**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>

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>