Familiarity with Denial-of-service (DoS) Attacks

Introduction: Description of DoS/DDoS attacks and their objectives

In the realm of cybersecurity threats, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks occupy a notorious position. Characterized by their intent to disrupt and deny legitimate access to online services, these attacks overwhelm targeted networks, websites, or online services with a flood of internet traffic. This deluge of data, typically originating from a network of compromised computers, is designed to overload systems and render them inoperable, thereby denying service to legitimate users.

DoS attacks involve a single source flooding the target with traffic, while DDoS attacks are more complex, utilizing multiple infected sources to launch a coordinated assault. These attacks aim not only to disrupt business operations and services but can also serve as a smokescreen for other malicious activities, including data breaches and malware infiltration.

Identification: How to recognize signs of an ongoing DoS/DDoS attack

Detecting a DoS or DDoS attack early is crucial to minimizing its impact. Here are key indicators that may suggest your system or network is under such an attack:

Unusually Slow Network Performance

- A significant slowdown in network speed or inability to access websites and online services.
- Unexplained delays in loading web pages or network resources.

Unexpected Increase in Traffic

- A sudden spike in network traffic without a clear source or reason.
- Traffic analytics showing an unusual influx of requests to a single endpoint or service.

Website or Service Unavailability

- Repeated timeouts or error messages when trying to access websites or online services.
- The inability of customers or users to access your platform is indicated by an increase in complaints or support requests.

Disproportionate Request Volume
- A large number of requests from a single IP address or multiple requests from varied sources but with similar characteristics.
- Unusual patterns in traffic, such as spikes at odd hours or uniform request intervals.

Performance Discrepancies
- Disparity in website performance or accessibility from different geographic locations.
- Internal network functioning normally while external services are impacted, or vice versa.

Security Software Alerts
- Intrusion detection systems or firewalls triggering alerts about potential DoS/DDoS activities.
- Notifications from security software indicating blocked access attempts from suspicious sources.

Systematic Website Crashes
- Repeated and unexplained crashing or rebooting of web servers.
- Server logs indicate resource exhaustion, such as memory or CPU overload.

Unusual Network Data Patterns
- Analysis of network packets revealing uncharacteristic data types or patterns associated with known DoS/DDoS tactics.
- Patterns that deviate from the normal profile of network traffic, both in quantity and type.

If any of these signs are observed, it's critical to take them seriously and investigate further to confirm whether a DoS or DDoS attack is underway. Early detection is key to implementing effective countermeasures and mitigating the impact of the attack.

Immediate Actions: What to do when you've identified a DoS/DDoS attacks

Once a DoS or DDoS attack is identified, immediate action is crucial to mitigate its impact. Here are the essential steps to follow:

Alert Your IT Team
- Immediately inform your IT department or cybersecurity team about the suspected attack.
- Provide them with any relevant information, including the nature and onset time of the attack.

Engage Your Incident Response Plan
- Activate your organization's incident response plan specifically tailored for DoS/DDoS attacks.
- Ensure all team members are aware of their roles and responsibilities during the response.

Increase Bandwidth
- Temporarily increase your network bandwidth to handle the excess traffic, if feasible.
- This can help absorb or dilute the traffic influx, providing temporary relief.

Implement Traffic Filtering
- Use filtering tools to identify and block malicious traffic.
- Set up rate limiting or IP blocking to control the influx of requests.
-

Contact Your ISP
- Reach out to your Internet Service Provider (ISP) for assistance. They may be able to re-route traffic or provide additional resources.
- ISPs often have larger infrastructure and more capabilities to mitigate such attacks.

Deploy Additional Defense Mechanisms

- Utilize anti-DDoS services or technologies specifically designed to combat these attacks.
- Engage cloud-based DDoS protection services for enhanced traffic scrubbing.

Monitor Traffic and Systems

- Continuously monitor network traffic for changes in the attack pattern.
- Keep a close eye on system performance and resource utilization.

Communicate with Stakeholders

- Notify internal stakeholders and, if necessary, customers about the attack and potential service disruptions.
- Keep communication clear, concise, and frequent to manage expectations.

Preserve Logs and Evidence

- Ensure that all logs related to the attack are preserved for future analysis and potential legal actions.
- Document every step of the response process for post-incident review.

Legal and Regulatory Compliance

- Check if the attack requires reporting to regulatory authorities under compliance laws.
- Consider consulting with legal teams to understand the implications of the attack.

Post-Attack Analysis

- Once the attack is mitigated, conduct a thorough analysis to understand its origin, impact, and any system vulnerabilities exploited.
- Use the insights gained to strengthen defenses against future attacks.

Responding effectively to a DoS/DDoS attack requires a coordinated effort and rapid deployment of resources and strategies. Keeping a calm and organized approach is key to navigating through the situation effectively.

This project was funded by the European Union's Internal Security Fund - Police Programme under Grant Agreement No 101038738