Denial of Service Attacks

Carl Wahlberg
carl.wahlberg@hut.fi

What are DoS attacks ?

- They are Attacks for disrupting or completely denying
  - Access to services for Legitimate users
  - Access to networks
  - Access to systems
  - Access to other resources

What are DoS attacks? (2)

- The intent of attacks are usually malicious in nature
- There is actually little skill needed because there are many tools available for performing DoS-attacks.

Motivation of attackers?

- Using DoS-attack as a last resort when frustrated as no other hacking method has succeeded
- Personal or political vendettas against someone or some organization.
- DoS needed for compromising an vulnerable system

Different types of DoS attacks

- Bandwidth consumption
- Resource starvation
- Programming flaws
- Routing and DNS attacks

Bandwidth consumption

- Scenario 1 (Ping of Death)
  - Attackers are able to flood the victim’s network because the attackers have larger bandwidth.

    ex. attackers have 1,5Mbps link vs. victim’s 56kbps link.
  - it’s not confined to low-speed links. It’s possible to saturate an 1.5Mbps link if attackers have access to 100Mbps connection

Bandwidth consumption (2)

- Scenario 2: (DDoS)
  - Attackers amplify their attacks by engaging multiple sites to flood the victim's connection.
    - This way attackers can easily gather up to 100Mbps traffic by using just an 56kbps link
- in bandwidth consumption attacks it's difficult to find out the attackers because spoofing of addresses

Resource starvation

- Focuses on consuming system resources vs. network resources as in bw. consumption attacks
- Consuming CPU-utilization, memory, fs quotas etc.
- Often attackers have some legitimate access to the system, but abuses it to consume additional resources

Resource starvation (2)

- Then system and/or legitimate users are deprived of their share of resources
- Generally result in an unusable resource because the system crashes, file-system becomes full or processes hangs etc.

Programming flaws

- Are failures of an application, OS or embedded logic chip to handle exceptional conditions.
- Exceptional conditions result when an user sends unintended data to a vulnerable element.
  - ex. sending thousands of bytes to an application with an buffer of 128 bytes
    > buffer overflow >application crashes

Programming flaws (2)

- There is no such thing as a bug-free program, operating system or even CPU → Attackers also know this and will take full advantage of crashing critical applications and sensitive systems.
  - Pentium f00f bug allowed a user mode process to crash any OS by executing an invalid instruction 0xf00fc7c8

Routing and DNS Attacks

- Routing-based DoS attacks involves in manipulating routing table entries to deny service to to legitimate systems/networks.
  - RIP and BGP4 have very weak authentication which is rarely implemented, and this presents a scenario for attackers to alter legitimate routes by spoofing their source ip-address.
    → Victim’s traffic may be routed through the attackers network or to a black hole.

Routing and DNS Attacks (2)

- Most DNS DoS attacks involve convincing the victim server to cache bogus address information.
  - When a DNS server then performs a lookup attackers can redirect them to site of attackers’ liking or a black hole.