网络空间安全导论 · Ch9

计01　容逸朗　2020010869

Q1.

简述 DNS 缓存策略在性能提升和引入安全威胁上具有的影响。

- DNS 使用缓存策略后，可以减少 DNS 解析时查询域名服务器的次数，从而减少网络延迟和带宽占用，提高网络应用的响应速度和可用性。
- 但是 DNS 缓存策略也会引入安全威胁。攻击者可以利用 DNS 缓存中的信息进行攻击，例如通过伪造 DNS 响应把用户将流量重新定向到恶意网站。也可以将恶意 IP 地址存储在 DNS 缓存中，让用户访问受害域名时返回恶意 IP 地址。

Q2.

请描述一下 DNS 基础设施中，stub resolver, public resolver, open resolver, authoritative name server, recursive name server, iterative name server, root name server 之间的关系和区别。

- DNS 基础设施的关系和区别如下：
  - Stub Resolver 是客户设备上运行的 DNS 客户端，主要是向其他 DNS 服务器发出域名解析请求；
  - Public Resolver 是由 ISP 或其他组织提供的 DNS 服务器，一般只为该 ISP 或组织的用户提供 DNS 解析服务。Open Resolver 则是一种公共 DNS 服务器，可以响应来自任何客户端的 DNS 查询请求。
  - Authoritative Name Server 存储特定域名的 DNS 记录，或指示 Stub Resolver 前往其他 DNS 服务器进行查询。
  - Recursive Name Server 在收到 DNS 查询请求时，会向其他 DNS 服务器递归地发送查询请求，直到找到目标信息。而 Iterative Name Server 在收到 DNS 查询请求时的行为则和前者不同，它不会为 Stub Resolver 执行递归查找，而是返回另一个 DNS 服务器的地址让 Stub Resolver 自行寻找。
  - Root Name Server 是 DNS 基础设施中最高层次的 DNS 服务器，它存储了所有顶级域名服务器的地址。