网络空间安全导论 · Ch8

计01　容逸朗　2020010869

Q1.

请描述 IP 分片污染攻击的原理与攻击者需要具备的能力。

- 原理：数据包在网络中传输时，可能因为数据过长导致需要分为不同的片来传输，由于碎片化发生在源主机或中间路由器上，而重组往往都在目的接收端发生，因此可以通过伪造分片、重组分片等方式破坏原始报文，从而造成拒绝服务攻击和污染攻击。
- 在这一过程中，攻击者需要具备的能力包括：源地址欺骗、熟悉 IP 分片协议（猜测 IPID）、原始报文校验和的欺骗等。

Q2.

结合几个针对 DNS 域名服务实施的 DDoS 攻击案例分析提升 DDoS 攻击防御能力的可行措施。

- 针对 DNS 域名攻击的例子如下：
  - 2013 年 8 月 25 日凌晨，.CN 域名凌晨出现大范围解析故障，导致大面积 .CN 域名无法解析，直到当日凌晨 4 点左右，CN 根域名服务器解析才开始部分恢复；
  - 2016 年攻击者控制大量物联网设备发起 DDoS 攻击，造成 CNN, BBC, PayPal 等网站无法访问；
  - 2019 年亚马逊的云计算部门 AWS 遭受了持续了大约八小时的 DDoS 攻击。最终 AWS 通过 Shield Advanced 提供了缓解，但无法完全阻止攻击。
- 可行措施：
  - 通过非对称加密验证身份（DNSSEC）验证数据真实性和完整性；
  - 利用 bailiwick 检查防范缓存污染；
  - 使用去中心化的域名系统及公钥基础设施 Blockstack。