Ganpat University | Institute of Computer Technology
॥ विद्यया समाजोत्कर्षः ॥

Name: Tushar Panchal

En.No: 21162101014

Sub: INS (INFORMATION SECURITY)

Branch: CBA

Batch:61

----------PRACTICAL 02----------

❖ Question :

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.

1) Types of DOS
2) One Case Study - How it happened? When it happened? What is impact or damage caused? What Precautions they took for Prevention? How did they overcome this situation?

1. Types of DOS :

» different types of Denial-of-Service (DoS) attacks, each with its own method of disrupting access to resources :

1. Browser Redirection:

- ***Description***: In this type of DoS attack, the hacker redirects users from the intended webpage to a different URL, preventing them from viewing the original content.

- ***Impact*:** Users are unable to access the content they intended to visit, and the hacker may lead them to potentially malicious or fraudulent pages.

2. **Closing Connections:**
    - ***Description*:** The hacker forcibly closes connections between the server and client, disrupting communication and preventing further data exchange.
    - ***Impact***: Users experience a loss of connectivity, and the targeted server becomes isolated, rendering it inaccessible to legitimate users.
3. **Data Destruction:**
    - ***Description*:** The hacker intentionally destroys resources by deleting, erasing, wiping, overwriting, or dropping tables, making them unavailable.
    - ***Impact*:** Loss of critical data or resources, potentially causing permanent damage and making services or information unavailable to users.
4. **Resource Exhaustion:**
    - ***Description*:** The hacker overwhelms a web application by repeatedly requesting access to a resource, causing the application to slow down and eventually crash.
    - ***Impact*:** Users are unable to access the web application due to the excessive load, leading to service unavailability.

2. Case Study :

Case Study 1: EA Sports (Electronic Arts) DoS Attack :

When: June 10, 2022

How it happened: EA Sports, a leading game company, fell victim to a massive Denial-of-Service (DoS) attack during the launch of a highly anticipated game title. Attackers flooded EA's servers with a barrage of traffic, rendering the online gaming platforms inaccessible for users worldwide.

Impact/Damage: The DoS attack resulted in significant downtime for EA's online services, disrupting the gaming experience for millions of players. This not only led to financial losses but also caused a dent in EA's reputation for the unstable launch of the new game.

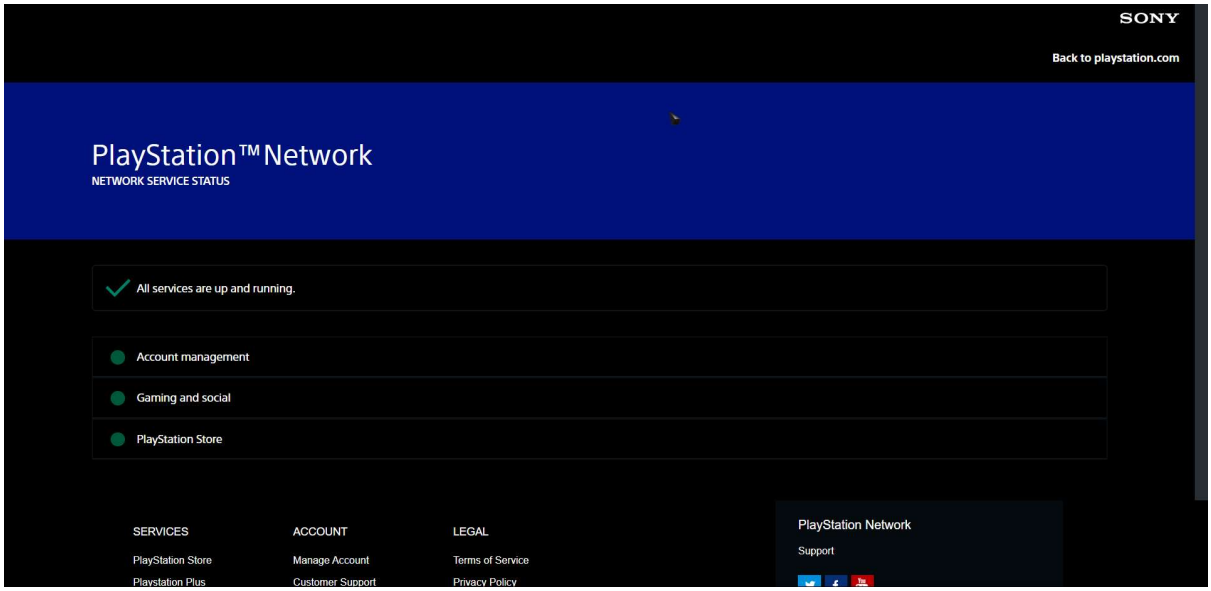
Precautions Taken for Prevention:

1. **Increased Server Capacity:** EA Sports enhanced server capacity in anticipation of high traffic during the game launch.
2. **DDoS Mitigation Services:** Implementing advanced DDoS mitigation services to identify and filter malicious traffic.
3. **Communication and Transparency:** EA communicated transparently with users, explaining the situation, and provided regular updates on the progress of resolving the issue.

Overcoming the Situation:

1. **Quick Response:** EA's incident response team quickly identified the DoS attack and initiated countermeasures.
2. **Collaboration with ISPs:** Engaging with Internet Service Providers to filter malicious traffic and restore normal service.
3. **Post-Incident Analysis:** Conducting a thorough post-incident analysis to identify vulnerabilities and improve future response strategies.

» Case Study 2 : Sony PlayStation Network (PSN) Attack :



When: April 20, 2023

How it happened: Sony's PlayStation Network (PSN) experienced a sophisticated DoS attack that overwhelmed its servers. The attackers exploited a combination of vulnerabilities in the

network infrastructure, leading to a temporary shutdown of online gaming services and the PlayStation Store.

Impact/Damage: The DoS attack disrupted online gaming for millions of PlayStation users and resulted in a halt to digital purchases through the PlayStation Store. Sony faced financial losses and a considerable backlash from its user base.

Precautions Taken for Prevention:

1. **Enhanced Network Monitoring:** Sony implemented advanced network monitoring tools to detect and respond to abnormal traffic patterns.
2. **Geographic Redundancy:** Establishing geographic redundancy to distribute server loads and minimize the impact of regional attacks.
3. **User Authentication Improvements:** Strengthening user authentication mechanisms to prevent unauthorized access during DoS attacks.

Overcoming the Situation:

1. **Collaboration with ISPs:** Sony collaborated with Internet Service Providers to filter malicious traffic and restore normal service.
2. **Post-Incident Review:** Conducting a thorough post-incident review to identify vulnerabilities and enhance the overall security posture.
3. **Compensation and Apology:** Sony offered compensation to affected users and issued a public apology, outlining the steps taken to prevent future incidents.