网络安全技术课堂作业

Homework 3

网络空间安全学院 信息安全专业
2112492 刘修铭 1027

1 简要分析 DNS 存在的安全风险及应对策略

1.1 DNS安全风险

1. **DNS 欺骗（Spoofing）**：攻击者通过伪造 DNS 响应来引导用户访问恶意网站。这种攻击可以导致用户无意中泄露敏感信息或下载恶意软件。

2. **DNS 放大攻击（Amplification Attack）**：利用 DNS 服务器对小请求进行大量响应的特性，攻击者向多个 DNS 服务器发送小量的伪造查询，使DNS服务器产生大量流量攻击目标系统。

3. **DNS 劫持（Hijacking）**：攻击者控制 DNS 服务器或路由器，改变 DNS 解析结果，使用户流量被重定向到恶意网站。

4. **DDoS 攻击**：利用 DNS 服务器作为攻击工具，对目标执行分布式拒绝服务攻击（DDoS），消耗目标的网络带宽和资源。

5. **子域名接管（Subdomain Takeover）**：当 DNS 条目指向的资源（如云服务）不再有效但 DNS 记录未更新时，攻击者可以接管子域名并托管恶意内容。

1.2 应对策略

1. **使用 DNSSEC（DNS Security Extensions）**：DNSSEC 为 DNS 提供了数据完整性验证机制，确保DNS响应的真实性和完整性，防止DNS欺骗和缓存投毒。

2. **部署安全的DNS架构**：采用递归和权威服务器的分离，限制哪些服务器可以进行递归查询，增加网络隔离，降低被攻击的风险。

3. **利用防火墙和入侵检测系统（IDS）**：配置网络防火墙和 IDS 以监控异常 DNS 流量和潜在的 DNS 攻击行为。

4. **访问控制和率限制**：对 DNS 查询进行访问控制和率限制，以减少恶意流量对 DNS 服务器的影响。

5. **及时更新和维护**：定期更新 DNS 服务器软件，修补已知的安全漏洞，以及对 DNS 配置进行定期审核，确保安全设置仍然有效。