# DNS 及 DNS 攻击



N10.1. 希望除了 `localhost` 外，还能在本机使用 `myhost` 这个名称，应如何配置？

N10.2. 使用 `dig` 查询 `nsf.gov` 域的名称服务器信息。

N10.3. DNS 使用什么传输层协议和端口号？

N10.4. 验证 DNS 查询可以通过 TCP 发送。提示：`dig` 提供强制使用 TCP 的选项；运行命令并用 Wireshark 捕获 DNS 报文。

N10.5. 使用 `dig` 模拟本地 DNS 解析器为 `www.example.com` 查找 IP 地址的迭代过程，并给出每一步结果。

N10.6. 使用 `dig` 模拟本地 DNS 解析器对 IP 地址 `93.184.216.34` 进行反向解析的过程，并给出每一步结果。

N10.7. 本地 DNS 解析器软件最初如何知道根名称服务器的 IP 地址？

N10.8. DNS 查询报文中的哪些随机字段必须原样包含在响应中？

N10.9. 什么是 DNS 缓存投毒攻击？

N10.10. DNS 协议存在哪些根本问题，使它容易受到缓存投毒攻击？

N10.11. 对远程 DNS 服务器实施缓存投毒攻击非常困难。(1) 具体有哪些困难？(2) Kaminsky 攻击如何克服这些困难？

N10.12. Bob 想对一个递归 DNS 解析器实施 Kaminsky 缓存投毒攻击；他的目标是让解析器缓存主机名 `www.example.com` 的错误 IP 地址。Bob 知道迭代解析时，查询会依次发送到根服务器、`.COM` 名称服务器，最后到 `example.com` 的名称服务器。触发解析器开始迭代查询后，他可以选择伪造其中任意名称服务器的响应。Bob 决定伪造 `.COM` 服务器的响应。请说明攻击能否成功。

N10.13. Bob 想对一个递归 DNS 解析器实施 Kaminsky 缓存投毒攻击。他的目标是污染解析器的缓存，使自己的名称服务器能够回答对 `bank32.com` 域的任意查询。请用类似 `dig` 输出的格式给出 Bob 伪造响应的示例。

N10.14. Bob 想对递归 DNS 解析器实施 Kaminsky 缓存投毒攻击，但他的机器没有主机名（攻击从咖啡店 Wi-Fi 发起）。他计划在权威部分使用一个随机主机名，再在附加部分提供自己机器的 IP 地址。下面是伪造响应的一部分。这种方法可行吗？

```
;; AUTHORITY SECTION:
example.com. 259200   IN   NS   ns.ARandomName.net

;; ADDITIONAL SECTION:
ns.ARandomName.net 259200 IN  A  132.2.1.4
```

N10.15. 本地 DNS 服务器规定：任何尚未过期的缓存 NS 记录，每 20 分钟最多更新一次。例如，example.com 的 NS 记录在时刻 T 创建后，要到 T 加 20 分钟或记录过期时（以较早者为准）才能更新。这个策略会给 Kaminsky 攻击造成什么困难？

N10.16. 本地 DNS 解析器收到以下响应。哪些记录不会被缓存或不会被当作可信记录使用？请解释。

```
;; QUESTION SECTION:
;www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 259200 IN A 129.211.32.34

;; AUTHORITY SECTION:
example.net. 259200 IN NS ns.tklp-server.net
example.com. 259200 IN NS ns.gltd-server.net

;; ADDITIONAL SECTION:
ns.gltd-server.net 259200 IN A 132.2.10.9
ns.tklp-server.net 259200 IN A 130.3.11.39
ns.atfz-server.com 259200 IN A 128.0.31.66
```

N10.17. XYZ 公司建立了仅供内部使用的 www.example.com，但没有用防火墙限制来源。Web 服务器只对客户端 IP 做反向 DNS 查询：若 PTR 结果以 example.com 结尾就允许访问，否则拒绝。外部攻击者如何绕过该检查？

N10.18. DNS 根服务使用 IP Anycast 提高可扩展性和抗故障能力。Anycast 允许分布在不同地点的多台服务器通告同一服务地址，路由系统把报文送往拓扑上代价较低的实例。请说明根名称服务器如何使用这一技术扩展服务。

N10.19. 如果你负责一个 DNS 区域，会采取哪些措施降低 DDoS 风险？

N10.20. 在两国网络冲突中，国家代码顶级域（ccTLD）的权威 DNS 可能成为目标。若 A 国使 B 国 ccTLD 的全部权威服务器不可用，会严重影响 B 国域名解析。假设你负责资源有限的 B 国 ccTLD，应如何抵御强大对手的大规模 DDoS？

N10.21. 递归 DNS 服务器如果配置不当，可能被用于 DNS 放大攻击。这是一类 DDoS 攻击，攻击者借助第三方服务器（这里是 DNS 服务器）放大攻击流量。请查找相关资料并概述其原理。

N10.22. 在书中描述的 DNS 重新绑定攻击示例里，哪些机制阻止攻击者直接与目标 IoT 服务器交互？

N10.23. 在 DNS 重新绑定攻击中，运行在受害者浏览器里的攻击者 JavaScript 代码如何绕过同源策略？

N10.24. DNS 重绑定攻击中，如果受害者浏览器把 HTTP 请求所用主机名的 IP 缓存一小时，攻击还能成功吗？为什么？