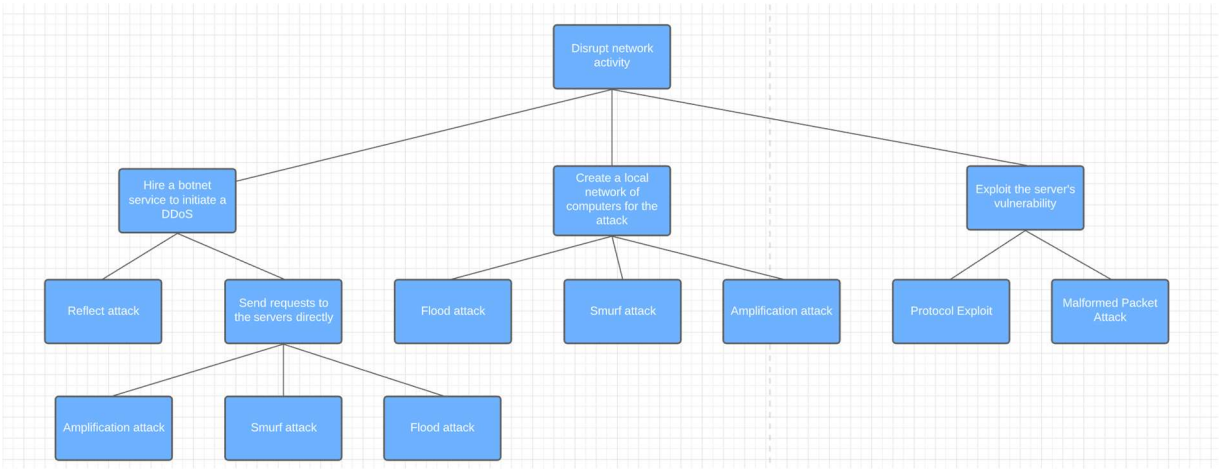
(Problem Domain is located on the next page)

Threat Model

For the threat model regarding DDoS attacks, I will be using the DREAD model to rank the threat of a DDoS attack. However, the challenge of ranking a DDoS attack is variable as the effects are dependent upon the quality and quantity of hardware being used by both parties.

When taking into account the effects of a DDoS attack, an attack tree was designed to list the different types of requests and packets a DDoS attack might use.



- Damage Potential – (2-3)
    - Damage potential is difficult to give a specific rating to because it depends on the intensity and duration of the attack. At best, network and server functionality will be halted.
    - A DDoS attack can also leave a server vulnerable to other attacks due to all processing power and attention being focused on the DDoS attack itself, leaving other potential vulnerabilities unchecked.
        - Once example is when multiple servers are experiencing a DDoS attack, they may become unsynchronized which would allow a malicious user to duplicate certain actions assuming the servers are not idempotent.
    - A DDoS attack can lead to a complete halt in operations which would lead to loss in revenue and reputation if the attack lasts for long periods of time.
        - One example is a popular game, Titanfall 1, which had to be removed from game stores indefinitely due to a DDoS attack that has lasted for over 2 years and persists to this day[1].
- Reproducibility-2
    - I gave reproducibility a rating of 2 because a DDoS attack is very simple to initiate en masse and is very simple for an attacker as long as the attacker has a method of reaching their target online.
    - The main challenge for the attacker is initiating an attack on a scale large enough to create noticeable performance degradation for a server.

[1] https://www.pcgamer.com/after-years-of-struggling-against-ddos-attacks-titanfall-is-being-removed-from-sale/

- Exploitability Cost-3
    - A rating of 4 was given to the exploitability because DDoS attacks in general are easy to implement as long as the attacker can make contact with the target server.
    - While DDoS attacks are normally not resource intensive for a malicious machine, a large number of computers must be acquired or a vulnerability found in a server must be exploited for a successful attack.
    - However, an attacker can simply hire a botnet service which fronts the cost of acquiring the hardware necessary for a large scale attack and leases these malicious network users for relatively low prices ranging at around a few thousand dollars[2].
- Affected Users – (2-3)
    - The rating was provided assuming that a DDoS attack was successful in disrupting network functionality. However, an attacker would have to launch a DDoS attack against the entire network, including a majority of a network's servers, to cause a noticeable impact for the end-user.
        - The larger scale a network becomes, the more difficult it becomes to disrupt the entire network.
        - The user, on the other hand, may not even notice this attack if redundancy and redirection is used to distribute the server load across the network unless the attacker manages to target every available server.
    - When a DDoS attack is successful, a server becomes unable to process every incoming request, eventually becoming unable to honor any requests given by legitimate users.
    - However, this affects only targeted servers. If a company's amount of usable servers outnumber the set of the attacker's targeted servers, then the company will be able to continue its operation, albeit with reduced functionality and efficiency.
    - In addition, some servers may be more capable of handling large numbers of requests if they require the server to process simple tasks.
    - Servers may also share some of its tasks through redundancy, meaning that another server can take over a downed server's tasks if necessary. This would allow multiple servers to mitigate the effects of a DDoS attack.
        - An example of this would be the Nov. 1, 2015 Root DNS Event which proved to be ineffective due to the DNS servers being designed to handle large amounts of simple queries[3].
- Discoverability – 1
    - A DDoS attack has no intention of being stealthy as the goal is to create enough noise on a server's network to disrupt the network.
    - Network engineers and cybersecurity professionals will have access to performance readings of their company's networks which allows them to identify spikes in activity and server performance which will allow them to hypothesize a timeframe of a DDoS attack.

[2] Namestnikov, The economics of botnets

[3] Moura, Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event

- Users affected by DDoS attacks will share and report a server's accessibility, allowing them to quickly figure out if a network is unusable which will most likely be reported to the targeted company.
- The only DDoS attack that goes unnoticed is a failed DDoS attack.

As a result, the DREAD model lists DDoS's threat rating to be between 8 and 10 which would be considered to be of medium threat level. The difficulty in assessing a DDoS attack's effectiveness comes primarily from the attacker's pool of resources, what other methods the attacker can use alongside the attack, and how well a server can process and resist such attacks. It can be assumed that as a network grows in scale and complexity, it becomes more difficult and costly for an attacker to effectively take down compared to smaller networks.

Problem Domain

DDoS attacks can be considered one of the most widespread attacks in cybersecurity due to the attack being simple to execute and effective against establishments that are unwilling or unable to acquire the necessary hardware and/or software to resist such attacks. Attackers can simply use botnet services to launch a large-scale attack that, if effective, can either be used to halt all activity to that server or leave a server vulnerable to other potential threats due to having to sacrifice its processing power and attention against an overload of requests which could be difficult to discern from an ordinary user or a hijacked machine being told to continually spam requests to the server. One difficult challenge that service providers face is how to differentiate between a user and a malicious attacker as either party would be using the same requests and queries to the server for different purposes. In these scenarios, I would also like to describe the attack methods initiated by an attacker that masquerades their botnets as overloaded network traffic and how server owners are able to detect and reduce the impact of these DDoS attacks, if they are capable of doing so.

Sources:

A. Sardana and J. R.C., "An Integrated Honeypot Framework for Proactive Detection, Characterization and Redirection of DDoS Attacks at ISP Level," *Journal of Information Assurance and Security 1,* vol. 1, no. 1, pp. 1-15, 2008.

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.580.3346&rep=rep1&type=pdf

G. C. Moura, R. D. O. Schmidt, J. Heidemann, W. B. D. Vried, M. Muller, L. Wei and C. Hesselman, "Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event," Association for Computing Machinery, New York, 2016.

https://dl.acm.org/doi/pdf/10.1145/2987443.2987446

R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS Attack & its Effect in Cloud Environment," *ScienceDirect,* vol. 49, pp. 202-210, 2015.

https://www.sciencedirect.com/science/article/pii/S1877050915007541

S. Yu, W. Zhou and R. Doss, "Information theory based detection against network behavior mimicking DDoS attacks," in *IEEE Communications Letters*, vol. 12, no. 4, pp. 318-321, April 2008, doi: 10.1109/LCOMM.2008.072049.

https://ieeexplore.ieee.org/abstract/document/4489680

Y. Namestinikov, "The economics of botnets," Kaspersky, Moscow, 2009.

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2009/07/01121538/ynam_botnets_0907_en.pdf