CAN304 W10

DoS Attacks

Denial of Service Attacks

对某些服务可用性的一种攻击形式。可能受到攻击的资源类别有：

- Network bandwidth
  - 与连接服务器到因特网的网络链路的容量有关
- System resources
  - 旨在使网络处理软件过载或崩溃
- Application resources
  - 通常涉及许多有效请求，每个请求都会消耗大量资源，从而限制了服务器响应其他用户请求的能力

Flooding Attacks

Classic DoS Attack: Flooding - 此攻击的目的是淹没目标组织的网络连接容量。

Flooding ping command：对目标网络进行大量 ping。攻击源明确；Response packets 影响源系统的网络性能。

Source Address Spoofing

使用伪造的源地址进行攻击。攻击者生成大量以目标系统为目的地址的数据包。

更难识别攻击系统；Response packets 不再反射回源系统。

SYN Spoofing

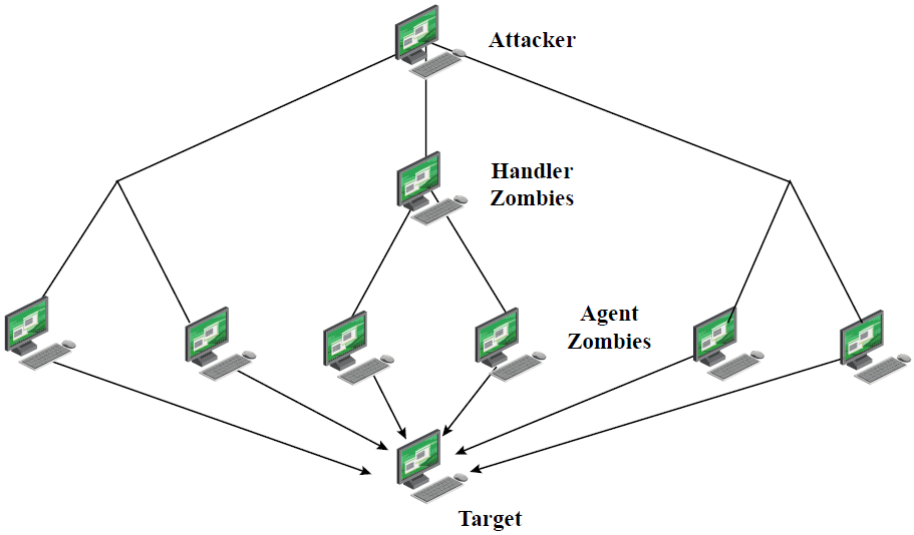
SYN：Synchronize Sequence Numbers

常见的 DoS 攻击，通过溢出用于管理它们的表来攻击服务器响应未来连接请求的能力。

合法用户被拒绝访问服务器，并且攻击系统资源，特别是操作系统中的网络处理代码。

例如：正常情况下，客户端使用 TCP 连接服务器，服务器有一个表记录请求。在 TCP SYN Spoofing Attack 中，攻击者发送大量请求，让记录请求的表溢出，让任何人都无法连接服务器。

Distributed Denial of Service Attacks



攻击者控制大量 agent aombles 对目标进行攻击。

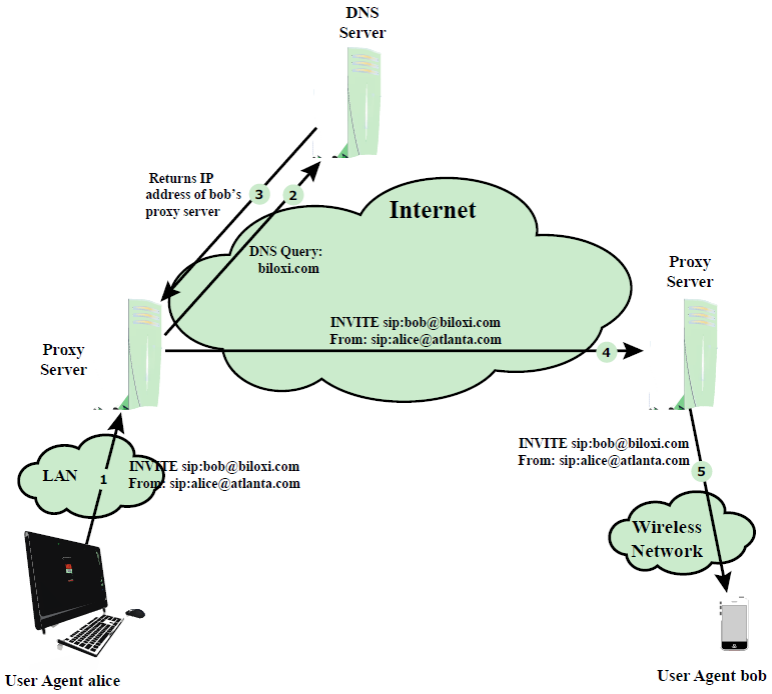
Application Based Bandwidth Attacks

策略：强制目标执行消耗资源的操作。

HTTP flooding attacks：用请求攻击 Web 服务器，例如 HTTP 请求下载大文件。

SIP flooding

SIP: Session Initiation Protocol for VoIP



同样是攻击服务器，使其过载。

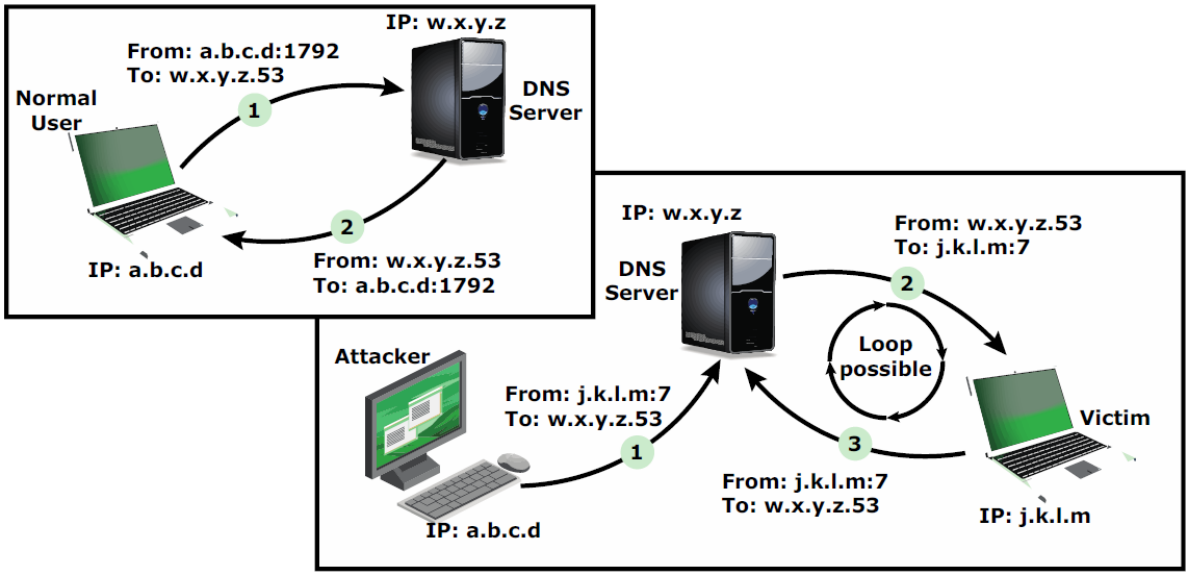
Reflector and Amplifier Attacks

Reflection Attacks

攻击者把自己的地址伪造成目标的地址，将数据包发送到中介上的已知服务。当中介响应时，响应将被发送到目标。相当于是让中介 (reflector) 来进行攻击。

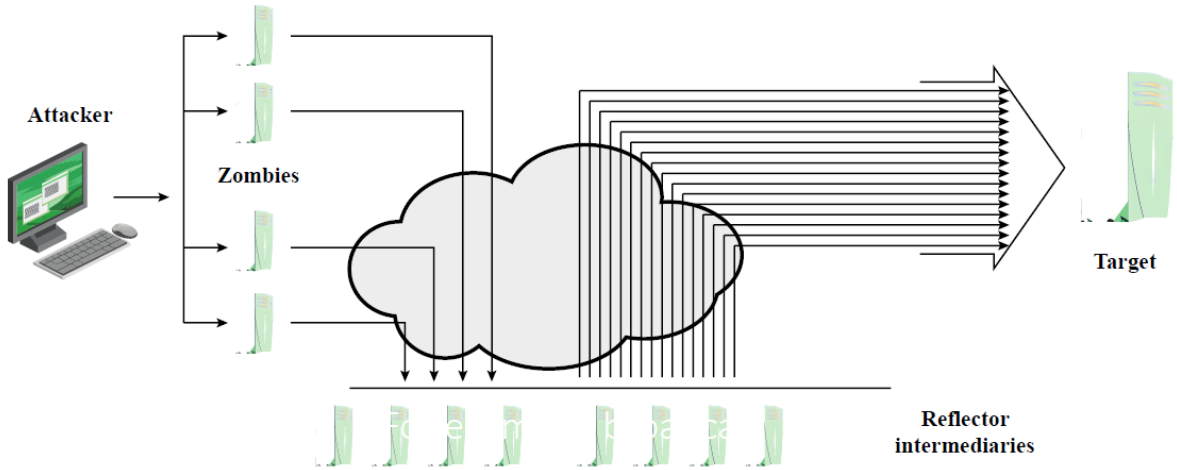
针对这些攻击的基本防御措施是阻止伪造的源数据包。

DNS Reflection Attack



让 DNS 来充当中介 (intermediary)。

Amplication Attack



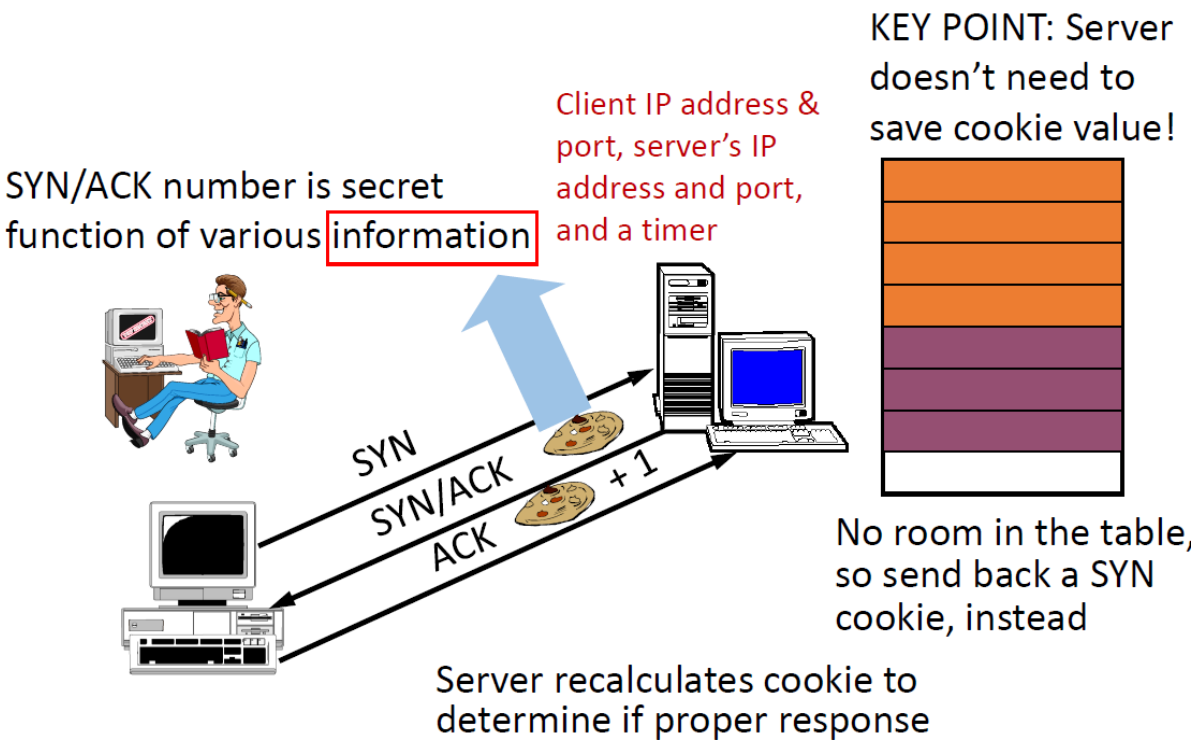
攻击者把请求发送给中介，中介会将请求扩增 (比如使用广播机制)，来发送给目标。

DoS Attack Defenses

这些攻击无法完全阻止，因为高流量可能是合法的 - 关于特定网站的高宣传，或在一个非常受欢迎的网站上的活动。

SYN cookies

在 TCP 服务器收到 TCP SYN 包并返回 TCP SYN+ACK 包时，不分配一个专门的数据区，而是根据这个 SYN 包计算出一个 cookie 值。在收到 TCP ACK 包时，TCP 服务器再根据那个 cookie 值检查这个 TCP ACK 包的合法性。如果合法，再分配专门的数据区进行处理未来的 TCP 连接。



这样可以防止 SYN Flooding attacks。