DDoS Assignment 2.2

Keegan Heaton

Security Essentials

09/17/2023

DDoS attacks are well known to be one of the most malicious and hard-to-predict network attacks today. DDoS, otherwise known as Distributed Denial of Service, is a kind of remote network attack that restricts the use of a service and keeps any users from accessing the effected applications. DDoS attacks can be launched against any susceptible website and target the compromised system by flooding the networks with requests, effectively overwhelming the server and crashing it soon after. With a 31% increase in attacks from 2020 to 2021(CompTIA, n.d.), DDoS attacks pose a significant threat to small businesses and can cause large corporations to lose millions in just an hour. In February 2020, Amazon Web Services (AWS) suffered a DDoS attack so sophisticated that it kept their incident response teams occupied for several days. Amazon not only lost millions due to the attack, but it also affected customers worldwide, keeping them from using Amazon services.

(CompTIA, n.d.)

In 2020 alone, DDoS attacks over 100GB/s in volume have grown almost tenfold, as shown in the blue circle. Additionally, the average attack size from DoS and DDoS attacks grew to 500 Mbps, making attacks of this size the standard in today's world. DDoS Attacks are also becoming the most common, growing by 154% in the 2020-2021 dataset according to ZDnet. With DDoS attacks getting more sophisticated and common, it's important to know the warning signs to help protect against them.

The first major red flag of a possible DDoS attack is unexplained spikes in web traffic. By monitoring the website server logs or using a web analytics tool, if there are sudden spikes in traffic from a small group of IP addresses or from a specific location it may indicate that the website's server is in the beginning stages of the attack. In the beginning stages, using geo-blocking or IP address filtering would temporarily reduce the DDoS threat while resources are being gathered and a DDoS expert should be kept up to speed on any possible error codes or server malfunctions.

Another significant red flag of a possible DDoS attack is slow loading times. If the website is loading incredibly slowly, then it may be due to the website's server being flooded with requests. As requests begin to accumulate, the website will become more and more inoperable. At best, contacting the ISP, the Internet Service Provider, could help temporarily with the request congestion and advise on the next course of action. It's also important to call or contact a network administrator as slow loading times could be due to maintenance or an in-house network issue. If it's not sourced from the administrators, then mitigating the situation using rerouting practices would help stall time.

Unexplained errors or timeouts are other red flags to a DDoS attack. If the surge of requests is greater than what the server can handle, the site may start displaying error codes like HTTP 503 unavailable. At this stage, the server has nearly met capacity. If IP filtering and geo-blocking have become ineffective, the next step would be to migrate the customer traffic to another IP address. This will temporarily stop the server from being overwhelmed and hopefully isolate the traffic coming from the attacker's IP addresses.

As described, these signs happen in the beginning to mid stages of a DDoS attack. If an attack progresses to the advanced stage where services become completely inaccessible, it may be necessary to shut down the server, and a DDoS expert should be consulted to guide the defense against the attack. The DDoS experts should always be the first resource used in a DDoS attack and any signs of a DDoS attack, from web traffic spikes to unexplained error codes should be evaluated by a DDoS expert. These experts will have quality insight and possible solutions to stop the attack before a complete server shutdown happens. However, this is after a network administrator has clearly stated that the server isn't under maintenance and an in-house issue has been ruled out. Once a DDoS expert is connected, the next step to blocking a DDoS attack would be to upgrade any firewall and configure it to restrict any traffic coming and going from the affected systems. Additionally, adding multiple layers of firewalls and DoS protections will help filter unreasonable requests and reduce the strain on the network. Once the proper protections have been applied, creating an Attack Threat Model will help identify attackers, which attack vectors are being used, and the level of risk this DDoS attack puts the network in. Then, forensic and security teams can help recover the network and find points of access, infection, and any changes to the system that the attackers could’ve introduced.

Conclusively, DDoS attacks are a significant threat in today's interconnected world. Recognizing the warning signs, like unexplained traffic spikes, slow loading times, and error codes, is crucial for intervention and as little damage as possible. While beginning-stage measures like geo-blocking and IP filtering can provide temporary solutions, it's essential to involve DDoS experts when signs of an attack emerge. After which, a team can be created to efficiently recover and restore any damages done during the attack.

Citations

CompTIA. (n.d.). What Is a DDoS Attack and How Does It Work | Cybersecurity | CompTIA. Retrieved from https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works

Gopalan, V. (2023, April 25). 15 Best Practices for DDoS Protection | Indusface Blog. Retrieved from https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks/#:~:text=A%20Web%20Application%20Firewall%20(WAF,block%20vulnerabilities%20in%20the%20application.

Kimachia, K. (2023, July 7). How To Tell If You've Been DDoSed: 5 Signs of a DDoS Attack. Retrieved from https://www.esecurityplanet.com/networks/how-can-you-tell-if-youve-been-ddosed/

Kime, C. (2022, December 1). How to Stop DDoS Attacks | eSecurity Planet. Retrieved from https://www.esecurityplanet.com/networks/how-to-stop-ddos-attacks-tips-for-fighting-ddos-attacks/

Organization, C. (2021, February 1). Understanding Denial-of-Service Attacks | CISA. Retrieved from https://www.cisa.gov/news-events/news/understanding-denial-service-attacks