Agenda

- Distributed Denial of Service Attack
What is a DDoS attack

- A denial-of-service (DoS) attack is intended to render any type of service inaccessible. For example, shutting down access to an external-facing online asset like an ecommerce site constitutes a denial-of-service.
- A distributed denial-of-service (DDoS) is when the same result is achieved but initiated from multiple connected devices.
- The main intention behind DoS or DDoS attacks is to make a service unavailable and cause havoc rather than trying to breach the security perimeter of the target.
The dog ate our website.

Ok, ok, ok we know that's not an excuse. We'll have it back up-and-running for you shortly.

DNS resolution error

You've requested a page on a website (www.yelp.com) that is on the CloudFlare network. CloudFlare is currently unable to resolve your requested domain (www.yelp.com). There are two potential causes of this:

Most likely: if the owner just signed up for CloudFlare it can take a few minutes for the website's information to be distributed to our global network.

Less likely: something is wrong with this site's configuration. Usually this happens when accounts have been signed up with a partner organization (e.g., a hosting provider) and the provider's DNS fails.

Ray ID: 2a401d9e480225af
Your IP address: 208.117.11.6
Requested URL: www.yelp.com/

image source: thousandeyes.com
Some other recent DDoS incidents

- DDoS attack on DNS root servers, June, 2016
- Dyn DNS outage, October, 2016 (Dyn: a DNS provider)
Types of DDoS attack

- Volumetric attacks - a.k.a. volume based attack.
- Protocol attacks - a.k.a. Layer four DDoS attack.
- Application attacks - a.k.a. Layer seven DDoS attack.
Volumetric Attacks

- What is it? - Attacks that use massive amount of traffic saturating the bandwidth of the target. Volumetric attacks are easy to generate by employing simple amplification techniques.
- Examples: NTP amplification, DNS amplification, UDP flood, TCP flood.
Example: a DNS-based volumetric reflection attack

image source: thousandeyes.com
Example: a DNS-based volumetric reflection attack

▶ Attackers often issue a special type of DNS request called an ANY request. ANY requests ask the DNS resolver for ALL information that it currently knows about the domain which may include where the mail servers are (MX records), what the IP addresses are (A records) and so on. The responses, which are much larger than the request, amplify the amount of bandwidth sent to the victim.

▶ Run this command to send a ANY request to DNS server, and view all the records types. # dig -t ANY boisestate.edu
In NTP Amplification attacks the perpetrator exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted server with User Datagram Protocol (UDP) traffic. In an NTP amplification attack, the query-to-response ratio is anywhere between 1:20 and 1:200 or more. This means that any attacker that obtains a list of open NTP servers (e.g., by using tool like Metasploit or data from the Open NTP Project) can easily generate a devastating high-bandwidth, high-volume DDoS attack.
The OSI 7 Layer Model

image source: infosecinstitute.com

To remember: Please Do Not Teach Students Pointless Acronyms, or All Presidents Say They Never Did Pot
Protocol Attacks

- **What is it?** - Attacks that render a target in-accessible by exploiting a weakness in the Layer 3 and Layer 4 protocol stack.
- **Examples:** Syn Flood
- **The recent Dyn outage,** consisted of TCP Syn floods targeting port 53 of Dyn’s DNS servers.
A SYN flood uses the inherent patience of the TCP stack to overwhelm a server by sending a flood of SYN packets and then ignoring the SYN ACKs returned by the server. This causes the server to use up resources waiting a configured amount of time for the anticipated ACK that should come from a legitimate client. Because web and application servers are limited in the number of concurrent TCP connections they can have open, if an attacker sends enough SYN packets to a server it can easily chew through the allowed number of TCP connections, thus preventing legitimate requests from being answered by the server.
Establish a Normal TCP Connection
SYN Flood

watch this: https://www.youtube.com/watch?v=cfoqQ8mHafM
Application Attacks

- What is it? - Attacks that exploit a weakness in the Layer 7 protocol stack. The most sophisticated of attacks and most challenging to identify/mitigate.
- Examples: HTTP Flood
In HTTP flood DDoS attack the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request.
Difference between the three types of DDoS attack

- Volumetric attacks - saturate network bandwidth.
- Protocol attacks - consume actual server resources, e.g., memory resource.
- Application attacks - comprised of seemingly legitimate and innocent requests.
A large portion of the material is adapted from:

- Fundamentals of Information Systems Security - David Kim, Michael G. Solomon