NETWORK DDOS INCIDENT RESPONSE CHEAT SHEET

Tips for responding to a network distributed denial-of-service (DDoS) incident.

General Considerations

DDoS attacks often take the form of flooding the network with unwanted traffic; some attacks focus on overwhelming resources of a specific system.

It will be very difficult to defend against the attack without specialized equipment or your ISP's help.

Often, too many people participate during incident response; limit the number of people on the team.

DDoS incidents may span days. Consider how your team will handle a prolonged attack. Humans get tired.

Understand your equipment's capabilities in mitigating a DDoS attack. Many under-appreciate the capabilities of their devices, or overestimate their performance.

Prepare for a Future Incident

If you do not prepare for a DDoS incident in advance, you will waste precious time during the attack.

Contact your ISP to understand the paid and free DDoS mitigation it offers and what process you should follow.

Create a whitelist of the source IPs and protocols you must allow if prioritizing traffic during an attack. Include your big customers, critical partners, etc.

Confirm DNS time-to-live (TTL) settings for the systems that might be attacked. Lower the TTLs, if necessary, to facilitate DNS redirection if the original IPs get attacked.

Establish contacts for your ISP, law enforcement, IDS, firewall, systems, and network teams.

Document your IT infrastructure details, including business owners, IP addresses and circuit IDs; prepare a network topology diagram and an asset inventory.

Understand business implications (e.g., money lost) of likely DDoS attack scenarios.

If the risk of a DDoS attack is high, consider purchasing specialized DDoS mitigation products or services.

Collaborate with your BCP/DR planning team, to understand their perspective on DDoS incidents.

Harden the configuration of network, OS, and application components that may be targeted by DDoS.

Baseline your current infrastructure's performance, so you can identify the attack faster and more accurately.

Analyze the Attack

Understand the logical flow of the DDoS attack and identify the infrastructure components affected by it.

Review the load and logs of servers, routers, firewalls, applications, and other affected infrastructure.

Identify what aspects of the DDoS traffic differentiate it from benign traffic (e.g., specific source IPs, destination ports, URLs, TCP flags, etc.).

If possible, use a network analyzer (e.g. tcpdump, ntop, Aguri, MRTG, a NetFlow tool) to review the traffic.

Contact your ISP and internal teams to learn about their visibility into the attack, and to ask for help.

If contacting the ISP, be specific about the traffic you'd like to control (e.g., blackhole what networks blocks? rate-limit what source IPs?)

Find out whether the company received an extortion demand as a precursor to the attack.

If possible, create a NIDS signature to focus to differentiate between benign and malicious traffic.

Notify your company's executive and legal teams; upon their direction, consider involving law enforcement.

Mitigate the Attack's Effects

While it is very difficult to fully block DDoS attacks, you may be able to mitigate their effects.

Attempt to throttle or block DDoS traffic as close to the network's "cloud" as possible via a router, firewall, load balancer, specialized device, etc.

Terminate unwanted connections or processes on servers and routers and tune their TCP/IP settings.

If possible, switch to alternate sites or networks using DNS or another mechanism. Blackhole DDoS traffic targeting the original IPs.

If the bottle neck is a particular a feature of an application, temporarily disable that feature.

If possible, add servers or network bandwidth to handle the DDoS load. (This is an arms race, though.)

If possible, route traffic through a traffic-scrubbing service or product via DNS or routing changes.

If adjusting defenses, make one change at a time, so you know the cause of the changes you may observe.

Configure egress filters to block the traffic your systems may send in response to DDoS traffic, to avoid adding unnecessary packets to the network.

Wrap-Up the Incident and Adjust

Consider what preparation steps you could have taken to respond to the incident faster or more effectively.

If necessary, adjust assumptions that affected the decisions made during DDoS incident preparation.

Assess the effectiveness of your DDoS response process, involving people and communications.

Consider what relationships inside and outside your organizations could help you with future incidents.

Key DDoS Incident Response Steps

1. Preparation: Establish contacts, define procedures, and gather tools to save time during an attack.
2. Analysis: Detect the incident, determine its scope, and involve the appropriate parties.
3. Mitigation: Mitigate the attack's effects on the targeted environment.
4. Wrap-up: Document the incident's details, discuss lessons learned, and adjust plans and defenses.

Additional DDoS Response References

Denial-of-Service Attack-Detection Techniques
http://www.computer.org/portal/site/dsonline...

A Summary of DoS/DDoS Prevention, etc. Techniques
http://sans.org/reading_room/whitepapers/intrusion/1212.php

Network Protocols and Tools Cheat Sheets
http://packetlife.net/cheatsheets/

This cheat sheet incorporates insights from Daniel Fairchild, Chris Lemieux, Peter McLaughlin, Jose Nazario, Donald Smith, Jim Tuttle, and Lenny Zeltser. It was compiled by Lenny Zeltser, and is distributed according to the Creative Commons v3 "Attribution" License. File version 1.3. More cheat sheets?