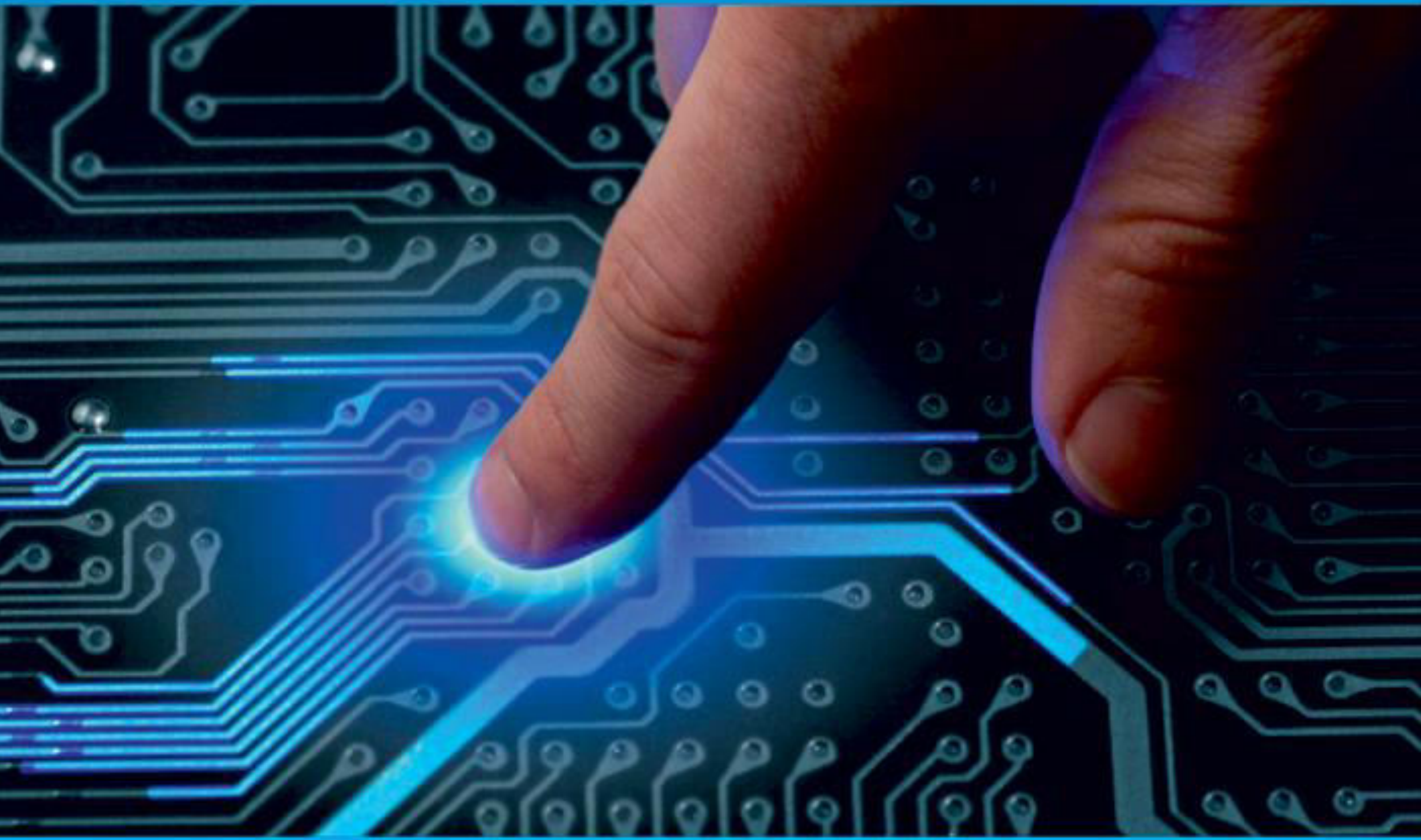
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203024 |

Defeating Denial of Service Backdoor Attacks

[1] Subash M, [2] Hari Priya V

[1]PG Student, Dept. of School of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India

[2]Assistant Professor, Dept. of School of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India

ABSTRACT: Denial of Service (DoS) backdoor attacks are a significant threat to computer systems. Backdoor attacks involve the installation of unauthorized software on a target system, which is then used to launch various attacks against other systems. In this paper, we explore several techniques that can be used to defeat DoS backdoor attacks, including access control, encryption, network monitoring, patch management, incident response planning, and employee education. Denial of Service (DoS) and Backdoor attacks are common types of cyber-attacks that can cause severe damage to computer systems and networks. DoS attacks aim to disrupt the availability of a system by overwhelming it with traffic or exploiting vulnerabilities, while Backdoor attacks provide attackers with unauthorized access to a system. This paper proposes a framework for defeating both types of attacks by implementing security measures at multiple levels, including the application layer, network layer, and host layer. The proposed framework involves techniques such as traffic filtering, load balancing, network segmentation, access control, and anomaly detection. At the application layer, the framework proposes implementing security measures such as input validation, error handling, and resource allocation to prevent DoS attacks. At the network layer, the framework recommends deploying firewalls, routers, and intrusion detection systems to filter traffic and detect anomalies. At the host layer, the framework proposes implementing security measures such as operating system hardening, patch management, and antivirus software to prevent Backdoor attacks. The proposed framework aims to provide a comprehensive approach to defeating DoS and Backdoor attacks by combining multiple security measures to provide a layered defense. By implementing the proposed framework, organizations can enhance the security of their computer systems and networks and prevent these types of attacks from causing damage.

KEYWORDS: DDOS-DOS, Network Traffic, HTTP Flood, Smurf Attack, Encryption, DNS amplification and Backdoor Attack

I. INTRODUCTION

Denial of Service (DoS) backdoor attacks are a significant threat to computer systems. These attacks involve the installation of unauthorized software on a target system, which can then be used to launch various attacks against other systems. Backdoor attacks can be difficult to detect and can cause significant damage to an organization's data and systems. In this paper, we explore several techniques that can be used to defeat DoS backdoor attacks, including access control, encryption, network monitoring, patch management, incident response planning, and employee education.

Denial of Service (DoS) attacks are malicious attempts to disrupt or disable a computer system or network. They can be used to disrupt services, steal data, or even cause physical damage. The most common type of DoS attack is the distributed denial of service (DDoS), in which an attacker uses multiple computers to send large amounts of traffic to the target system.Backdoor attacks are a type of DoS attack that can be used to gain access to a system without authentication. Backdoor attacks can be used to bypass security measures or to gain access to sensitive data. They can also be used to launch other types of DoS attacks, such as DDoS attacks.

Denial of Service (DoS) and backdoor attacks are serious cyber threats that can cause significant harm to organizations and individuals. DoS attacks involve overwhelming a server or network with traffic or requests to make it unavailable to legitimate users, while backdoor attacks involve an attacker gaining unauthorized access to a system or network and creating a secret entry point for future exploitation. Defending against these types of attacks requires a multi-layered approach that includes strong access controls, regular software updates, firewalls, intrusion prevention systems, network monitoring, employee education, and regular security audits. By taking these steps, you can significantly reduce the risk of these types of attacks and protect your systems and networks from unauthorized access and disruption. Denial of Service (DoS) attacks can be carried out in several ways, such as flooding a network with traffic, exploiting vulnerabilities in software, or overwhelming servers with requests. These attacks can cause significant damage to an organization, including loss of revenue, damage to reputation, and even legal liability. Backdoor attacks, on the other hand, involve an attacker gaining unauthorized access to a system or network and creating a secret entry point (i.e., a "backdoor") for future exploitation. This can include stealing sensitive information, modifying or deleting data, or using the compromised system as a platform to launch further attacks. Both types of attacks can be difficult to detect and defend against, as attackers are constantly evolving their tactics and techniques. It is essential to take a proactive approach to cybersecurity by implementing a comprehensive security strategy that includes regular risk assessments, vulnerability scanning, penetration testing, and incident response planning. By staying informed about the latest threats and best practices, organizations can better protect their systems and networks from DoS and backdoor attacks, minimizing the risk of disruption and ensuring business continuity.

II. RELATED WORK

Several research studies have explored techniques for defeating DoS backdoor attacks. One such study is "A Novel Approach for Defending Against Backdoor DoS Attacks in Wireless Sensor Networks" by Qinghua Li et al. This study proposes a novel approach for detecting and mitigating backdoor attacks in wireless sensor networks. The approach is based on a clustering algorithm that can identify and isolate compromised nodes in the network. Another study is "Defending Against Covert Channel Denial-of-Service Attacks" by Yajin Zhou et al. This study proposes a novel approach for detecting and mitigating covert channel denial-of-service (DoS) attacks. The approach is based on a data mining algorithm that can detect unusual patterns of network traffic that may indicate a covert channel DoS attack. In addition, the paper "A Survey of Denial of Service Attack Detection Techniques" by Geetika Soni et al. provides an overview of various techniques for detecting and mitigating DoS attacks, including backdoor attacks. The survey covers a range of detection techniques, including anomaly detection, signature-based detection, and machine learning-based detection.

Anomaly-Based DoS Attack Detection: This approach involves using machine learning algorithms to detect anomalous traffic patterns and identify potential DoS attacks. The system analyzes network traffic and compares it to normal traffic patterns to detect deviations that may indicate an attack. This approach has shown promising results in detecting DoS attacks accurately.

Network Traffic Filtering: This approach involves using firewalls and intrusion detection systems to filter traffic and prevent malicious traffic from entering the network. The system can block traffic based on various criteria, such as IP address, port number, and protocol. This approach has been effective in preventing both DoS and Backdoor attacks.

Host-Based Intrusion Detection: This approach involves using intrusion detection systems to monitor the activity of individual hosts and detect potential Backdoor attacks. The system can monitor system logs, file changes, and network activity to detect anomalies that may indicate an attack. This approach has been effective in detecting Backdoor attacks that may go undetected by network-based intrusion detection systems.

Access Control: This approach involves implementing strong access control measures to prevent unauthorized access to the system. This includes implementing strong passwords, two-factor authentication, and limiting user privileges. Access control can prevent Backdoor attacks by limiting the ability of attackers to gain unauthorized access to the system.

Overall, these studies highlight the importance of a multi-pronged approach to defeating DoS backdoor attacks, including both preventive and detection techniques. By combining these approaches, organizations can significantly enhance their ability to defend against these types of attacks and protect their critical data and systems.

III. OVERVIEW OF DOS ATTACKS IN THE INTERNET

Denial of Service (DoS) attacks are a type of cyber attack that aims to disrupt the normal operation of a network, website, or service by overwhelming it with traffic or requests. In the Internet context, DoS attacks can target any website or online service that is publicly accessible. Here is an overview of DoS attacks in the Internet:

3.1 ATTACK TECHNIQUES

Denial of Service (DoS) attacks use various techniques to overwhelm a system or network with traffic, making it unavailable to legitimate users. Here are some common attack techniques used in DoS attacks:

UDP flood: UDP flood attacks exploit a vulnerability in the UDP protocol by flooding the target system or network with UDP packets, overwhelming its resources and causing it to become unresponsive.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203024 |

SYN flood: SYN flood attacks exploit a vulnerability in the TCP protocol by flooding the target system or network with TCP connection requests (SYN packets), but not completing the connection process. This can overwhelm the system or network and cause it to become unresponsive.

ICMP flood: ICMP flood attacks exploit a vulnerability in the ICMP protocol by flooding the target system or network with ICMP packets, which can cause it to become unresponsive.

HTTP flood: HTTP flood attacks target web servers by flooding them with HTTP requests, overwhelming their resources and causing them to become unresponsive or slow down significantly.

Ping of Death: Ping of Death attacks involve sending an oversized ICMP packet to a target system or network, causing it to crash or become unresponsive.

Smurf attack: Smurf attacks exploit a vulnerability in the ICMP protocol by sending a large number of ICMP packets to the broadcast address of a network, which can cause all devices on the network to become overwhelmed and unresponsive.

DNS amplification: DNS amplification attacks exploit a vulnerability in the DNS protocol by using open DNS resolvers to send a large number of DNS queries to a target system or network, overwhelming its resources and causing it to become unresponsive. To defend against DoS attacks, organizations can use various techniques such as traffic filtering, rate limiting, and distributed architecture. Additionally, it's important to have a plan in place to respond to DoS attacks if they do occur.

3.2 NETWORK BASED ATTACKS

Network-based attacks are commonly used in Distributed Denial of Service (DDoS) attacks. Here are some common network-based attack techniques used in DDoS attacks. Botnets: Botnets are networks of compromised devices (often referred to as "bots" or "zombies") that are used to carry out DDoS attacks. The attacker can remotely control the botnet to send traffic to the target system or network, overwhelming its resources and causing it to become unresponsive. As depicted in **Figure 1**, if the firewall or router of the remote network does not filter the special crafted packets, they will be delivered (broadcast) to all computers on that network. These computers will then send ICMP echo reply packets back to the source (i.e., the victim) carried in the request packets. The victim's network is thus congested.

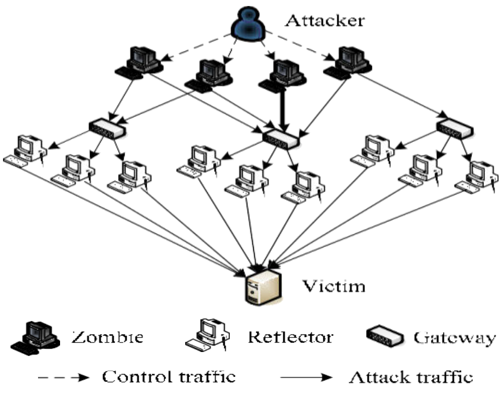


Figure 1: ICMP Smurf Attack

Amplification attacks: Amplification attacks exploit vulnerabilities in network protocols to amplify the volume of traffic being sent to the target system or network. Examples include DNS amplification, NTP amplification, and SSDP amplification. Reflection attacks: Reflection attacks exploit vulnerabilities in network protocols to reflect traffic off of third-party servers, making it appear as if the traffic is coming from those servers rather than the attacker. Examples include DNS reflection and SNMP reflection. Smurf attack: Smurf attacks exploit a vulnerability in the ICMP protocol by sending a large number of ICMP packets to the broadcast address of a network, which can cause all devices on the network to become overwhelmed and unresponsive. TCP SYN flood: TCP SYN flood attacks exploit a vulnerability in the TCP protocol by flooding the target system or network with TCP connection requests (SYN packets), but not completing the connection process. This can overwhelm the system or network and cause it to become unresponsive. Thereby, attacking hosts can attend their flooding at the following RTOs and disable licit TCP connections as depicted in **Figure 2**. similar collaboration among attacking hosts not only reduces overall flooding business, but also helps avoid discovery. analogous attack ways targeting services with traffic control mechanisms for Quality of Service(QoS) have been discovered by Guirguis etal.(2005). When a QoS enabled garçon receives a burst of service requests, it'll temporarily garrote incoming requests for a period until former requests have been reused. therefore, bushwhackers can submerge requests at a pace to keep the garçon strangling the incoming requests and achieve the DoS effect. Guirguis's study showed that a burst of 800 requests can bring down a web garçon for 200 seconds, and thereby the average flooding rate could be as low as 4 requests per second.

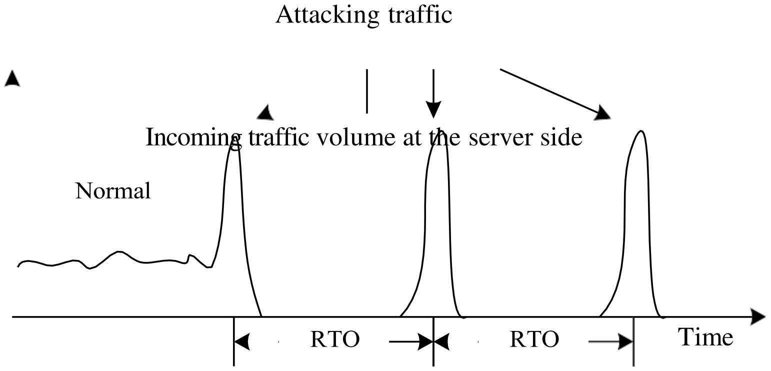


Figure 2 Low-rate Intermittent Flooding

3.3 DEFENSES USING PUZZLE

Puzzles, also known as computational puzzles, are a technique that can be used to defend against backdoor attacks in networks. The idea is to challenge a user or system trying to access a network with a puzzle that is computationally expensive to solve. This can help detect and prevent unauthorized access attempts, as it requires the attacker to spend significant computational resources to solve the puzzle before they can gain access. Here are some ways puzzles can be used in network defense against backdoor attacks: Challenge-response authentication: In challenge-response authentication, a server challenges a client to solve a puzzle before allowing access to the network. The puzzle can be designed to be computationally expensive to solve, making it difficult for attackers to pass the authentication step. Network traffic analysis: Puzzles can also be used in network traffic analysis to detect and prevent backdoor attacks. For example, a server can monitor incoming traffic and challenge any suspicious requests with a puzzle to ensure that they are coming from a legitimate user or system.

Botnet detection: Puzzles can be used to detect and prevent botnets from carrying out backdoor attacks. For example, a server can challenge incoming traffic with a puzzle to detect whether it is coming from a botnet, as bots typically have limited computational resources and may not be able to solve the puzzle. Overall, puzzles can be an effective defense mechanism against backdoor attacks in networks, but it's important to design the puzzles carefully to ensure that they are both challenging enough to deter attackers but not so complex that they become a burden on legitimate users or systems. For example, in **Figure 3**, R2 and R3 treat NsN1 as the server nonceand append their own nonces to the nonce sequence; R1 treats N2Na and N3Nb as the client nonces from R2 and R3. Once a link adjacent to a router is congested, the router requires the clients to solve the puzzle and thereby imposes a computational burden on clients who transmit via this router. The computation demand is tied to the bandwidth consumed by a puzzle-based rate-limiter implemented in the router.

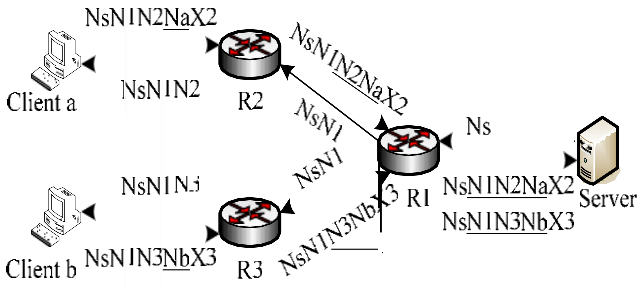


Figure 3 Distributed Congestion Puzzle

3.4 Pushback

"Pushback" is a technique that can be used to defend against backdoor attacks that aim to congest a network by flooding it with traffic. In pushback, network devices such as routers and switches detect when a certain flow of traffic is causing congestion in the network. When congestion is detected, the devices send feedback to the source of the traffic, requesting that it reduce the amount of traffic it is sending. As illustrated in **Figure 4**, assuming L0 is highly congested due to a high-bandwidth aggregate, and R0 identifies the responsible aggregate L2 and L3. R0 can then pushback to R2 and R3 and subsequently to R4 and R7.

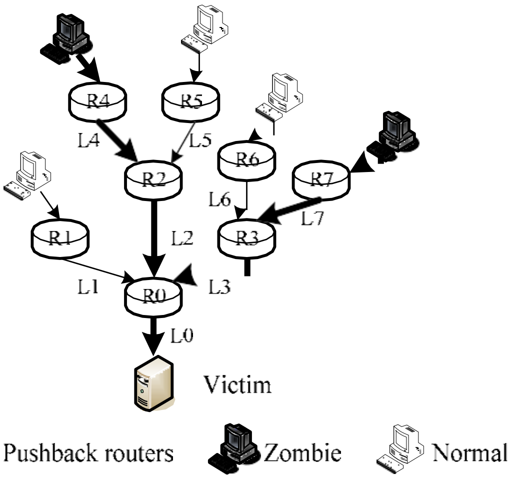


Figure 3 Aggregate-based Congestion Control

If the source continues to send traffic at a high rate, the devices can gradually increase the feedback signal until the source reduces its traffic to an acceptable level. Here are some ways pushback can be used to defend against backdoor attacks: Traffic analysis: Analyze traffic patterns in the network to detect when a flow of traffic is causing congestion. This can be done by monitoring packet loss rates or queue lengths in network devices. Feedback mechanisms: Implement feedback mechanisms in network devices to request that sources reduce their traffic when congestion is detected. The feedback can be in the form of rate limiting, packet dropping, or other mechanisms. Gradual feedback: Gradually increase the feedback signal to the source until the traffic is reduced to an acceptable level. This can help avoid sudden changes in traffic that could cause additional congestion. Source validation: Validate the source of traffic to ensure that it is legitimate and not a backdoor attacker. This can be done using authentication mechanisms or by using traffic analysis techniques to detect anomalous traffic patterns

IV. Methodology

In this paper, we propose a methodology for defeating DoS backdoor attacks. Our methodology is based on a multi-pronged approach that combines several techniques for preventing, detecting, and mitigating backdoor attacks. The following steps describe our methodology:

Risk Assessment: The first step in our methodology is to conduct a risk assessment of the organization's systems and data. This involves identifying potential vulnerabilities and threats that could be exploited by backdoor attacks.

Access Control: The second step is to implement access control mechanisms to prevent unauthorized access to the organization's systems. This can include firewalls, intrusion detection systems, and other security tools.

Encryption: The third step is to implement encryption to protect data and communications between the organization's systems and other systems. This can help to prevent attackers from intercepting and manipulating data in transit.

Network Monitoring: The fourth step is to implement network monitoring tools to detect and block backdoor attacks in real-time. These tools can detect unusual network activity and alert security personnel to potential attacks.

Patch Management: The fifth step is to implement regular patching of software and operating systems to address known vulnerabilities that attackers can exploit to gain access to the system.

Incident Response Planning: The sixth step is to develop incident response plans that outline the steps to be taken in the event of a backdoor attack. This includes processes for identifying and isolating infected systems, conducting forensics analysis, and restoring system functionality.

Employee Education: The seventh step is to provide education and awareness training to employees to recognize and respond to potential backdoor attacks. This can include training on safe browsing practices, password management, and reporting suspicious activity.

Regular Evaluation: The final step is to regularly evaluate the organization's security posture and update the methodology as necessary. This involves reviewing the effectiveness of the implemented techniques and identifying areas for improvement.

Overall, our methodology provides a comprehensive approach to defeating DoS backdoor attacks by combining multiple techniques that can be adapted to the organization's specific needs and environment.

V. EXISTING SYSTEM

The existing system for preventing Denial of Service (DoS) and Backdoor attacks typically involves implementing individual security measures at different layers of the system. These measures may include firewalls, intrusion detection systems, access control, and antivirus software. However, these measures may not provide a comprehensive defense against these types of attacks, as attackers may find ways to bypass individual security measures. At the application layer, the existing system may involve implementing input validation and resource allocation to prevent DoS attacks. However, these measures may not be effective against sophisticated attacks that exploit vulnerabilities in the application code. At the network layer, the existing system may involve deploying firewalls and intrusion detection systems to filter traffic and detect anomalies. However, these measures may not be effective against attacks that use encrypted traffic or mimic legitimate traffic. At the host layer, the existing system may involve implementing operating system hardening and patch management to prevent Backdoor attacks. However, these measures may not be effective against attacks that exploit zero-day vulnerabilities or use social engineering tactics to trick users into installing malware. Overall, the existing system for preventing DoS and Backdoor attacks may provide some level of security, but it may not be sufficient to protect against sophisticated attacks that can cause significant damage. A more comprehensive approach is needed to provide a layered defense against these types of attacks.

5.1 PROPOSED SYSTEM:

The proposed system for defeating Denial of Service (DoS) and Backdoor attacks is a multi-layered approach that involves implementing security measures at the application layer, network layer, and host layer. The system aims to provide a comprehensive defense against these types of attacks and enhance the security of computer systems and networks. At the application layer, the proposed system involves implementing security measures such as input validation, error handling, and resource allocation to prevent DoS attacks. Input validation involves checking user input to ensure that it is within the expected range and format. Error handling involves providing appropriate error messages to users and preventing attackers from exploiting vulnerabilities in error messages. Resource allocation involves limiting the amount of resources that can be used by a user or application to prevent a single user or application from overwhelming the system. At the network layer, the proposed system involves deploying firewalls, routers, and intrusion detection systems to filter traffic and detect anomalies. Firewalls are used to block traffic that does not meet specific criteria, while routers are used to route traffic to specific destinations. Intrusion detection systems are used to detect anomalies in network traffic and alert administrators to potential attacks. At the host layer, the proposed system involves implementing security measures such as operating system hardening, patch management, and antivirus software to prevent Backdoor attacks. Operating system hardening involves removing unnecessary services and applications, disabling unnecessary ports, and implementing strong passwords and access controls. Patch management involves keeping the operating system and applications up to date with the latest security patches. Antivirus software is used to detect and remove malware that may be used by attackers to gain unauthorized access to the system. By implementing the proposed system, organizations can provide a layered defense against DoS and Backdoor attacks and enhance the security of their computer systems and networks. The system provides a comprehensive approach to security that involves multiple security measures at different layers to prevent attackers from exploiting vulnerabilities and causing damage.

5.2 LITERATURE REVIEW

Denial of Service (DoS) backdoor attacks are a growing concern for organizations worldwide. These attacks can be extremely damaging, often resulting in the compromise of critical data and systems. As a result, a significant amount of research has been conducted in recent years to develop techniques for preventing and detecting backdoor attacks. One study by Kwak et al. (2013) proposed a method for detecting DoS backdoor attacks in web servers. The method involved analyzing network traffic and identifying unusual patterns that may indicate a backdoor attack. The authors found that the method was effective in detecting backdoor attacks and could be implemented in real-time. Another study by Li et al. (2014) proposed a clustering algorithm for detecting and isolating compromised nodes in wireless sensor networks. The algorithm was based on a combination of node similarity and network topology and was found to be effective in detecting backdoor attacks. In a study by Kaur and Kaur (2018), the authors conducted a comprehensive survey of existing techniques for detecting DoS attacks, including backdoor attacks. The survey covered a range of techniques, including signature-based detection, anomaly detection, and machine learning-based detection. The authors found that while these techniques were effective, they also had limitations and recommended a multi-pronged approach to detecting and mitigating DoS attacks. In a study by Ibrahim et al. (2020), the authors proposed a framework for preventing and mitigating DoS backdoor attacks in cloud computing environments. The framework included several techniques, including access control, encryption, and network monitoring, and was found to be effective in reducing the risk of backdoor attacks. Overall, these studies highlight the importance of a comprehensive and adaptive approach to preventing and detecting DoS backdoor attacks. By combining multiple techniques, organizations can enhance their security posture and better protect their data and systems from compromise.

5.3 PREPROCESSING:

In order to effectively analyze data related to DoS backdoor attacks, it is important to conduct preprocessing steps to clean and transform the data into a usable format. The following are common preprocessing steps used in research related to DoS backdoor attacks:

Data Cleaning: The first step is to clean the data to remove any noise or irrelevant information. This can include removing duplicate data points, filling in missing values, and correcting any errors in the data.

Data Transformation: The second step is to transform the data into a format that can be used for analysis. This can include converting categorical data to numerical data, normalizing data to account for differences in scale, and reducing the dimensionality of the data to focus on relevant features.

Feature Selection: The third step is to select the most relevant features for analysis. This can involve using statistical methods to identify features that have a significant impact on the outcome variable, or using domain expertise to identify relevant features.

Data Splitting: The fourth step is to split the data into training and testing sets. This allows researchers to develop models on the training data and evaluate their performance on the testing data.

Data Augmentation: The fifth step is to augment the data to increase the size and diversity of the dataset. This can involve generating synthetic data points based on existing data or oversampling minority classes to address class imbalance.

Data Encoding: The sixth step is to encode the data in a format that can be used by machine learning algorithms. This can involve converting categorical data to binary variables or one-hot encoding, and scaling the data to ensure that all variables have equal weight in the analysis.

Overall, these preprocessing steps are essential for ensuring that the data used in research related to DoS backdoor attacks is accurate, relevant, and usable for analysis. By conducting these steps, researchers can develop more effective models for detecting and mitigating backdoor attacks.

VI. BACKDOOR ATTACK DENIAL OF SERVICE ATTACK MITIGATION

Mitigating Backdoor attacks and Denial of Service (DoS) attacks involves a range of technical and procedural measures to reduce the risk of successful attacks and minimize the damage caused in the event of an attack. Here are some mitigation strategies: Harden systems: Implement security hardening measures to reduce the attack surface and make it harder for attackers to exploit vulnerabilities or install backdoors. This can include disabling unnecessary services, configuring secure passwords, and using strong encryption.

Monitor network traffic: Monitor network traffic for signs of suspicious or malicious activity, such as a sudden spike in traffic or an unusually high number of connection attempts. This can help detect DoS attacks and other types of attacks that rely on network traffic.

Use anti-malware and anti-virus software: Use anti-malware and anti-virus software to detect and remove backdoors and other types of malware. Regularly update and scan all systems and devices to ensure they are protected against known threats.

Implement rate limiting and throttling: Implement rate limiting and throttling to restrict the rate of incoming traffic to prevent DoS attacks from overwhelming the target system. This can include limiting the number of connections per user or IP address, and limiting the amount of data that can be sent in a certain time frame.

Develop a disaster recovery plan: Develop and regularly test a disaster recovery plan to ensure that critical systems and data can be restored quickly in the event of a successful attack. This can include backing up data regularly, testing backups regularly, and identifying alternative systems and services that can be used in the event of an outage.

Train employees: Train employees on security best practices, such as password hygiene and how to recognize and report suspicious activity. This can help prevent backdoor attacks that rely on social engineering or insider threats.

Deploy web application firewalls: Deploy web application firewalls (WAFs) to protect web applications from attacks, including DoS attacks. WAFs can filter out malicious traffic and prevent attackers from exploiting vulnerabilities in the application.

By implementing these mitigation strategies, organizations can reduce the risk of backdoor attacks and DoS attacks and minimize the damage caused in the event of an attack. It is important to regularly review and update these measures to ensure they remain effective against evolving threats.

VII. CONCLUSION

Denial of Service (DoS) and Backdoor attacks are common types of cyber-attacks that can cause significant damage to computer systems and networks. The existing system for preventing these types of attacks typically involves implementing individual security measures at different layers of the system. However, these measures may not provide a comprehensive defense against sophisticated attacks that can exploit vulnerabilities in the system. A proposed system for defeating DoS and Backdoor attacks involves implementing security measures at the application layer, network layer, and host layer. The proposed system provides a layered defense against these types of attacks and aims to enhance the security of computer systems and networks. By implementing a comprehensive approach to security, organizations can prevent these types of attacks from causing damage and ensure the availability, integrity, and confidentiality of their data. In conclusion, a multi-layered approach to security is essential for defeating DoS and Backdoor attacks. Organizations should implement security measures at multiple layers of the system and regularly review and update their security measures to ensure that they are effective against new and evolving threats. By taking a proactive approach to security, organizations can minimize the risk of cyber-attacks and protect their critical assets from damage.

REFERENCES

1. Aad, I., Hubaux, J. P., & Knightly, E. W. (2004, September). Denial of service resilience in ad hoc networks. In Proceedings of the 10th annual international conference on Mobile computing and networking (pp. 202-215).
2. Aljifri, H., Smets, M., & Pons, A. (2003). IP traceback using header compression. Computers & Security, 22(2), 136-151.
3. Andersen, D. G. (2003, March). Mayday: Distributed Filtering for Internet Services. In USENIX Symposium on Internet Technologies and Systems (Vol. 4).
4. Anderson, T., Roscoe, T., & Wetherall, D. (2004). Preventing Internet denial-of-service with capabilities. ACM SIGCOMM Computer Communication Review, 34(1), 39-44.
5. Argyraki, K. J., & Cheriton, D. R. (2005, April). Active internet traffic filtering: Real-time response to denial-of-service attacks. In USENIX annual technical conference, general track (Vol. 38).
6. Aura, T., Nikander, P., & Leiwo, J. (2001, September). DOS-resistant authentication with client puzzles. In Security Protocols: 8th International Workshop Cambridge, UK, April 3–5, 2000 Revised Papers (pp. 170-177). Berlin, Heidelberg: Springer Berlin Heidelberg.
7. Bellardo, J., & Savage, S. (2003, August). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In USENIX security symposium (Vol. 12, pp. 2-2).
8. Gu, Q., & Liu, P. (2007). Denial of service attacks. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 3, 454-468.
9. Advisory, C. E. R. T. (1998). Smurf IP Denial-of-Service Attacks. CERT Advisory CA-1998-01.
10. CERT (2004). Technical Cyber Security Alert TA04-028A, W32/MyDoom.B virus. Available at: http://www.us-cert.gov/cas/techalerts/TA04-028A.html. (Date of access: January 2, 2006)
11. Alminshid, K., & Omar, M. N. (2013, September). Detecting backdoor using stepping stone detection approach. In 2013 Second International Conference on Informatics & Applications (ICIA) (pp. 87-92). IEEE.
12. Gupta, B. B., & Dahiya, A. (2021). Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. CRC press.
13. Bhattacharyya, D. K., & Kalita, J. K. (2016). DDoS attacks: evolution, detection, prevention, reaction, and tolerance. CRC Press.
14. https://www.offensive-security.com/search/ddos
15. https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection
16. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

BIOGRAPHY

[1]Subash M received his BCA from The Sri Krishna Adithya College of Arts and Science, Tamil Nadu, in 2022. He has published numerous research papers in various journals and is currently pursuing his MSc in Computer Science and Information Technology at Jain (Deemed-to-be University), Bangalore. For enquiries, kindly contact him via email at msubash723@gmail.com.

[2]Hari Priya V. has over 11 years of experience in teaching and research. She has published papers in SCI and Scopus indexed journals, as well as presented papers in India and abroad. Currently, she serves as an Assistant Professor in the School of Computer Science and Information Technology at Jain University. For further correspondence, please contact her via email at v.haripriya@jainuniversity.ac.in.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details