DDoS

HW 7 - CNS Sapienza

Daniele Oriana 1457625

9 Dec 2016

General descryption of DDoS

Answer

DDoS stays for Distributed Denial of Service, it is a cyber attack which main purpose is to make a resource unavailable for any users (or machine) that requires it. This is done sending a lot of useless packets to the resource provider that, managing these packet, will not be able to serve all the others meaningfull requests for the resource. Usually the kind of packet that is sent to the resource provider is the SYN one, in fact this packet is used in the famous TCP Three Way Handshake Protocol to start a TCP connection; when the receiver achieved this packet, he starts to reserve some resources for the probably following connection, obviously sending a lot of these packets leads to a overload of the system that will be not able to serve other requests. The attacker sends these packets using different unique IP addresses, in the past we had the DoS attack, a sort of previous version of the DDoS attack in which the attacker had only few IP addresses to exploit in order to send packets, while now, with the growing of the number of devices connected to internet, the attacker has a lot of IP addresses to use in a DDoS attack as a sort of flood that starts from all these IP addresses all over the world and ends in the resource provider (the first D that stays for Distributed derived from this fact).
Besides the standard definition and description of the DDoS attack we can describe other two differentiations of this attack:

- An advanced persistent DoS (APDoS), in which actors are very skilled, with powerfull commercial grade computer resources and capicities. This kind of attack is aimed by explicit motivation (a calculated end game/goal target) and exploited by tactical execution.

- Denial-of-service as a service, in which some people provide so-called "booter" or "stresser" services, based on simple web-based front ends, and accept payment over the web. These services are marked as stress test tools, but selling these to unauthorized and, very often, not skilled people, can leads anyway to a powerfull DoS attack.

Example of DDoS

Answer

The increasing number of devices having an internet connection has led to the IoT (Internet of Things) infrastructure, in which a lot of devices can exchange information, evolve and, therefore, work (through a Machine to Machine mechanism) without the continously partecipation of a human (here you can find a small presentation that i have made for the course of Pervasive System about IoT and a tool to manage this kind of network with a small example of usage in a GitHub project: http://www.slideshare.net/DanieleOriana1/thingstudio-presentation). Analyzing these new infrastructures we can understand that they represents a huge potential fot DDoS attack. One of the most recent malware that exploit very well this potentiality is Mirai; it is able to transform informatic systems into botnets (an infrastructure over which the attacker has the completely control in order to use it for large scale attacks, such as DDoS). How does it works? Mirai propagates by bruteforcing telnet servers with a list of 62 insecure default credentials, so Mirai could technically infect anything upon successful login. After the successfull login the malware will attempt to kill and block anything running on ports 22, 23, and 80, essentially locking out the user from their own device and preventing infection by other malware. In this way the malware can create a botnet for a DDoS attack.
Mirai is very powerfull, in fact the 27 Nov 2016 it infects 900000 internet connections and devices in Germany, exploiting a vulnerbility in the routers of the Deutsche Telekom. Another example that can help us in understanding the power of Mirai is the case of the attack to the site of the journalist Brian Krebs , in which the malware created a botnet that guaranteed a flood traffic of 620 Gbps!!

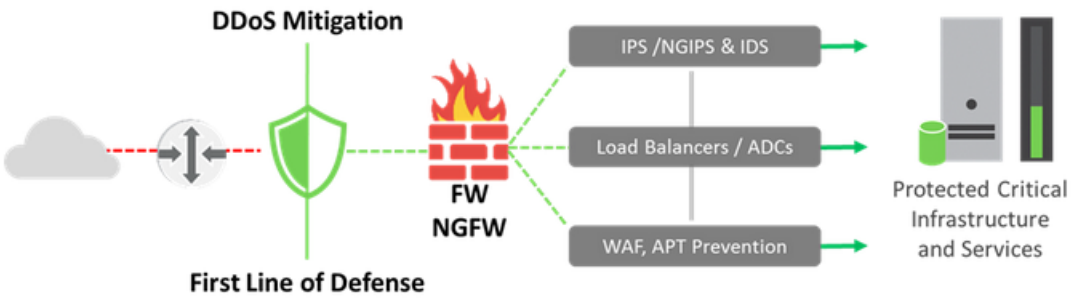

Figure 1: DDoS Mitigation configuration.

How firewall can help in protecting the network?

Answer

Firewalls are not designed with the purpose to defend against DDoS attacks, in fact we know that a firewall is a stateful device that configured to block undesired ports. But, ports 80, 53, 25 and 443 are always open because they are the entry points for desired services. The DDoS attacks exploits this fact occurring on these open ports and are therefore transparent to firewalls. Moreover, volumetric flood attacks exploit the stateful nature of the firewall by filling up the state tables with volumes of unwanted traffic, so that it has little time to pass legitimate traffic. So, as a conseguence of that, a possible solution could be to use a sort of bottleneck that can reduce the traffic of a possible DDoS attack, and then analyze the resulting traffic through the firewall. This bottleneck can be realized through a DDoS mitigation system deployed in-line and at the edge of the network, this system can conduct inspections of control traffic (network and application headers),determining whether there is a DDoS attack present or not, and instantaneously mitigate an attack at line rates of tens of Gbps. In conclusion we can say that the DDoS mitigation system is able to minimazing a DDoS attack and also to ensure the passing of good traffic.