Héctor Ocaña

Denial of Service Playbook

Version History

Version	Update Date	Updated by	Resaon for Update
1.0	22/02/2024	Héctor	Initial Draft

Playbook

How to Use This Playbook

Purpose

To guide our organization in responding to a web application compromise incident. This playbook may also be used for a **Denial of Service Attack.**

How to use this Playbook

The steps in this playbook should be followed sequentially where appropriate. With many steps in the **Containment, Eradication, and Recovery** steps, some overlap may occur and is expected.

Playbook

Introduction

A Denial-of-Service (DoS) attack is a malicious strategy aimed at disrupting the normal operation of a computer system, network, or online service by inundating it with an overwhelming volume of traffic or exploiting vulnerabilities. The objective is to render the target temporarily or indefinitely unavailable to its intended users. DoS attacks encompass various techniques, including flooding systems with traffic, exhausting resources, exploiting network protocol vulnerabilities, and specifically targeting application vulnerabilities. Distributed Denial-of-Service (DDoS) attacks, involving multiple coordinated systems, are particularly challenging to defend against.

Playbook

Escalation Path

1. Initial Detection:

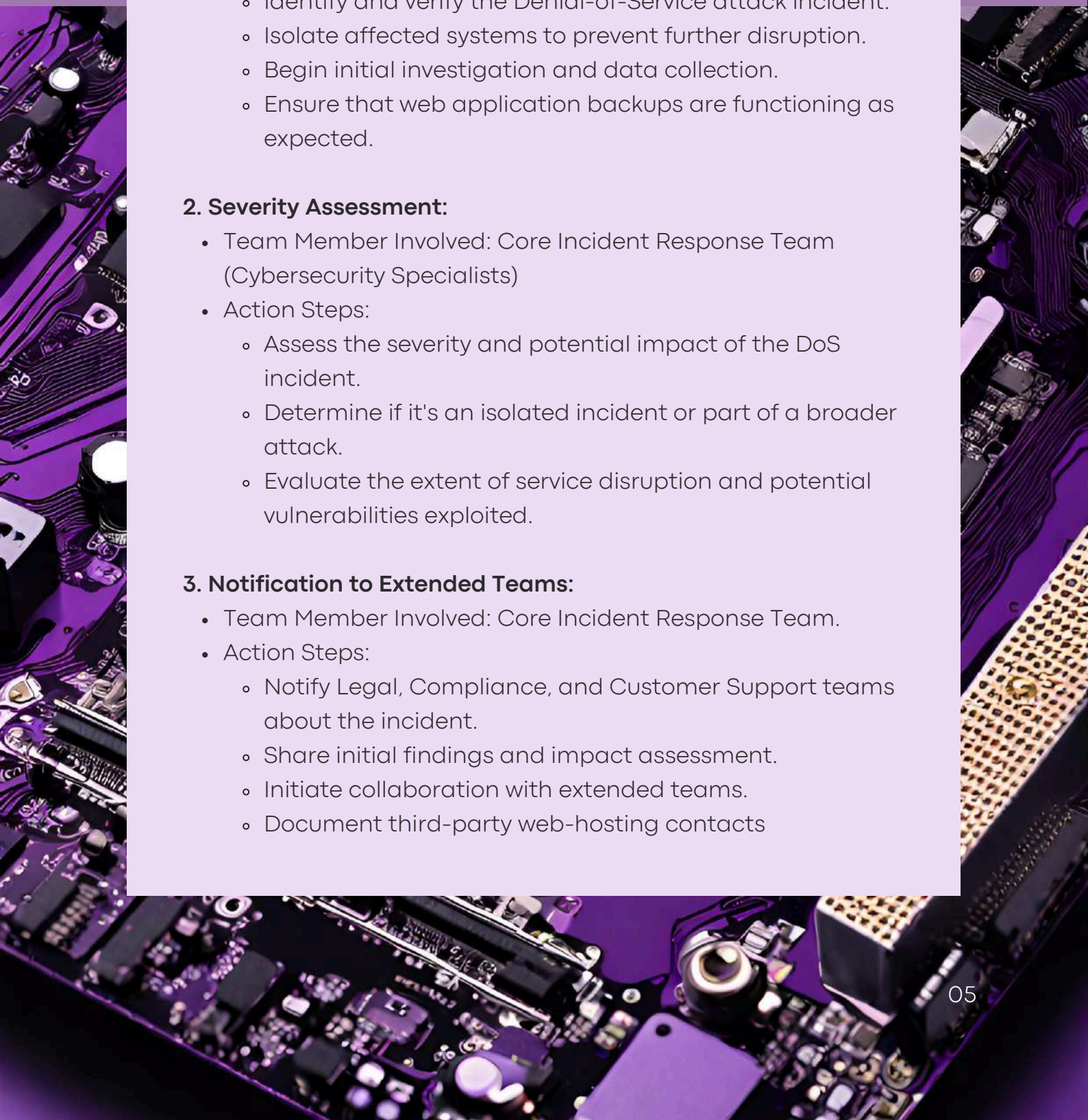
- Team Member Involved: Core Incident Response Team
- Action Steps:
  - Identify and verify the Denial-of-Service attack incident.
  - Isolate affected systems to prevent further disruption.
  - Begin initial investigation and data collection.
  - Ensure that web application backups are functioning as expected.

2. Severity Assessment:

- Team Member Involved: Core Incident Response Team (Cybersecurity Specialists)
- Action Steps:
  - Assess the severity and potential impact of the DoS incident.
  - Determine if it's an isolated incident or part of a broader attack.
  - Evaluate the extent of service disruption and potential vulnerabilities exploited.

3. Notification to Extended Teams:

- Team Member Involved: Core Incident Response Team.
- Action Steps:
  - Notify Legal, Compliance, and Customer Support teams about the incident.
  - Share initial findings and impact assessment.
  - Initiate collaboration with extended teams.
  - Document third-party web-hosting contacts



Playbook

Escalation Path

4. Investigation Deepening:

- Team Member Involved: Extended Teams (Legal and Compliance)
- Action Steps:
  - Legal team assesses any legal implications or obligations.
  - Compliance team ensures adherence to regulatory requirements.
  - Communicate with external stakeholders if required.

5. Executive Briefing:

- Team Member Involved: Core Incident Response Team (Team Lead)
- Action Steps:
  - If severity warrants, brief Executive Leadership on the incident.
  - Provide a high-level overview of the situation, potential impact, and current actions being taken.
  - Discuss resource allocation and strategic decisions.

6. Public Relations Engagement:

- Team Member Involved: Extended Teams (Public Relations)
- Action Steps:
  - Public Relations team prepares for potential public communication.
  - Craft a message for customers or the public, if necessary.
  - Coordinate with Legal to ensure messaging compliance.

Playbook

Escalation Path

7. Full Incident Response Activation:

- Team Member Involved: Core Incident Response Team (Team Lead)
- Action Steps:
  - If the situation escalates further, activate the full incident response plan.
  - Coordinate with all relevant teams to execute response actions.
  - Continue monitoring and updating stakeholders.

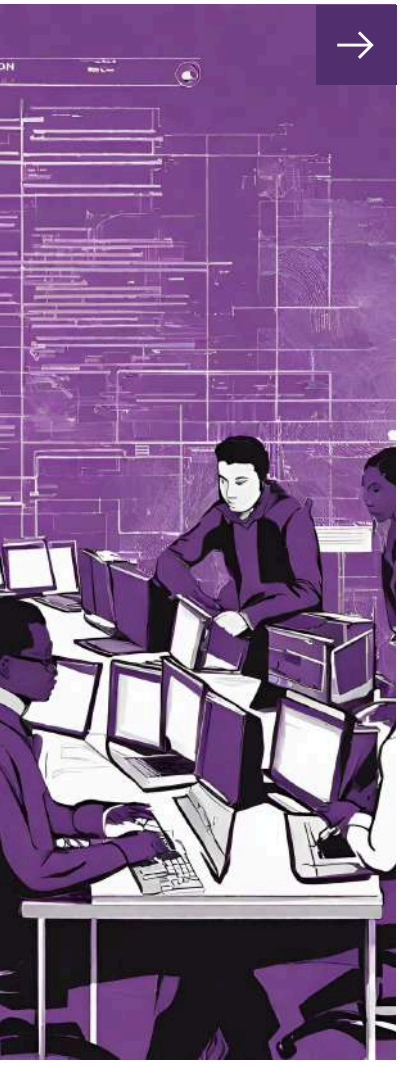
8. Post-Incident Review and Improvement:

- Team Member Involved: Core Incident Response Team (Post-Incident Review Lead)
- Action Steps:
  - Conduct a post-incident review to analyze the response effectiveness.
  - Identify areas for improvement in detection, response, and communication.
  - Update the SQL Injection Playbook based on lessons learned.

Playbook

Planning and Prevention

Regular security analyses throughout the software development process are vital for identifying potential vulnerabilities to Denial-of-Service (DoS) attacks. By utilizing static code analysis tools and vulnerability scanners, developers can detect and address security concerns before deploying the application in a production environment, fortifying it against potential exploitation and disruption.



01 Rate Limiting

In summary, rate limiting is a method of **controlling traffic flow** to a service or server by restricting the number of requests that can be made within a certain time frame. It is an essential technique for preventing resource abuse, ensuring fair use of services and protecting against DoS attacks.

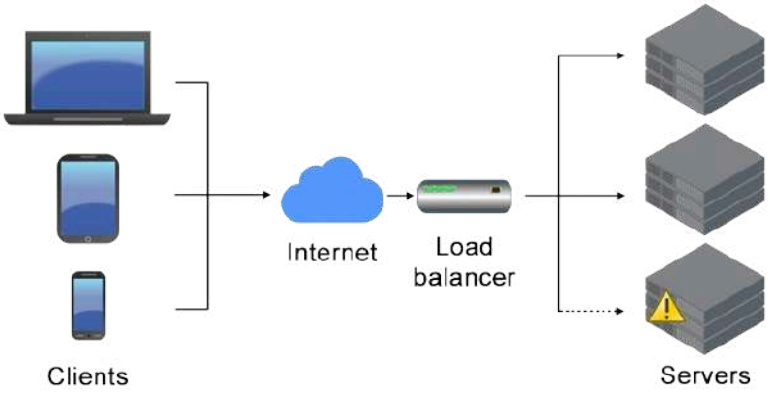
02 Traffic Monitoring and Anomaly Detection

Utilize **traffic monitoring tools** and **anomaly detection systems** to identify unusual patterns or sudden spikes in network traffic. Unusual behavior may indicate a potential DoS attack, and timely detection allows for swift response.

Planning and Prevention

03 Load Balancing

Distribute incoming network **traffic across multiple servers** using load balancing mechanisms. This not only improves overall system performance but also helps to distribute and mitigate the impact of a DoS attack by spreading the load.



04 Intrusion Detection & Prevention System (IDPS)

Our organization can enhance their cybersecurity by actively monitoring and analyzing network and system activities. IPS **can be configured to automatically detect and respond to patterns indicative of suspicious or malicious behavior**, providing real-time protection against potential threats. Furthermore, these systems **are capable of mitigating Distributed Denial of Service (DoS) attacks by identifying and blocking malicious traffic**, thereby safeguarding the integrity and availability of network resources. The proactive nature of IPS helps fortify the overall security posture by swiftly responding to emerging threats and minimizing the impact of cyberattacks on the organization's infrastructure.

SURICATA SNORT®

Planning and Prevention

Playbook

05 Collaboration with ISP

Establishing effective communication channels with our **Internet Service Providers (ISPs)** is crucial for a robust response to Denial of Service (DoS) attacks. This **involves developing an incident response plan, maintaining up-to-date contacts, and collaborating closely with ISPs to share threat intelligence.** By implementing traffic monitoring and filtering solutions upstream, our organization can prevent malicious traffic from reaching their networks. Service Level Agreements (SLAs) should be established, and regular coordination exercises conducted to ensure a swift and coordinated response.

06 DNS Filtering

Implement Domain Name System (DNS) filtering to **prevent the resolution of malicious domains associated with DoS** attacks. Deploy a DNS filtering solution like **DNS sinkholing** or utilize threat intelligence feeds. Configure our DNS server to **regularly update its blocklist** from reputable threat intelligence sources. Additionally, consider implementing a policy to block DNS requests to domains with suspicious or anomalous patterns indicative of DNS amplification attacks. Regularly review and update your DNS filtering rules to stay ahead of emerging threats and enhance our network's security posture.

Playbook

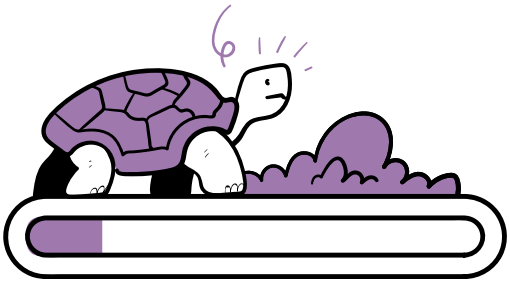
Identification

01 Unusual Spike in Traffic Volume

Monitor network traffic patterns for sudden and **significant increases** in inbound or outbound traffic volume, especially if it's coming from unexpected or **suspicious sources**.

02 Service Degradation or Outages

Keep an eye on system performance metrics, such as **response times**, **latency**, and **service availability**. A DoS attack often leads to **slowdowns** or complete unavailability of services.



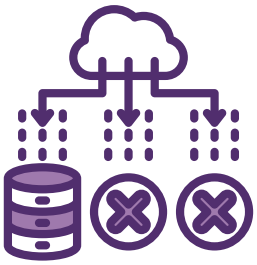
Identification

03 Abnormalities in Server Logs

Review server logs searching **errors**, **warnings**, or **unusual patterns** of **requests**. Look for **repeated requests** from the same IP address or unusual user-agent strings.

04 Unexplained Network Congestion

If your network experiences **congestion** or packet loss **without any** obvious **cause**, it could indicate a DoS attack overwhelming your network infrastructure.



05 Inability to Access Resources

Users reporting difficulties accessing your website, application, or network resources may be experiencing the effects of a DoS attack.

06 Anomalous Behavior from Security Devices

Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) may trigger alerts or block traffic due to suspicious activities associated with a DoS attack.

Identification

07 Unusual Patterns in Traffic Sources

Analyze the geographic origin, IP addresses, and behavior of incoming traffic. A DoS attack **may involve traffic originating from a large number of compromised devices** (botnet) or spoofed IP addresses.

08 DNS Resolution Issues

If our **Domain Name System** (DNS) **server is overwhelmed by a flood of requests**, it may struggle to resolve domain names, resulting in DNS resolution failures.

09 Unexpected Resource Utilization

Monitor system resource utilization, such as CPU, memory, and bandwidth usage. A sudden **increase in resource consumption without corresponding legitimate activity** could indicate a DoS attack.

10 Alerts from Network Security Devices

Pay attention to **alerts generated by firewalls, WAFs** (Web Application Firewalls), **or other network security devices** indicating suspicious or malicious activity.

Playbook

Containment & Erradication

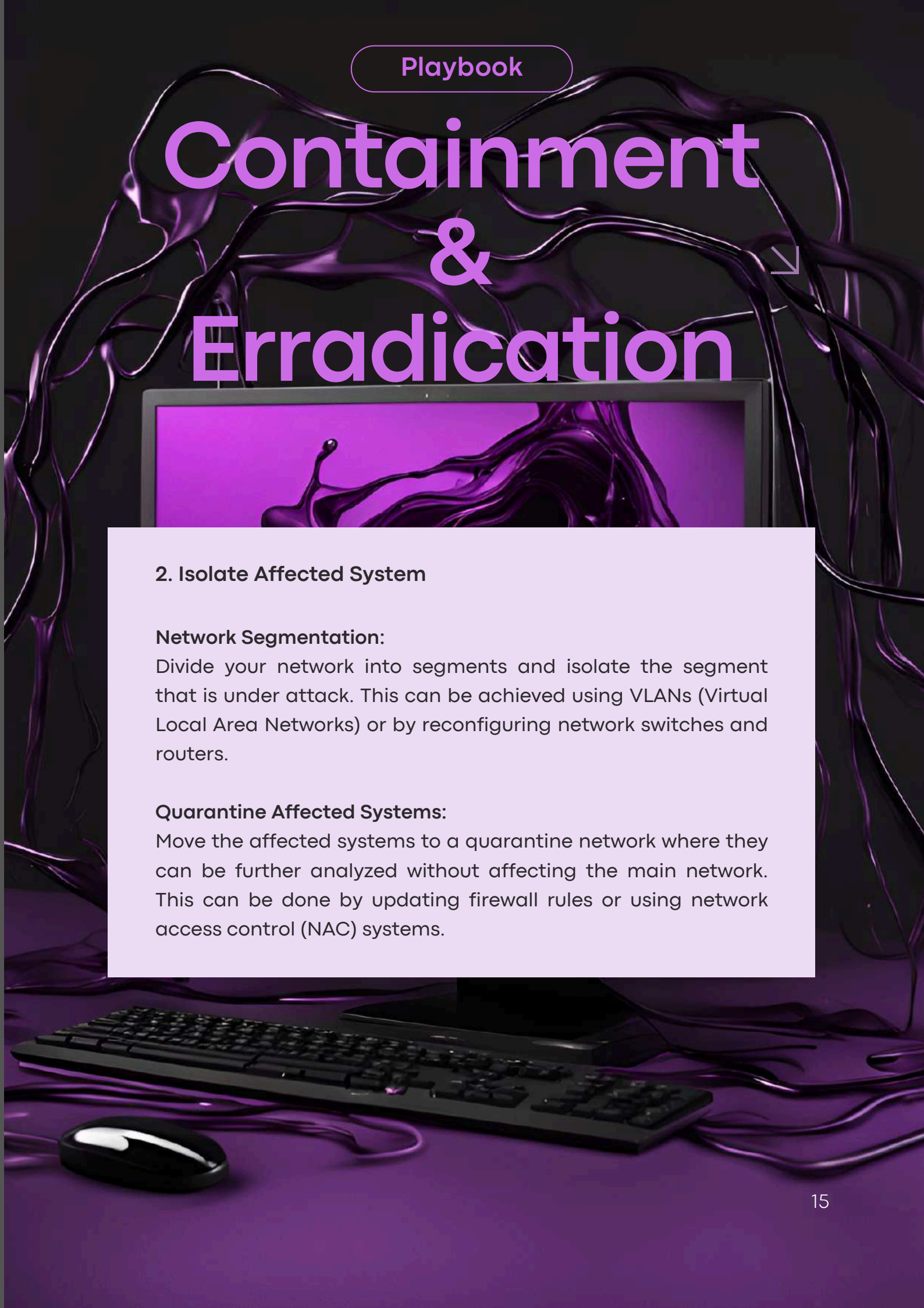
1. Activate Mitigation Measures

Rate Limiting:
Configure servers and applications to limit the number of requests that can be made by a single IP address within a given time frame. For example, allow only 100 requests per minute from a single IP address.

Traffic Filtering:
Pay attention to firewalls or intrusion prevention systems (IPS) to filter malicious traffic. To establish the appropriate rules for this case.

Traffic Shaping:
Apply traffic shaping techniques to prioritize critical traffic over non-essential traffic. This ensures that essential services remain operational even under attack.

Containment & Erradication



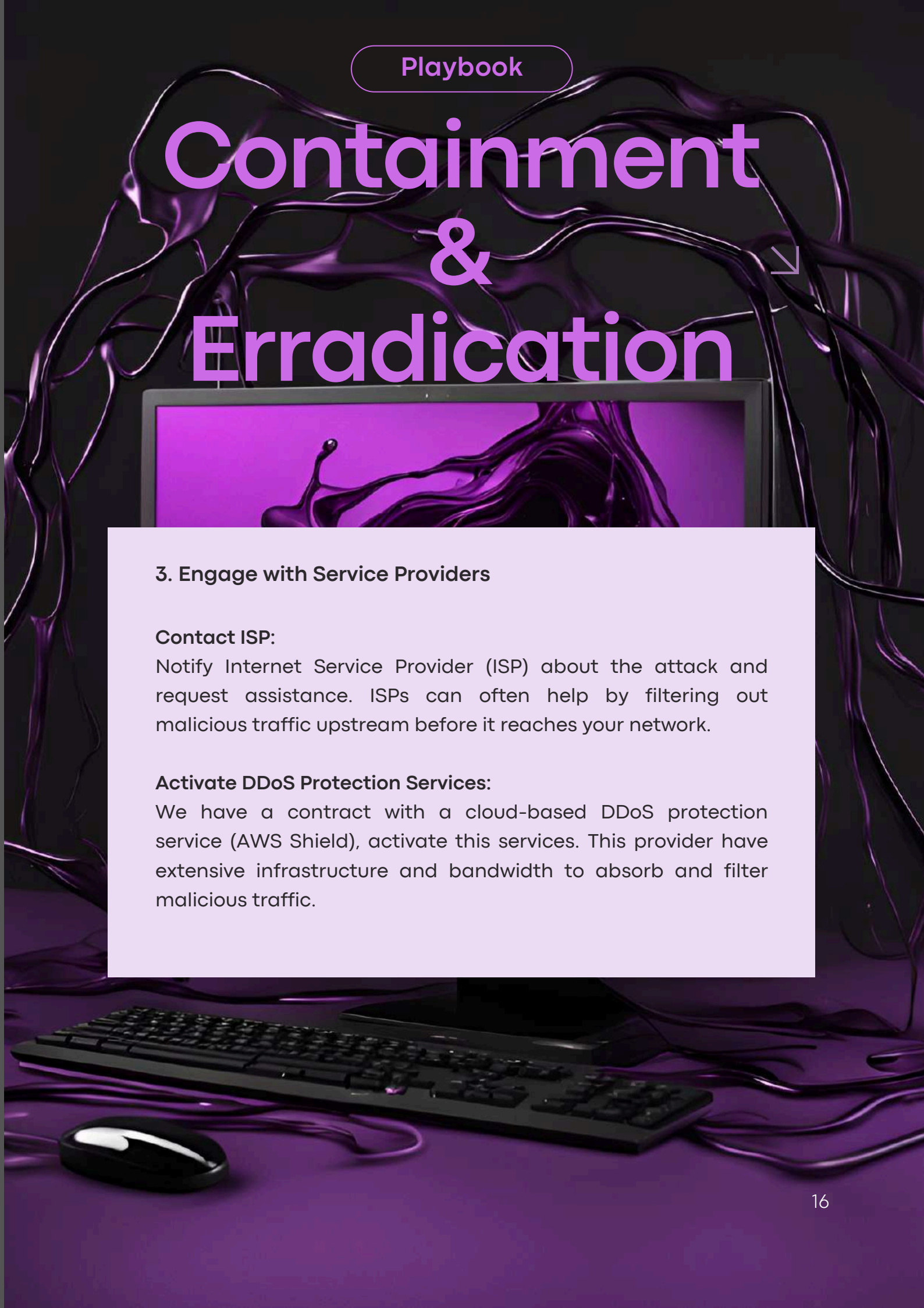
2. Isolate Affected System

Network Segmentation:
Divide your network into segments and isolate the segment that is under attack. This can be achieved using VLANs (Virtual Local Area Networks) or by reconfiguring network switches and routers.

Quarantine Affected Systems:
Move the affected systems to a quarantine network where they can be further analyzed without affecting the main network. This can be done by updating firewall rules or using network access control (NAC) systems.

Playbook

Containment & Erradication



3. Engage with Service Providers

Contact ISP:
Notify Internet Service Provider (ISP) about the attack and request assistance. ISPs can often help by filtering out malicious traffic upstream before it reaches your network.

Activate DDoS Protection Services:
We have a contract with a cloud-based DDoS protection service (AWS Shield), activate this services. This provider have extensive infrastructure and bandwidth to absorb and filter malicious traffic.

Containment & Erradication

4. Adjust Firewall Rules

Blocking Malicious IPs:
Identify and block IP addresses that are generating malicious traffic using your firewall. This can be done manually or using automated tools.

Throttling Specific Ports:
Configure the firewall to throttle or limit traffic to specific ports that are under attack. For example, if web server's port 80 is being targeted, you can limit the number of connections allowed to that port.

Deploying Access Control Lists (ACLs):
Use ACLs to control which IP addresses can access specific network resources. This helps ensure that only legitimate traffic is allowed through.

Containment & Erradication

5. Redirect Traffic

Load Balancing:
Use load balancers to distribute incoming traffic across multiple servers. Configure your load balancers to detect and mitigate attack traffic by routing it to less critical systems or by applying rate limiting.

Traffic Scrubbing:
Route traffic through a scrubbing center where malicious traffic is filtered out before it reaches your network. Many cloud providers offer scrubbing services that can be integrated with your existing infrastructure.

Containment & Erradication

6. Increase System Resources

Scaling Up Infraestructure:
Temporarily increase the capacity of your infrastructure by adding more servers, increasing bandwidth, or allocating additional virtual machines. Cloud services can be particularly useful for quickly scaling resources.

Utilizing Content Delivery Networks (CDNs):
Deploy CDNs to cache and distribute content across multiple locations. CDNs can absorb and mitigate traffic from DoS attacks by serving content from various points of presence (PoPs).

Elastic Resource Allocation:
Use cloud-based auto-scaling features to automatically allocate more resources when an attack is detected. Configure triggers that initiate scaling based on traffic volume or system load.

Playbook

Recovery

Once the Denial-of-Service (DoS) attack has been mitigated, you can begin to restore normal operations. Gradually re-enable services and open the ports that were temporarily closed during the attack. Start by verifying that the attack has fully ceased, and then proceed with a phased approach, reactivating less critical services first and monitoring their performance closely to ensure stability and security. Re-enable network interfaces (NICs) that were disabled, confirming they are properly configured and secure.

As services and ports are restored, continuously monitor network traffic and system performance for any signs of lingering issues or a resurgence of the attack. Ensure that all standard firewall rules and security policies are reapplied, and inform relevant stakeholders about the restoration of services. Conduct a post-incident review to document the attack details, mitigation steps, and lessons learned, and update your incident response plans to strengthen defenses against future attacks.

Playbook

POST-INCIDENT REVIEW

Conduct a post-mortem review with the security and development teams to analyze the response to the DDoS attack.

Assess the effectiveness of incident response procedures and identify any shortcomings or areas for improvement.

Determine corrective actions to prevent similar incidents in the future.

Update the cybersecurity playbook with new recommendations and best practices.

Disseminate lessons learned across the organization to foster continuous improvement and enhance cybersecurity awareness.

Disseminate lessons learned across the organization to foster continuous improvement and enhance cybersecurity awareness.