Denial of Service Attacks

Objectives

- Explain how denial of service attacks work
- Differentiate the different kinds of denial of service attacks
- Summarize defenses to denial of service attacks

Definition

- A denial-of-service attack is an attack on the availability of a service by blocking or overwhelming communication or resources to that service.
- From NIST: “An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.”

What are resources?

- Network Bandwidth – in most cases
- System Resources – CPU, Memory
- Application Resources – web server, DNS server, etc.

Common DoS Attacks – Ping attack

- What is it: Pings the server to initiate a response
- How is it carried out: Multiple pings either overwhelm the server or overwhelm the connection
- How to possibly prevent: Disable ping replies or responses either in software on the server or through firewall rules
- Other notes: This is an older style of attack

Common DoS Attacks – SYN

- What is it: Sends a half open SYN packet to the server
- How is it carried out: Multiple half open queries overwhelms software resources – typically through open sessions
- How to possibly prevent: Session timeout rules
- Other notes: This is a very effective attack, but most operating systems can handle it.

Common DoS Attacks – Other flooding

- What is it: Sends various requests to overwhelm resources
- How is it carried out: Depending on what the software is on the other side is how the attack is successful
- How to possibly prevent: Application memory handling, other firewall rules

Common DoS Attacks – Reflection or Recursion

Common DoS Attacks – Reflection or Recursion

- What is it: Sends requests on behalf of another system
- How is it carried out: Server asks another server that isn’t well protected to ask something on behalf of it
- How to possibly prevent: Disable recursion or at least lock down recursion to inside the network.
- Could be DNS or NTP

Defenses

- There are really no good defences other than firewall or operating system rules
- If enough traffic is generated, your systems will go down
- Developing a good plan is best
- Make sure you contact your upstream provider, they can help
- Backups?