Module - 9
Denial of Service

Denial of Service (DoS) : It is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host.

Distributed Denial of Service (DDoS) : it is a Dos attack originating from multiple source in order to increase the effectiveness of the attack due to increase traffic volumes.

 # What makes DoS Attacks so effective ??
- They don't require specific software or infrastructure vulnerability
- Attacks can be executed at a very low cost.
- DDoS services are plentiful
- They can be mounted using a variety of Protocols and attack techniques
- They can be very difficult to trace back to an origin and a perpetrator

 # Motivation :

1. DDoS in Gaming :
- Gaming Service :
  - Appeals to attackers seeking notoriety
  - The "Grinch" Syndrome; Attackers are antogonists
  - Gaming is emotive and amplifies frustation
- Gaming Oppo nent :
  - Increase with the growth of online games
  - Introduce additional latency to gameplay
  - May make it impossible to play

2. DDoS for Revenge :
3. DDoS in Law Enforcement
4. DDoS as a Diversion Technique
5. DDoS and Extortion
6. DDoS and Hacktivism

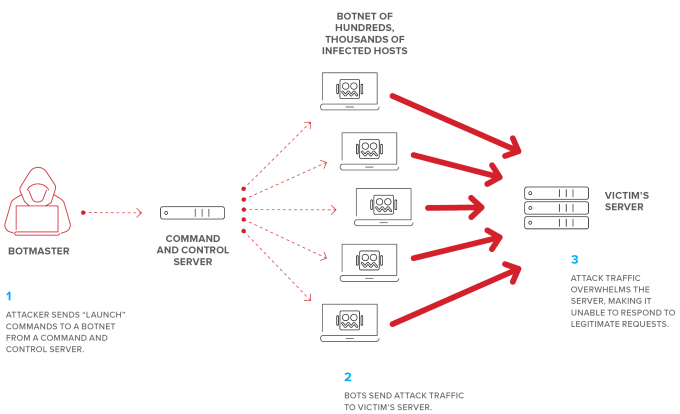
 # Unintentional DoS :

- A Sudden influx of legitimate traffic can have the same effect as a coordinated DoS Attack
- We see this in scenarios such as **"the slashdot effect" ******
- it's often driven by major events that drive organic traffic to the site
- It can also be caused by inadvertant traffic

 # Impact of Denial of Service Attacks :

- Loss of Business
- Reputation Damage
- Financial Impact

 # Role of Botnets in DDoS Attacks :



 # Attack Techniques :

1. HTTP Flood Attacks :

- They are “Volumetric” attacks - they are normal HTTP requests
  can saturate web server resources (“service request floods”)
  can saturate bandwidth (“bandwidth attack”)
- Attack effectiveness can be amplified via certain app features
  Anything using a slow hashing function
  Requests that results in SMTP connections
  Long-running requests such as executing a report (may overload the database)
  Download large files to flood the bandwidth
- requests can adhere to legitimate patterns which makes defence difficult

 # Variation of HTTP Flood Attacks

- can be GET or POST (app or HTTP overhead is more important)
- can be HTTP or HTTPs
- Can mimic legitimate Traffic
  - User Agent
  - Referrer
  - Cookies
  - “Organic” request body parameter
- can force loading from the origin in order to prevent laoding of site from web cache or CDN
  - make a request with the random data so they it is not present in cache

2. Syn-Flood Attacks

Attacker sends the SYN flags only and then the server send SYN/ACK and then server wait to get ACK from the attacker … but the attacker don’t send ACK flag
Another form is
SYNchronize(Spoofed Source IP address) : This form is used to make more **anonymity**

3. UDP and ICMP Attacks :

UDP (User datagram Protocol) :

- Floods random ports on the target
- The Target consumes resources responding with **“destination unreacheable”** packets… and. This response creates an overhead
- No Initial handshake means the spoofed ip address for more anonymization

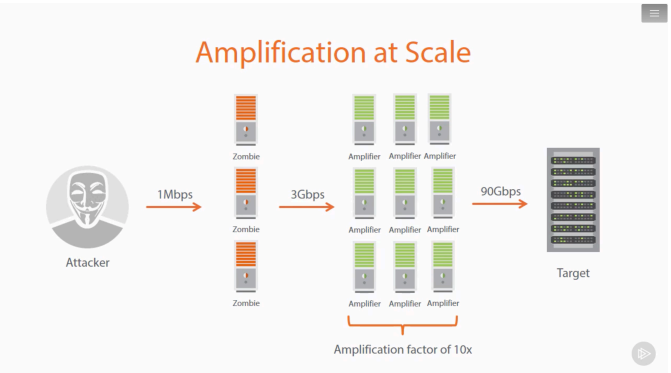
ICMP (Internet Common mail protocol) :

- Supports utilites such as ping using “Echo Request” and “Echo Reply”
- Source IP in a ping can be forged to create a **“smurf attack”**
- Can be used to send a **“ping of death”**, a large packet causing a buffer overflow

4. DNS Amplification Attack :

Sometime it is also known as **DNS Reflection.**

In this attacker Send the small Query and in Response DNS Server has to Respond large Data.



 # Other Form of Amplification Attacks :

(a) SNMP (Simple Network Management Protocol) :
Can Amplify by a factor of **650x**
but very few open on the web today
(b) NTP (Network Time Protocol) :
Can return a large result via the monlist command
monlist command : this return the address of up to the last 600 machines that the NTP server interacted with.
Amplification Factor can be up to **206x**
(c) SSDP (Simple Service Discovery Protocol) :
It is used for the advertisement and discovery of the network services
Attackers query home devices with uPnP service enabled
Response are larger Than the incoming request.

5. Peer-to-Peer Attacks :

Bugs in **DC++**, the free and open source peer to peer file sharing client. Attcker exploit the vulnerability and become the **puppet master** similer to a bot herder but in this we don't have any zombie machine we have legitimate peer to peer user. Now the attacker connects to the peer and by exploiting that weakness in the system then instruct the client to disconnect from the peer to peer network and start sending request to the target machine.

6. Slowloris :

Slowloris is an attack referred to as "slow" and "low" attack tool
uses a low volume of traffic to generate slow rate
Sends HTTP requests without a termination sequence
Causes website to leave the connection open
Resources are allocated to wait for the termination sequence
Can originate from the single origin
Partial requests are sent and then reset and then reset

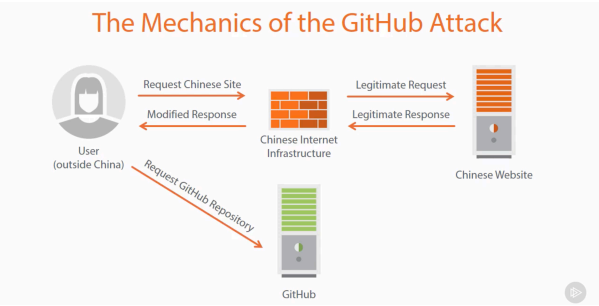
7. Permanent and DoS and Phlashing :

A PDoS attacks render a device unusable, usually by replacing the firmware with a malicious variants
Phlashing would be the method by which we update firmware on a device
It's also frequently referred to as "bricking"
It exploit the weakness in the target device

8. Github's "Man on the side" DDoS Attacks :

In march 2015, Github suffered a significant DDoS Attacks
It targets two Github Repositories :
GreatFire.org : Monitores Chinese Internet Censorship
cn-nytimes - Chinese New York Times
These are mirror sites which makes it hard for censors
Chinese infrastructure MITM'd request to Baidu analytics and substitued them with attacks scripts against GitHub

-> The Mechanics of the Github Attacks :



 # Incapsula Client's DDoS Attacks :

- SYN flood Attack of 30gbps (no amplification)
- HTTP Flood of 10M requests per seconds targeting resources heavy pages
- Targeted attack against APIs (not protectable via Javascript challenges)
- Attackers adds new bots capable of persisting cookies between requests
- The Bot was meant to transparently open the browers windows
- They identified the botnet as "Cutwail" (a.k.a "PushDo")

 # Tools and Services Used in DoS Attacks :

1. LOIC : Perform DOS attack
2. JS LOIC : Javascript version of LOIC
3. HOIC : More powerfull version of LOIC and perform DDoS Attacks
4. Booters and Stressors : they are simply distributed denial of service as a service term

 # Defending Against Attacks :

Overview :
1. There are many different mechanisms for DoS defence
2. They Typically sit at layer 4 and Layer 7
3. A Robust defence strategy is multifaceted
4. Preparation before *attack* is key

 # Defensive Consideration :

How quickly you can act ?
Do you have multiple defence type depending on the attack ?
Are you able to adapt as the attack does ?
Can you do all this without neglecting other security imperatives ?

 # Discovering the Attack Pattern :

What type of attack it is ??
    Layer 4 (UDP, TCP, ICMP)
    Layer 7 (HTTP)
Where is it coming from and what is it targeting ?
Are there any unique signatures ?
    Headers
    Target Resources
Establish intent - unintentional DDoS versus malicious DDoS

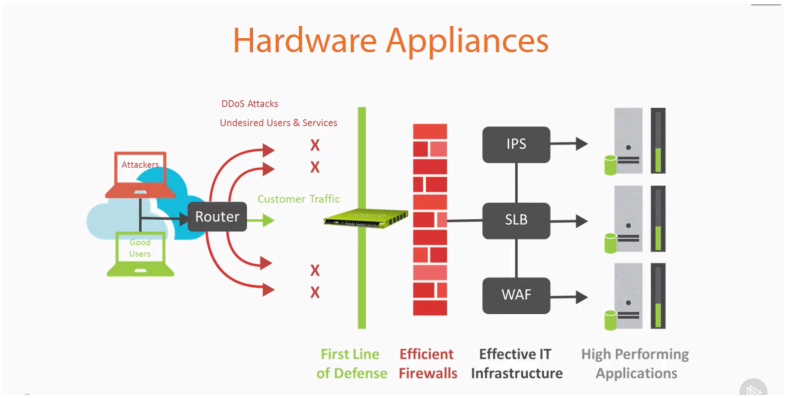
 # Absorbing the attack :

Pros :
    No Disruption for legitimate users
    Auto scale is simplified in the cloud era
    Scalling buys time to determine other countermeasures
Cons :
    can become very expensive
    may not be practically feasible for a large enough attack

 # Network Layer Defenses :

Layer - 4

- Hardware Appliances



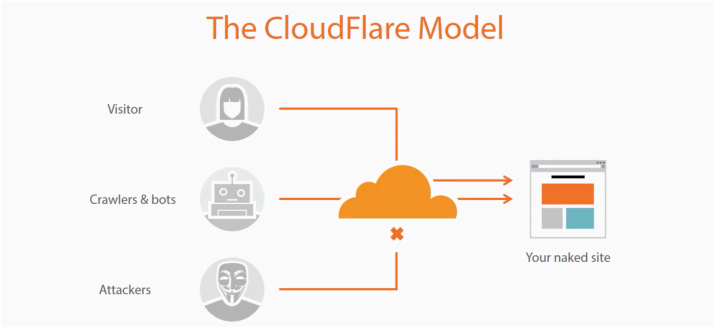
- Disable all unused ports
- Block unnecessary protocols (i.e. ICMP)
- Filtering ingress traffic
  Reputation based blocking
- Implement “blackholing” or “tarpitting”
  Terminate traffic upstream of the origin server
  no response is sent, the traffic just “disappears”
- But this only works if the network isn’t saturated with data….
- Anycast : It is a network addressing and routing methodology , You can stand up a single ip address and then depending on where the traffic originates from route it to nearest possible node.
- Block that anycast node from where the malcious data is originating

 # Application Level Defense :

Important when there’s not anomalous layer 4 traffic
Dedicated devices such as a web application firewall can inspect HTTP Traffic
  make sure they can also inspect HTTPS traffic
Minimizing the attack surface area
  Take anything that doesn’t have to be public off that network segment
  place them within a private subnet
Design the application for DDoS

 # DDoS Prevention as a service :

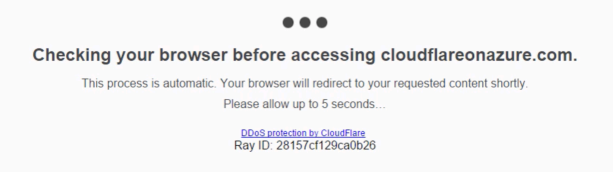
The CloudFlare Model



Q : How CloudFlare Responds :
They have 4 ways to deal with the incoming traffic

1. **Allow** : if the traffic is good let them Flow
2. **Challenge** : if they are not sure about the traffic then they will represent a captca page “I’m not a robot”
3. **Interstitial page** :

This page shows and now the cloudflare runs a bunch of javascript in the client and it’s looking to establish whether the client is actually a legitimate browser or whether it is a bot



4. **Block** : if it find the traffic is not legitimate then it will simply block the data

 # Preparing for DoS Resiliency :

Implement a DoS Strategy well in advance of an attack
    some defences can have long lead-time to implement
Defences are great, but do they actually work ??
    use legitimate stress test services !!
Do you have a Crisis management plan ?
    Have an incident response runbook prepared
Do you know what a successful DoS attack will actually cost you ??