Practical-2

Aim: - The MGTech assurance Pvt. Ltd. company has appointed you as server administrator. Your task is to ensure the server is always available to process the client request. Also identify the threats to availability of server. Prepare a detailed document for the said task with below topic detailed study.

Types of DOS

1) **Volume-based Attacks**

   UDP floods: These attacks send a large number of User Datagram Protocol (UDP) packets to the target system, which must process each packet even if it doesn't contain any data.

   ICMP floods: Similar to UDP floods, but use Internet Control Message Protocol (ICMP) packets, such as ping requests.

   SYN floods: These attacks exploit the three-way handshake process used in TCP connections by sending a large number of SYN (synchronization) packets without completing the handshake, leaving the target system waiting for non-existent return packets and consuming resources.

2) **Protocol Attacks:** These attacks exploit vulnerabilities in the network protocols used by the target system to disrupt its normal operation. Common types of protocol attacks include:
   Smurf attacks: These attacks send spoofed ICMP packets to a large number of broadcast addresses, amplifying the attack traffic and overloading the target system
   Ping of Death: These attacks send oversized ICMP packets that can crash or reboot the target system.
   Teardrop attacks: These attacks send fragmented IP packets in a specific order that can cause the target system to crash.
3) **Application-layer attacks:** These attacks target specific vulnerabilities in web applications or services to disrupt their operation. Common types of application-layer attacks include:
   HTTP floods: These attacks send a large number of HTTP requests to the target server, overwhelming its resources and preventing legitimate users from accessing it.
   Slowloris attacks: These attacks send incomplete HTTP requests that keep connections open for long periods, consuming server resources and preventing legitimate users from accessing it.

DNS amplification attacks: These attacks exploit vulnerabilities in DNS servers to amplify attack traffic and overwhelm the target system.

4) **Distributed denial-of-service (DDoS) attacks:** DDoS attacks are a type of DoS attack where the attack traffic is distributed across multiple compromised systems, making it more difficult to defend against. DDoS attacks can be even more disruptive than traditional DoS attacks, as they can overwhelm the target system with a much larger volume of traffic.

CASE STUDY

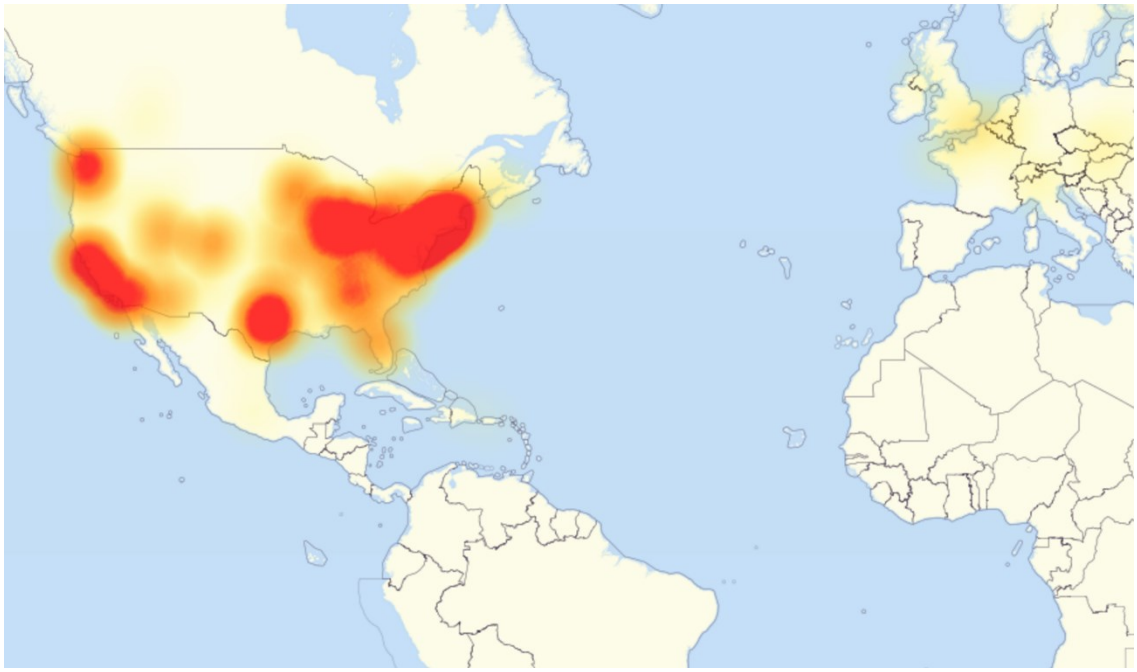
The Mirai Dyn DDoS Attack in 2016

When it happened: The attack occurred on October 21, 2016.

How it happened: This was a massive Distributed Denial-of-Service (DDoS) attack targeting the Domain Name System (DNS) provider Dyn. The attack used the Mirai botnet, which comprised hundreds of thousands of compromised Internet of Things (IoT) devices like cameras, routers, and baby monitors. Mirai scans the Internet for IoT devices that run on the ARC processor. This processor runs a stripped-down version of the Linux operating system. If the default username-and-password combo is not changed, Mirai is able to log into the device and infect it. The botnet sent millions of requests to Dyn's servers, overwhelming them and making many popular websites inaccessible for users in Europe and North America.

Impact/Damage: The attack caused significant disruptions:

- **Major websites outage:** Popular websites like Twitter, GitHub, Reddit, Netflix, Spotify and Amazon became unavailable or experienced slowdowns for several hours.

- 
Date	October 21, 2016
Time	11:10 – 13:20 UTC 15:50 – 17:00 UTC 20:00 – 22:10 UTC[2]
Location	Europe and North America, especially the Eastern United States
Type	Distributed denial-of-service
Participants	Unknown
Suspects	New World Hackers, Anonymous (self-claimed)

- **Economic losses:** Businesses relying on these websites likely suffered financial losses due to lost traffic and potential sales.
- **Public concern:** The attack highlighted the vulnerability of critical internet infrastructure and sparked public concern about cyberattacks.

Precautions taken for prevention: While it's impossible to completely prevent such attacks, Dyn and other organizations have implemented various measures:

- **Strengthening infrastructure:** Improving server capacities and redundancy to handle larger attacks.

- **Filtering malicious traffic:** Utilizing advanced traffic filtering techniques to identify and block suspicious requests.
- **Promoting IoT security:** Raising awareness about the importance of securing IoT devices and updating firmware regularly.
- **Collaboration:** Cooperating with security researchers and law enforcement agencies to track attackers and develop mitigation strategies.

Overcoming the situation: Dyn eventually mitigated the attack by filtering out malicious traffic and rerouting requests through unaffected servers. While the attack caused substantial disruption, it prompted action across the industry:

- **Increased focus on IoT security:** The attack exposed the potential dangers of unsecured IoT devices, leading to more focus on securing these devices and developing security standards.
- **Improved DDoS mitigation capabilities:** Service providers like Dyn invested in better DDoS mitigation tools and strategies to handle future attacks.
- **Greater collaboration:** The attack encouraged increased collaboration between governments, businesses, and security experts to share information and combat cyber threats.

Additional details:

- The creators of the Mirai botnet were eventually identified and prosecuted.
- The Mirai attack served as a wake-up call for both individuals and organizations about the importance of cybersecurity and responsible use of technology.
- The event continues to shape ongoing discussions and efforts to combat the evolving threat of large-scale DDoS attacks.