DENIAL OF SERVICE

Can someone break a system so valid users are unable to use it? Denial of service attacks work by flooding, wiping or otherwise breaking a particular service or system.

An example of denial of service is where a Web server has been made temporarily unavailable or unusable with a flood of traffic generated by a botnet.

KEY CONCEPTS:

- Availability
- Botnets
- DDoS
- Content delivery network

Flooding of network traffic

- Failure to apply network isolation to a service which does not need to be on the internet
- Exposure of unnecessary services to the Internet
- Fails to filter network flooding attacks at OSI network layers 2 or 3
- Failure to use a CDN (for example Fastly, Cloudflare or AWS CloudFront)
- System was not designed to meet current traffic demands

Scripted application attacks

- Lack of rate limiting in Internet facing user interfaces

Operational concerns

- Lack of logging to determine source of flooding
- Lack response plans to block traffic from a particular source
- Lack of response plan to report issue to upstream infrastructure suppliers

And what else?

ThoughtWorks®

thoughtworks.com