南開大學
Nankai University

网络空间安全学院

网络安全技术实验报告

DNS 安全风险及应对策略

姓名：魏伯繁

学号：2011395

专业：信息安全

2023 年 6 月 4 日

目录

1 DNS 简介

DNS（Domain Name System）是一个用于将域名转换为 IP 地址的互联网服务，它是互联网中最重要的服务之一。DNS 协议定义了一种分布式数据库的网络协议，可以在互联网上映射域名和 IP 地址。

DNS 服务的作用是将人们熟知的域名转换成计算机可以识别的 IP 地址，这样计算机才能够与其他计算机进行通信。当用户输入一个域名时，计算机首先会查询本地 DNS 缓存，如果缓存中没有该域名的 IP 地址，则会向 ISP（Internet Service Provider，互联网服务提供商）提供的 DNS 服务器发出查询请求。ISP 的 DNS 服务器通常存储有众多的域名和 IP 地址的映射关系，如果该服务器中也没有该域名的 IP 地址，则会向其他 DNS 服务器发出查询请求，直到找到该域名的 IP 地址为止。最终，该 IP 地址会被返回给本地计算机，使网络连接得以建立。

DNS 服务可以使用户无需记住每个网站的 IP 地址，只需记住域名即可。而且，由于 IP 地址可能会发生变化，DNS 服务可以使网站管理员更方便地更改其服务器的 IP 地址，而无需更改其域名。

DNS 服务的实现基于一种分布式数据库系统，该系统分为根域名服务器、顶级域名服务器、权威域名服务器和本地 DNS 服务器四个层次。根域名服务器是整个 DNS 系统的最顶层，它负责管理所有顶级域名服务器的地址，它们是 DNS 系统中最高级别的服务器。顶级域名服务器负责管理特定的顶级域名，例如.com、.org、.edu 等。权威域名服务器则负责管理特定域名下的所有子域名和主机，例如，一个公司的权威域名服务器可能管理该公司的所有子域名和主机名。而本地 DNS 服务器则是用户计算机直接连接的 DNS 服务器，它通常由 ISP 提供，也可以是用户自己搭建的 DNS 服务器。本地 DNS 服务器可以缓存查询结果，提高查询速度，避免频繁查询。总之，DNS 服务在互联网中具有极其重要的作用，它的快速、准确和安全性对于互联网的稳定和发展至关重要。

2 DNS 安全风险

2.1 容易遭受 DNS 放大攻击

DNS 放大攻击是一种常见的 DDoS 攻击，攻击者会向公共 DNS 服务器发送 DNS 名称查询，使用受害者的地址作为源地址。这会导致公共 DNS 服务器将响应发送到目标系统，从而淹没目标系统。攻击者通常会查询尽可能多的域名信息，以最大限度地发挥放大效果。同时，通过使用僵尸网络，攻击者也可以轻松生成大量虚假 DNS 查询。由于响应来自有效服务器的合法数据，因此很难防止 DNS 放大攻击。

2.2 容易遭受 DNS 劫持/重定向

DNS 劫持（或 DNS 重定向）是指绕过 DNS 查询的名称解析。攻击者会通过恶意软件来修改系统的 TCP/IP 配置，将 DNS 服务器指向他们控制的 DNS 服务器，以实施 DNS 劫持攻击。此外，攻击者还可能操纵可信赖的 DNS 服务器，以运行网络钓鱼等恶意活动。

2.3 容易缓存中毒

攻击者会利用 DNS 服务器存在的漏洞来接管它们，以进行 DNS 缓存中毒。攻击者会注入恶意数据到 DNS 解析器的缓存系统中，从而将用户重定向到他们选择的网站，从而导致个人或其他数据被盗。DNS 缓存中毒代码通常通过垃圾邮件或网络钓鱼电子邮件中的 URL 传播。如果网络犯罪分子控

制了 DNS 服务器，则可以操纵缓存的信息。由于 DNS 服务器可以访问其他 DNS 服务器的缓存，因此这种类型的攻击可能会迅速扩散。主要风险是数据被盗窃。

2.4 容易遭受 DNS 隧道攻击

DNS 隧道是另一种常见的攻击模式，攻击者利用 DNS 协议注入恶意软件和其他数据，使用这些数据有效负载接管 DNS 服务器，并访问其管理功能和驻留在其上的应用程序。DNS 隧道通过 DNS 解析器在攻击者和目标之间创建隐藏连接，可用于实施数据泄露等攻击，并绕过防火墙。通常，DNS 隧道需要借助受感染系统作为跳板，以访问具有网络访问权限的内部 DNS 服务器，因为受感染的系统可以连接到外网。

2.5 僵尸网络反向代理

Fast Flux 是一种 DNS 规避技术，攻击者使用僵尸网络来隐藏其网络钓鱼和恶意软件活动，以逃避安全扫描。攻击者会使用受感染主机的动态 IP 地址充当后端僵尸网络主机的反向代理。此外，Fast Flux 还可以使用多种方法，如点对点网络、分布式命令和控制、基于 Web 的负载平衡和代理重定向等，以增加恶意软件网络被检测到的难度。

3 防御策略

3.1 严格控制访问

为了更好地控制谁可以访问企业网络，建议采用多因素或双因素身份验证。此外，确保在所有相关帐户上激活 MFA 并遵守适当的密码卫生规则也非常重要。CISA 建议，企业应及时更改所有可用于更改 DNS 记录的帐户的密码，包括管理公司 DNS 服务器软件的帐户、管理该软件的系统、DNS 运营商的管理面板和 DNS 注册商帐户。

3.2 部署零信任方案

由于许多组织已经采用了混合和远程工作模式，因此零信任方法越来越受欢迎。此外，零信任还可以帮助缓解 DNS 威胁。为降低风险，Gartner 建议安全和风险领导者实施两个与网络相关的关键零信任项目：一个是零信任网络访问 (ZTNA)，它会根据用户及其设备的身份、时间和日期、地理位置、历史使用模式和设备运行状况等其他因素授予访问权限。Gartner 认为，零信任能够提供一个安全且有弹性的环境，具有更大的灵活性和更好的监控。另一个项目是基于身份的网络分段，这是一种久经考验的方法，可以限制攻击者在网络中横向移动的能力。

3.3 检查/验证 DNS 记录

为确保网络安全，企业应该检查拥有和管理的所有域名，尤其是确保名称服务器引用的 DNS 服务器是正确的。此外，应该检查所有权威和辅助 DNS 服务器上的所有 DNS 记录。一旦发现任何差异和异常，应该立即调查并将其视为潜在的安全事件。

参考资料：知乎专栏