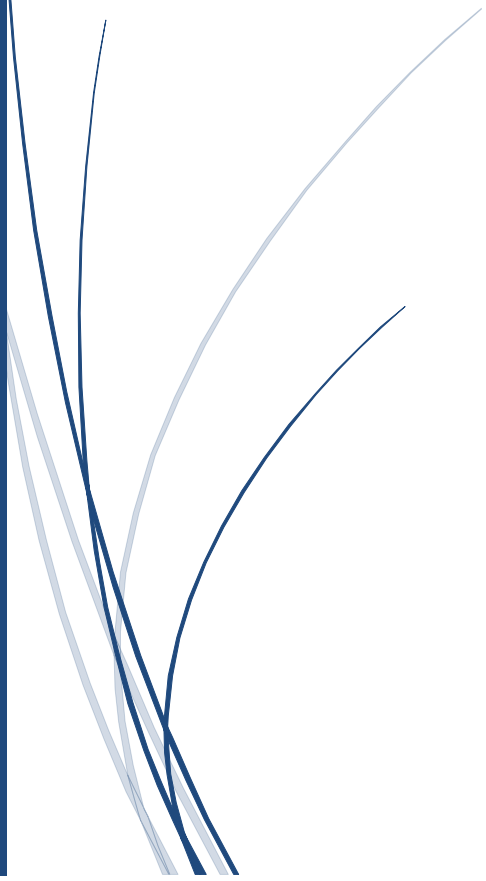
Chapter 10

Denial of Service

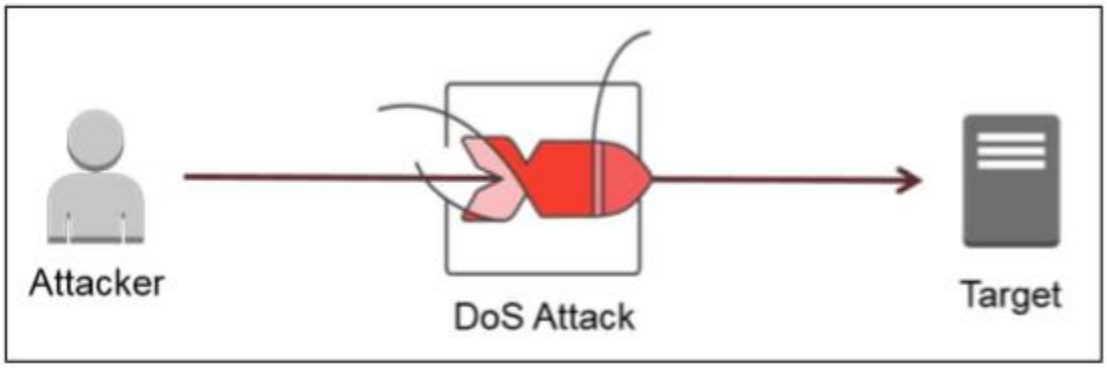
Theory



Ethical Hacking

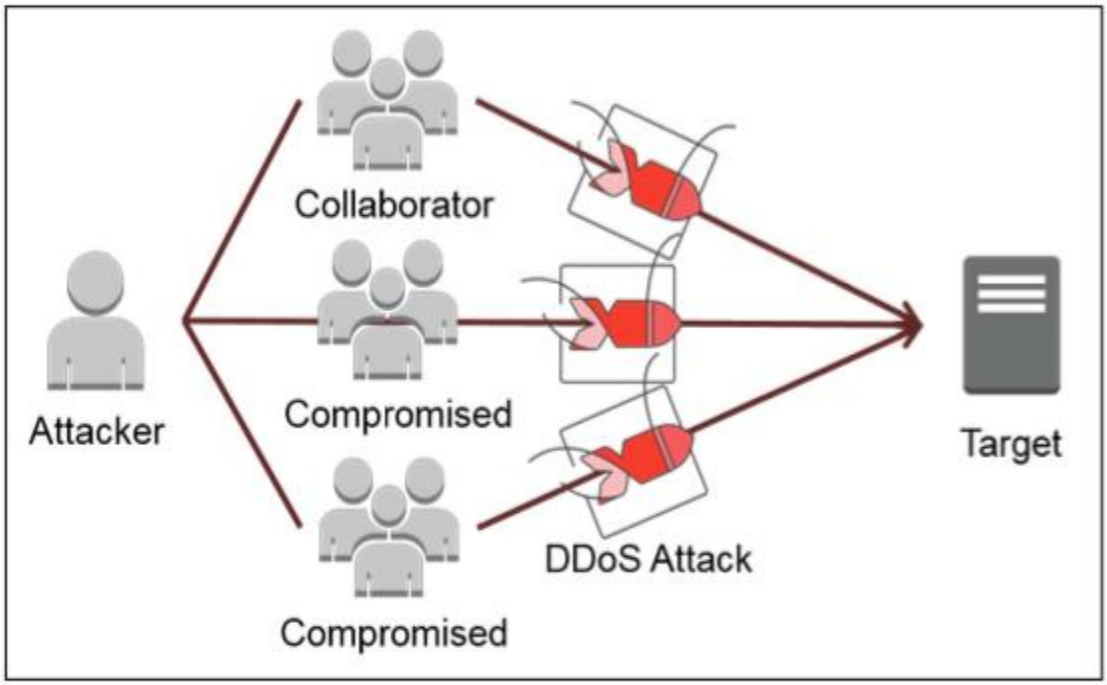
Denial of Service

a Denial of service (DoS) attack 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 connected to the Internet.



Distributed Denial Of service

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the targeted system with traffic to make the resources unavailable to its intended users, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the.



Botnet

A botnet is a collection of Internet-connected devices that are infected and controlled by a common type of malware each of which is running one or more bots. Infected machines are controlled remotely. Botnet infections are usually spread through malware, such as a trojan horse. Botnet malware is typically designed to automatically scan systems and devices for common vulnerabilities that haven't been patched. Botnet malware may also scan for ineffective or outdated security products, such as firewalls or antivirus software. Common tasks executed by botnets include:

- Using the machine's power to assist in distributed denial-of-service (DDoS).
- Generating spam emails.
- Internet traffic generation on a third-party website.
- Replacing banner ads in a web browser.

Exploiting System and Application Level Vulnerabilities

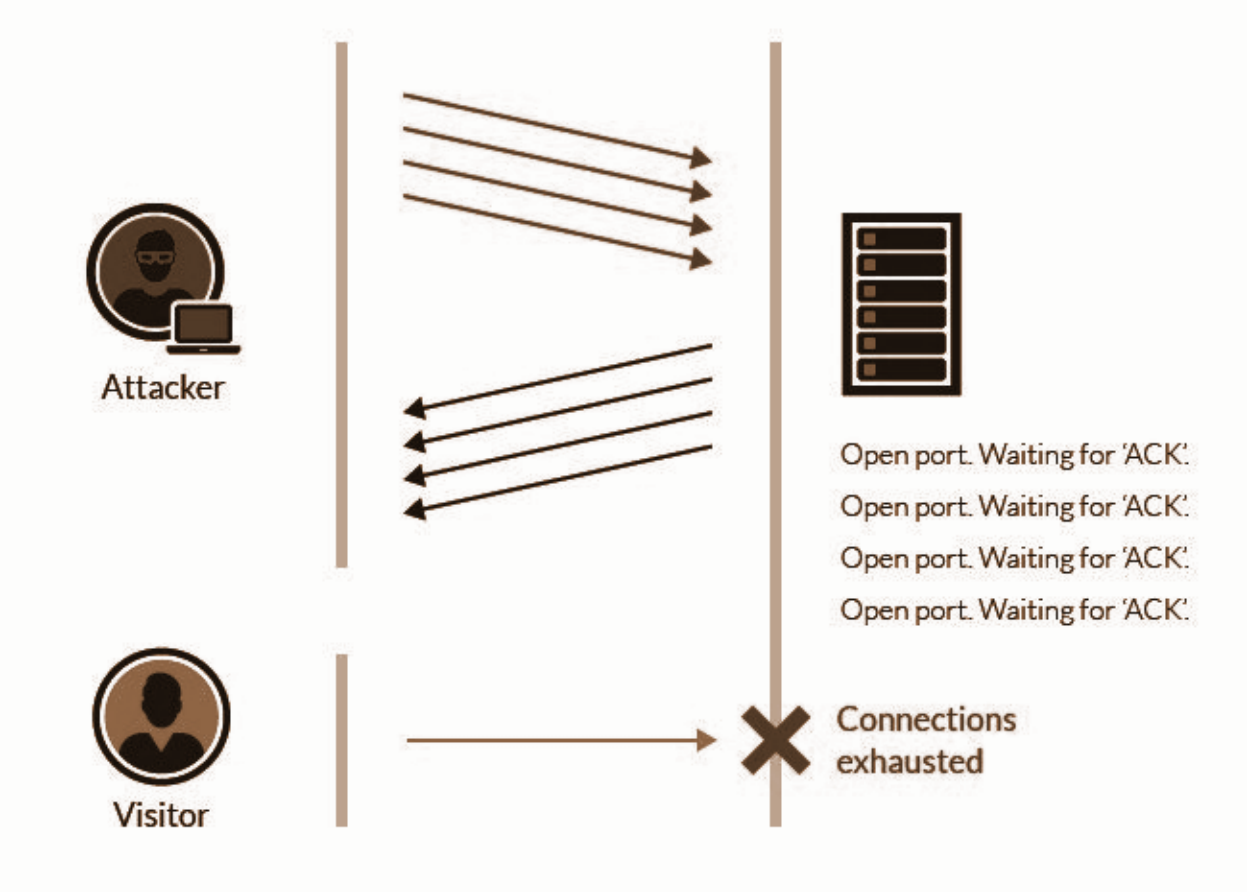
In this method, either the operating system or the application software will have bugs which will cause a denial of service situation. Once an attacker finds this vulnerability, he has to find out the working exploit code for the vulnerability, if an attacker finds the exploit code he can use it to DOS the target without any further problems.

TCP SYN Flood

TCP SYN flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive. With SYN flood DDoS, the attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, using a fake IP address. The server receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.

The attacker either does not send the expected ACK or if the IP address is spoofed never receives the SYN-ACK in the first place. Either way, the server under attack will wait for an acknowledgment for its SYN-ACK packet for some time. During this time, the server cannot close down the connection by sending RST packet, and the connection stays open. Before the connection can time out, another SYN packet will arrive. This leaves an increasingly large number of connections half-open



UDP Flood

UDP flood is a type of Denial of Service (DoS) attack in which the attacker sends a request to random ports on the targeted host with IP packets containing UDP datagrams.

The receiving host checks for applications associated with these datagrams and if no application is associated with the request, then it sends back a "Destination Unreachable" packet. As more and more UDP packets are received which need to be answered, the system becomes overwhelmed and unresponsive to other clients. The attacker may also spoof the IP address of the packets, both to make sure that the return ICMP packets do not reach their host, to anonymize the attack.

User Datagram Protocol (UDP) is a connectionless and session less networking protocol. Since UDP traffic does not require a three-way handshake like TCP, it runs with lower overhead and is ideal for traffic that does not need to be checked and rechecked, such as chat or VoIP.

In the absence of an initial handshake, to establish a valid connection, a high volume of traffic can be sent over UDP channels to any host, with no built-in

protection to limit the rate of the UDP DoS flood. This means that UDP flood attacks are highly-effective.

Some UDP flood attacks can take the form of DNS amplification attacks. Where UDP does not define specific packet formats, and thus attackers can create large packets fill them with junk text or numbers and send them out to the host under attack.

When the attacked host receives the garbage-filled UDP packets to a given port, it checks for the application listening at that port, which is associated with the packet's contents. When it observes that, no associated application is listening, it replies with an ICMP Destination Unreachable packet.

HTTP Flood

HTTP flood is a type of Distributed Denial of Service (DDoS) attack in which the attacker sends seemingly legitimate HTTP GET or POST requests to a target web server or application. HTTP client like a web browser communicates with application or server; it sends an HTTP request. A GET request is used to retrieve content while POST requests are used to send dynamically generated content.

The attack is effective when it forces the server or application to allocate the maximum resources possible in response to every single request. For this reason, HTTP flood attacks using POST requests tend to be the most resource effective. POST requests may include parameters that trigger complex server-side processing. On the other hand, HTTP GET based attacks are simple to perform.

Ping of Death

In this method of DOS, the attacker will try to send the large-sized ping packets which the target cannot handle which will cause DOS situation on the target device.

MAC Flooding

The Network switch maintains a table called CAM (content addressable memory) to prevent MITM attacks, but it contains a limited number of entries, so when an attacker tries to overload this CAM table with more number of mac addresses than it can handle, sometimes the switch may not be responding to the legitimate requests.

Other types of Flooding

An attacker can use any other protocol vulnerabilities to flood packets to the target device so that the target device will be busy with handling Flood packets and may not respond to the original request made by the legitimate user.

Countermeasures

- DoS detection techniques are based on identifying and discriminating the illegitimate traffic from legitimate packet traffic
- Set up Systems with limited security (Honeypots), to attract an attacker
- FortGuard Anti-DDoS Firewall provides a fundamentally superior approach to mitigating DDoS attacks, with a design that focuses on passing legitimate traffic rather than discarding attack traffic.

References:

1. DoS and DDoS attack image reference: What is DoS and DDoS Attack. (2017, September 12). Retrieved from https://www.jsys.co/denial-of-service-dos-and-distributed-denial-of-service-ddos-attacks/
2. TCP SYN flood image reference: (n.d.). Retrieved from https://www.incapsula.com/ddos/attack-glossary/syn-flood.html
3. UDP flood: (n.d.). Retrieved from https://www.incapsula.com/ddos/attack-glossary/udp-flood.html
4. HTTP flood: (n.d.). Retrieved from https://www.incapsula.com/ddos/attack-glossary/http-flood.html