Denial Of Service) and SSH Brute Force attacks where the Intrusion Prevention feature on the Untangle Firewall can recognize both attacks and can block the attacks using manually added rules.

Keywords: Data Security, Intrusion Prevention System (IPS), Snort, Untangle Firewall, DoS Attack, SSH Brute Force

INTRODUCTION

Data security in a network system is the most sensitive and vulnerable thing, especially for large agencies that need more secure data security. A real example of a network attack that has occurred is the attack on the Telkomsel Website some time ago by means of Web Defacing or it can be said that the web was breached and then the content of the display of the website was changed. In addition, a small example that often occurs in network systems is an attempt from a group of people to break into an access right such as username and password of a network system, of course such a thing is very unwanted and detrimental to the network owner because it can interfere and even damage the performance of the network itself. There are many alternative ways to prevent attacks on computer networks, one of which is to apply Intrusion Prevention System (IPS) technology, where the technology is a development of IDS (Intrusion Detection System) that uses Snort. This technology makes it possible to detect attacks and prevent them from doing so by working based on the rules applied. Each type of attack that is to be detected

and countered is applied through rules defined in the snort system. The application of IPS technology by installing snort and applying ip tables on linux. However, not many have applied Intrusion Prevention System technology using Untangle Firewall. In Untangle Firewall there are many features to help secure the network system that is built, one of which is the Intrusion Prevention feature. The existence of this feature attracted the author to learn how intrusion prevention works on Untangle Firewall. In the tests carried out, the author chose DoS Attack and SSH Bute Force. The test was chosen because both attacks are very commonly used and are quite easy to implement, although the impact of both attacks is also very bad where DoS Attack can damage the system by flooding the packets on the system and SSH Brute Force is an attack to find out the access rights of a system. The purpose of testing the Intrusion Prevention feature on the Untangle Firewall is to find out how the Intrusion Prevention on the Untangle Firewall works, and also to find out the results of the tests carried out. Then the benefits of testing the Intrusion Prevention feature on the Untangle Firewall are so that the network security system becomes better and get an overview of the performance of the Untangle Firewall on the Intrusion Prevention feature.

DoS Attack Definition

A DOS (Denial of Service) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by flooding the target or surrounding infrastructure with a flood of Internet traffic. This makes the service unavailable to authorized users. Here are the details of what you need to know about DOS attacks.

- Types of DOS Attacks
    1. Volumetric Attack:
        a. UDP floods: An attacker sends a large number of UDP packets to a random port on a remote host. The host checks the application listening on that port and, because it doesn't find it, sends back a packet indicating that its destination is unreachable. This process consumes significant resources.
        b. ICMP Flood (Ping Flood): An attacker sends a large number of ICMP Echo Request (ping) packets, thus flooding the target network.
    2. Protocol Attack:
        a. SYN Flood: An attacker sends a series of SYN requests to the target system in an attempt to use enough server resources to make the system unresponsive to legitimate traffic.

   b. Ping of Death: The attacker sends an incorrectly formatted or oversized packet to the target. These packets are fragmented and, when reassembled, cause crashes or crashes on the target system due to buffer overflow.
3. Application Layer Attack:
   a. HTTP Flood: An attacker sends a seemingly legitimate HTTP GET or POST request to the web server, thus overwhelming it.
   b. Slowloris: Attackers leave connections open by sending partial HTTP requests, never completing requests, and thus consuming server resources.

- Distributed Denial of Service (DDoS)

A DDoS attack is a large-scale DOS attack in which the perpetrator uses multiple systems, often a botnet (compromised computer network), to flood the target with traffic. Its scattered nature makes mitigation even more difficult.

- General Mitigation Techniques
  1. Firewalls and Routers: Enforce rules to stop malicious traffic.
  2. Load Balancer: Distributes incoming traffic across multiple servers to effectively manage the load.
  3. Rate Restrictions: Limits a user's requests to a service in a given period.
  4. Intrusion Detection and Prevention System (IDPS): Monitoring network traffic and responding to threats.
  5. Content Delivery Network (CDN): This network distributes traffic to multiple servers to absorb the impact of a DOS attack.
  6. Anti-DoS Services: Cloudflare, Akamai, and AWS Shield can help mitigate attacks.
- Detection and Response
  1. Traffic Analysis: Monitor and analyze network traffic to look for unusual patterns.
  2. Incident Response Plan: Have a plan in place to respond to DOS attacks, including communication protocols and measures to mitigate those attacks.
  3. Redundancy: Use redundant systems and failover mechanisms to maintain availability.

How DoS Attack Works

The main goal of a DoS attack is to make a server or network unavailable to users by overloading their traffic. Typically, this is done using one of two methods: flooding

the target with multiple malicious requests or crashing the target by sending a very large amount of data. Attackers most often use the first method. A flood attack is carried out by sending a large amount of traffic to a system or website, which ultimately overloads the system or website excessively and forces it to stop. These floods can be of various types such as ICMP floods, or SYN floods. They do so by submitting bugs that exploit weaknesses in the target system. As a result, the system crashes.

DoS attacks do not rely on the execution of specific programs on the targeted system but rather take advantage of weaknesses inherent in network communication protocols. In a DoS attack, the computer is programmed to send hundreds or thousands of fake requests to the target server. This request is usually sent only once to establish a connection between the end user and the website or server they are trying to access. The server/website then responds with a signal that recognizes that the user is authorized to connect. Every time you visit a website, a conversation occurs between your web browser and the server. The process by which the client and server make this connection is known as a handshake. When the target server is attacked with many fake requests, it will try to respond to the request, but because it is overwhelmed, it stops working.

Denial of Service (DoS) attacks exploit weaknesses in the communication infrastructure or protocols to overwhelm the target system's limited resources, making it unable to respond to legitimate user requests. Here are some common steps taken in a DoS attack:

1. Target Identification

   The attacker identifies the target, such as a website, server, or computer network, that they want to attack.

2. Method Selection

   The attacker chooses an attack method that suits the target system's weakness and the attack's goal. Common procedures include flood attacks, such as SYN floods, ICMP floods, HTTP floods, protocol attacks, or attacks on network infrastructure.

3. Resource Gathering

   The attacker gathers the resources necessary to launch the attack, such as a computer or botnet connected to the internet.

4. Launch of the attack

   The attacker launches the attack by sending many requests or traffic to the target system. This can be an incomplete TCP connection request (such as SYN packets in a SYN flood attack) or a large HTTP request in a short period (in an HTTP flood attack).

5. Distraction

   Some DoS attacks may also involve diverting attention from the source of the attack, such as using distributed DoS (DDoS) attacks that involve many different attack sources.

6. Monitoring and Handling

   The target system security team may try to monitor and handle attacks by identifying unusual traffic and blocking or filtering it or by adding additional resources to handle the additional load.

Examples of DoS Attack Cases

Here are some examples of Denial of Service (DoS) attacks:

1. Attacks on Electronic Commerce Websites

   A popular e-commerce website is the target of DoS attacks during periods of large sales, such as on "Black Friday" or "Cyber Monday." Attackers flood the website's servers with excessive requests, making it inaccessible to legitimate users. This can lead to huge losses for businesses that rely on online sales.

2. Attacks on Online Financial Services

   A large banking company was the target of a widespread DDoS attack. The attackers used a botnet of thousands of infected computers to flood banking websites with traffic, rendering online services inaccessible to customers who wanted to make banking transactions.

3. Attacks on Network Infrastructure

   A DoS attack aimed at disrupting business operations targets a corporate network. Attackers use flood attacks, such as SYN floods or ICMP floods, to flood a company's routers or network servers, causing a drop in performance or even an overall network failure.

4. Attacks on Cloud Service Providers

   A large cloud service provider was targeted by a DoS attack that made some major cloud services inaccessible to customers. This can disrupt business

operations that rely on cloud services for data storage, processing, or application hosting.

5. Attacks on Government Websites

   DoS attacks aimed at disrupting public services or spreading political messages target important government websites. This kind of attack can inconvenience citizens seeking information or services from government websites.

   In all of these cases, DoS attacks aim to make services unavailable to legitimate users, which can disrupt business operations, cause financial losses, or damage the targeted organization's reputation.

There are several examples of DoS Attack cases that have occurred in Indonesia, namely:

1. An attack by a child of the YogyaFree community on the website kaskus in 2008. This attack took place on May 16-17, 2008. The attack carried out by the yogyafree community resulted in the kaskus site being inaccessible and corrupt. This attack resulted in threads that had been created being locked by the kascus administrator. Because this lasted for quite a long time, finally the kaskus administrator was forced to shut down the kaskus server. This attack was a reply from the yogyafree community to the kaskus, according to the source this attack was carried out because yogyafree had been denounced on one of the forums in the kaskus. Some time there was a dispute between these two communities. Finally, this dispute was resolved when the site manager signed an online memorandum to end the dispute between the two. At that time, the message was displayed for several weeks on the pages of their respective websites. From this incident, Kaskus launched a new server that is more equipped with robust data security and is ready to face various attacks from various parties.
2. The incident that attacked DDOS also occurred in mid-2009, where domain.co.id had dropped for four days due to a DDOS attack. This shows a very basic weakness in the DNS CCTLD-ID system. This situation is very dangerous considering domain.co.id is one of Indonesia's strategic Internet infrastructures. Failure of the DNS CCTLD-ID system has the potential to cause economic losses. Because the domain drops automatically, the users cannot access the site with domain.co.id. for email users on yahoo.co.id. unable to access his email because his domain has gone down. Shortly after the incident, administrators were reported to be performing

maintenance on the domain's security system and until now it can still be enjoyed by the public.

3. Attack on government sites **http://www.polri.go.id**

   In 2013, there was an attack on a http://www.polri.go.id government website, which resulted in the disruption of public services. One of them is that in May 2013, the police website was down 10% and could not be accessed at all. As seen in the Picture.

The DDoS attack occurred because the public was dissatisfied with police services; in 2013, there were a lot of criminal cases related to the good name of the police, from fat accounts of police members to police officers who shot at residents. Several cases involving the name of the police attracted the cyber hacker community to take part in venting their frustrations. One of them is attacking the police website. Another factor that causes the DDoS attack on the police website is because of a prank, in other words, just following along. This is a criminal act that disrupts public services that are being disturbed by the police.

DDoS perpetrators are very difficult to catch because the location of the attack can be from anywhere, and it is carried out together at the same time; besides that, it is usually carried out by a fairly large community. Based on ITE Law No. 11 of 2008, some of the impacts of DDoS attacks can be charged with ITE Law No. 11 of 2008 Article 33, namely, "Every person deliberately and without rights or unlawfully commits any action that results in the disruption of the Electronic System and/or causes the Electronic System not to work as it should." With the threat of sanctions, the maximum prison sentence is 10 (ten) years and/or a maximum fine of Rp.10,000,000,000.00 (ten billion rupiah).

Disadvantages of DoS Attack

Denial of Service (DoS) attacks can cause various losses, whether for individuals, businesses, or organizations. Here are some of the losses that can occur as a result of a DoS attack:

1. Reputational Damage

   A successful DoS attack can make a service unavailable to legitimate users, harming the reputation of the targeted company or organization. If the attacks occur regularly or if the response to them is unsatisfactory, users may lose trust in the company and turn to competitors.

2. Financial Losses

   DoS attacks can cause both direct and indirect financial losses. Businesses that rely on online services for revenue, such as e-commerce or financial services, can lose revenue due to decreased sales or failed transactions. In addition, the costs incurred to address attacks and repair system failures can also be a significant financial burden.

3. Operational Disruption

   DoS attacks can disrupt overall business operations. The website or service that is the target of the attack may not be accessible to employees or customers, which can interfere with important communication, collaboration, or business processes.

4. Data Loss

   Some DoS attacks can lead to data loss or theft. DoS attacks that are accompanied by other attacks, such as malware attacks or distraction attacks, can be used to steal sensitive data or damage IT infrastructure.

5. Customer Losses

   Due to a DoS attack, customers or users who cannot access the services they need may lose trust and loyalty to the targeted company or organization. This can result in lost customers and potentially damage long-term relationships with the market.

6. Productivity Losses

   DoS attacks can disrupt employee productivity by disrupting access to systems or services needed to do their jobs. These disruptions can lead to decreased efficiency and employee performance and disrupt project schedules and deadlines.

Overall, DoS attacks have the potential to cause significant financial and operational losses to individuals, businesses, and organizations. Therefore, it is important to take appropriate preventive measures and have a good response plan to address DoS attacks.

How to Overcome DoS Attack

Addressing a Denial of Service (DoS) attack involves a combination of preventive and response measures. Here are some steps that can be taken to overcome a DoS attack:

1. Use of Firewall

   A powerful firewall installation can help filter traffic in and out of your network. A properly configured firewall can identify and block suspicious traffic that may be originating from a DoS attack.

2. Traffic Monitoring

   Monitoring network traffic regularly can help detect unusual activity or ongoing attacks. Network and system monitoring software can provide early warning of ongoing DoS attacks.

3. Using CDN (Content Delivery Network)

   The use of a CDN can help redirect web traffic from the original server to a geographically dispersed CDN server. This can help reduce the impact of DoS attacks by distributing traffic evenly across CDN networks.

4. Anti-DDoS Service Providers

   Some internet service providers offer anti-DDoS services specifically designed to protect websites and networks from DoS attacks. The service can filter out suspicious traffic and handle DoS attacks automatically.

5. Secure Server Configuration

   Configuring the server correctly and following strict security practices can help protect against DoS attacks. This includes updating the software regularly, restricting unnecessary access, and enabling security features such as SYN cookies to protect against SYN flood attacks.

6. Infrastructure Scalability

   Building a scalable infrastructure can help handle unexpected traffic spikes during a DoS attack. Having a backup of available resources and the ability to expand capacity can help keep services available even during an attack.

7. Emergency Response Plan

A detailed emergency response plan can help organizations address DoS attacks quickly and effectively. This plan should include steps to stop the attack, restore service, and investigate the incident after the attack has ended.

8. Cooperation with Authorities

   In the case of a severe DoS attack, it is important to work closely with authorities, such as internet service providers, law enforcement, or cybersecurity teams, to investigate the attack and follow up with the perpetrators.

9. Monitoring Traffic Gradually

   This step is in principle suitable to identify signs of a DDoS attack on our own server and we can distinguish which traffic is included in normal conditions and heavy conditions.

10. Increasing Bandwidth

    We can give the system we have additional time so that its processes do not go down and so that DDoS attacks are minimized.

    With a combination of technical precautions and the right response plan, organizations can reduce the risk of a DoS attack and reduce its impact if an attack occurs.

CONCLUSION

DOS attacks are a serious threat that can cripple online services, causing significant disruption and financial losses. Implementing robust security measures and a comprehensive incident response plan are essential to mitigate these attacks effectively.

BIBLIOGRAPHY

Bikhana R., 2006, Auditors' Perception of the Implementation of the Code of Ethics of Indonesian Accountants in Improving the Objectivity of Public Accountants. S-1 Thesis. University of Muhammadiyah Yogyakarta. Yogyakarta.

Fakih. 2001, Gender Analysis and Social Transformation, Yogyakarta: Pustaka Siswa.

Gibson et al., 1996, Organisasi (Perilaku, Struktur, Proses), Jaklarta: Binarupa Aksara.

Hendris, A., 2005, Perception of Accountants and Students on the Advertency of Public Accountant Services, S-1 Thesis. University of Muhammadiyah Yogyakarta. Yogyakarta.

Ietje, N., 2005, Praktik Komputer Statistik, Yogyakarta: UPFE.

Ietje, N., 2006, Research Methods, Yogyakarta: UPFE.

Indiana, F.M. and Sri, S., 2006, Perception of Accountants, Accounting Students, and Employees of the Accounting Section Viewed from a Gender Perspective on Business Ethics and Professional Ethics, Papers of the IX National Symposium on Accounting (SNA), Padang: August 23-26.

Susanto. 2008. *Proses berpikir anak tunenetra dalam menyelesaikan masalah matematika*. Disertasi tidak diterbitkan. Surabaya: UNESA.