Distributed Denial of Service Network Attacks

India Henry

Cybersecurity

CYSE250

Old Dominion University

Abstract

Distributed denial of service (DDoS) attacks are a huge threat to computer networks. Denial of service attacks are aimed at shutting down networks and the resources that rely on them, such as computers, routers, switches, gateways, firewalls and more. DDoS attacks require defense measures that evolve over time as these attacks also evolve with time. There are many techniques to mediate DDoS attacks from a networking level which starts with the application layer and works up to detecting when those attacks occur. With those mediation techniques, comes challenges ranging from the sophistication or diversity of the attack to the size of the attack.

Key Words: Distributed Denial of Service (DDoS), Application Layer, Port-Scanning, Network Resources, Distributed Denial of Service as a Service (DDoSaaS), Local Area Network (LAN), Wide Area Network (WAN), Software-Defined Networking (SDN)

Introduction:

Historically, distributed denial of service attacks have come from hackers focusing their attacks on the physical network, directing an influx of bots trying to access a singular network to a singular router or even computer. As technology has evolved, these attacks have become more sophisticated. DDoS attacks have become bigger to take on more defended network layers, they have become more focused, they have even evolved to look like the attack came from the local network. With the evolution of DDoS attacks, new mitigation techniques, and challenges to those techniques, have arisen.

Distributed Denial of Service Network Attacks:

Distributed denial of service (DDoS) attacks are malicious cyberattacks used to disrupt the traffic of a normal network by overloading it (Lau, 2024); in other words “zombies target the victim and deny services to legitimate users by inundating a network with

requests" (Aljuhani, 2021). These attacks have become much more sophisticated than when they first came to be, as DDoS attacks can now infect any device connected to a targeted local area network (LAN), or any devices that come in contact with the network or device operating on the network. Over time, these attacks have gone from infecting only a few devices to being large enough to take down entire companies. DDoS attacks do not need to be direct anymore, they can spread through phishing attacks that target someone on a server, if that person so much as opens the infected message the entire network can be compromised.

Impact on Network Resources:

Firewalls are used to protect networks and the physical technology that works within those networks. Firewalls are meant to allow or deny protocols and certain IP addresses. Firewalls are entirely necessary but cannot be the only measure deployed to protect a network. DDoS attacks have become more sophisticated and overwhelming over time, and because of that firewalls can be overloaded and effectively shut down if they are overwhelmed enough (Bhosale, 2018).

Once a DDoS attack is successful, if it infiltrates a network, any resource on that network is rendered compromised. DDoS attacks are like worms that spread malware from network to network, computer to computer, not allowing for any resource connected to that network to communicate with other technology without spreading the virus, or any outside resource to connect with anything impacted by the attack effectively.

Techniques to Mitigate DDoS Attacks:

As technology has evolved, DDoS attacks have evolved with them. With that, new mitigation techniques have arisen to try to ensure the safety of networks, individuals, and companies. One technique is the different ML techniques that are used to learn and identify certain patterns. This technique helps to sift out attackers from regular users. The machine learning algorithms go through a series of tests that help it recognize when a packet contains malware or not. If the system detects a DDoS attack in a

packet, it will remove the packet and update the filter policy for new traffic (Aljuhani, 2021).

In an experiment, intrusion detection and prevention systems (IDPS) using software defined networking (SDN) is experimented with to help reduce DDoS and port scanning attacks. The conclusion to this experiment suggests that features in SDNs are able to detect and prevent intrusions that instantaneously drop packets when they are found to be malicious (Birkinshaw, 2019). This experiment is huge because SDNs are used in many places and can be used to manage networks. This would mean that as long as SDNs are used properly, there is a possibility that they themselves can deter DDoS attacks. SDNs are also flexible and easy to manage, which makes it easy for them to become one of the most used and reliable techniques for mitigating attacks.

Another technique that could be used is to implement a series of algorithms that help to detect and mitigate DDoS attacks.

1. Access Control: when a host makes a request, its address is checked for presence in the blocked list and then the decision is taken whether to allow the request or not.
2. Signature IDS Using Naive Bayes We Use: Naive Bayes classifier to classify the incoming requests as anomaly or normal; based on the obtained values the users sending anomaly requests are sent a warning.
3. Signature IDS Using KNN: Use KNN classifier to classify the incoming requests as anomaly or normal; based on obtained values the users sending anomaly requests are sent a warning.

These techniques, amongst others, are used so the controller keeps an access control list, checks the MAC addresses of each packet, and detects if malware is present thus expelling it from the program (Barki, 2016). In *Detection of distributed denial of service attacks in software defined networks,* it focuses on the programming and network aspects related to DDoS attacks.

Challenges in Mediation Techniques

ML techniques are only as good as the techniques they have time to learn. While there is a way for that technique to detect the characteristics of a DDoS attack, with how advanced DDoS attacks are becoming, there is always the possibility that there could be an attack that doesn't follow the "rules" of a standard DDoS attack. This would mean the attack would fly below the radar and be effective on the network.

SDN can be used to mitigate DDoS attacks as it allows the network to be managed through a logical and centralized control function that provides instructions on how to filter network traffic. "However, the centralized control feature could potentially be a liability as it becomes a single point of failure risk due to the high dependency of the network on it" (Aladaileh, 2020). This would make SDNs the target of many DDoS attacks, as if that is the only thing a network is relying on, if the attacker can take down the SDN they have successfully infiltrated the network.

Implementing algorithms is not a failsafe way to deter DDoS attacks. With new algorithms comes trouble with the possibility of holes or hackers that try to exploit the functions of those algorithms. Other than the possibility of hackers infiltrating these defense programs, there runs the problems of these programs becoming obsolete. Technology progresses at a fast rate to the point where once programs are implemented, bugs and holes can be found at an accelerated rate or new technology renders the "improved" obsolete.

There are also two major application layer DDoS attacks as laid out in *The distributed denial of service attacks (DDoS) prevention mechanisms on application layer*. These attacks target specific characteristics by overloading the systems with the volume of the attack.

1. Reflection/Amplification based flooding attacks: uses an influx of fake IPs to generate DNS responses
2. HTTP flooding attacks: these attacks are broken up into three different types: session flooding attack, request flooding attacks, and asymmetric attacks. These

attacks are designed to take over a server's resources (CPU, bandwidth, memory, etc.) and render it unavailable to actual users.

Something new would be the concept of denial of service as a service (DDoSaaS) attacks. These attacks are denial of service attacks that use a number of powerful servers to send a larger amount of attack traffic to a specific target. These attacks are so major because it doesn't take much money to start one, but it could cause businesses millions of dollars (Aljuhani, 2021).

Conclusion

DDoS attacks are major attacks on networks that impact the network's resources in a way that can render them useless. The findings in this paper show just how vital network protection is to not only companies but also to ordinary people. Once DDoS attacks infiltrate a network, they can spread to the network's devices, rendering them useless.

There are techniques to mitigate DDoS attacks; however, there are drawbacks to every solution. The biggest point is to constantly evolve and pad the security of your technology because as technology evolves, holes can be found and exploited.

References

Aladaileh, M. A. (2020, August 3). *Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller - A Review*. Wikipedia. Retrieved April 22, 2024, from https://ieeexplore.ieee.org/abstract/document/9154703

Aljuhani, A. (2021, March 1). *Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments*. Wikipedia.

Retrieved April 22, 2024, from https://ieeexplore.ieee.org/abstract/document/9366480

Barki, L. (2016, November 3). *Detection of distributed denial of service attacks in software defined networks*. IEEE Xplore. Retrieved April 22, 2024, from https://ieeexplore.ieee.org/abstract/document/7732445?casa_token=WYz1unIFvP4AAAAA:4PUXdEjYXealo9r8eWaxrn1yRc6Jp2Imya1QBPPyggqOMWa1nCp7cnB_itHsHzX66eAH5Dp57Q

Bhosale, K. S. (2018, January 4). *The distributed denial of service attacks (DDoS) prevention mechanisms on application layer*. Wikipedia. Retrieved April 22, 2024, from https://ieeexplore.ieee.org/abstract/document/8246247

Birkinshaw, C. (2019, March 22). *Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks*. Wikipedia. Retrieved April 22, 2024, from https://www.sciencedirect.com/science/article/abs/pii/S1084804519301109

Lau, F. (2024, March 5). *Distributed denial of service attacks*. IEEE Xplore. Retrieved April 22, 2024, from https://ieeexplore.ieee.org/abstract/document/886455