

第5章 应用层协议安全

随着互联网的迅速发展和普及,各种网络应用层出不穷,而应用层协议作为网络通信的核心组件,其安全性显得尤为重要。在日常生活中,无论是浏览网页、在线购物,还是使用即时通信工具,都离不开应用层协议的支撑。本章主要探讨五种常见协议——DNS、HTTP、邮件传输协议、DHCP 和 FTP 面临的安全威胁、攻击方式和防御措施。针对每种协议,首先介绍其基本原理和功能,然后分析可能的安全风险和常见攻击手段,最后提出相应的安全防护和防御措施。

教学目标

- 理解和掌握 DNS、HTTP、邮件传输协议、DHCP 和 FTP 等应用层协议的基本原理和功能,以及它们在网络通信中的重要性。
- 识别和了解 DNS、HTTP、邮件传输协议、DHCP 和 FTP 等应用层协议面临的主要安全威胁和常见攻击方式。
- 掌握应用层协议常见的防御措施,提高应用层协议的安全性。

5.1 应用层协议概述

应用层协议是一种面向应用程序的通信协议,它位于 OSI/RM 模型的第七层,负责在网络中的不同应用程序之间传输数据。应用层协议不仅定义了数据的格式和传输方式,还提供了一些高级功能,例如错误恢复、流量控制和拥塞控制。具体来说,应用层协议的定义包括以下几点:

- (1) 应用进程交换的报文类型,如请求报文和响应报文。
- (2) 各种报文类型的语法,如报文中的各个字段及其详细描述。
- (3) 字段的语义,即包含在字段中信息的含义。
- (4) 进程何时、如何发送报文及对报文进行响应的规则。

应用层协议分为公用协议和专用协议。其中,公用协议由 RFC 文档定义,位于公共领域。例如,Web 的应用层的超文本传输协议 HTTP(RFC 2616)作为公用协议,如果浏览器开发者遵从 HTTP RFC 规则,所开发出的浏览器就能访问任何遵从该文档标准的 Web,并且服务器获取相应的 Web 页面。而专用协议则不能随意应用于公共领域。例如,P2P 文件共享系统大多数使用的是专用应用层协议。

由于应用层协议作为不同系统之间进行数据交流的桥梁,扮演着至关重要的角色。其

安全性不仅关系到个体用户的隐私,更关系到整个系统和组织的稳定运行,以及抵御各种恶意攻击的能力。因此确保应用层协议的安全性成为保护信息完整性、机密性和可用性的不可或缺的一环。应用层协议安全涵盖了多方面,包括但不限于认证、授权、数据完整性、机密性和抗拒否认等安全属性。在设计和实施应用层协议时,必须综合考虑这些安全要素,以确保系统和数据的全面保护。

然而,目前应用层协议安全面临诸多挑战。首先,应用层协议涉及的安全技术复杂多样,难以统一管理和维护。不同的协议需要采用不同的安全技术,每种技术的管理和维护都需要专业知识和技能。同时,随着技术的不断发展,新的安全技术也不断涌现,这进一步增加了管理和维护的难度。其次,随着攻击手段的不断升级,应用层协议的安全漏洞也不断被发现。黑客和恶意攻击者不断发明新的攻击手段,如 SQL 注入、跨站脚本攻击、远程命令执行等,这些攻击手段可以利用协议漏洞,对应用程序进行攻击和渗透。此外,移动互联网、物联网等新兴领域的应用层协议安全问题也日益凸显。



视频讲解

II 5.2 DNS 协议

5.2.1 域名系统

作为实现域名和 IP 地址相互映射的分布式数据库,域名系统(Domain Name System, DNS)由三大要素组成。

- (1) 域: 由地理位置或业务类型而联系在一起的计算机集合。
- (2) 域名: 由字符和(或)数字组成的名称,用于替代主机的 IP 地址。
- (3) 域名服务器: 提供域名解析服务(将域名映射 IP 地址)的主机。

下面分别介绍域名结构、域名服务器以及域名解析过程。

1. 域名结构

域名的实质是标识和定位计算机或资源层次结构的名称,通常按照从右到左的顺序,由多个标号组成,标号之间用点号(.)分隔。整个域名体系是一个树状结构,从根域名开始,通过一系列的子域名形成完整的域名层次结构。例如,域名 www.baidu.com 由三个标号组成,其中,标号 com 是顶级域名(TLD),标号 baidu 是二级域名,标号 www 是三级域名。

DNS 标准规定域名由英文字母和数字构成,每个子域名的长度不超过 63 个字符,为便于记忆,建议不超过 12 个字符。域名中除了连字符(-)外,不允许使用其他标点符号。域名从左至右,级别由低至高排列,最右边是最高级别的顶级域名。整个域名的总长度不得超过 255 个字符。DNS 不限制域名包含的子域名数量,也不指定各级别域名的具体含义。各级域名由其上级域名管理机构负责管理,顶级域名则由 ICANN 统一管理。这种设计确保了每个域名在全球互联网中的唯一性,并便于构建域名查找机制。

图 5-1 展示了互联网域名体系的结构,它形似一棵倒置的树。树的顶端是根节点,但并没有具体的名称。紧接在根节点下方的一级节点,代表了最高级别的顶级域名。由于根节点本身无名,所以其直接下属的域名就被称作顶级域名。顶级域名可以继续向下划分,形成二级域名。随后,可以进一步细分为三级域名、四级域名等。

2. 域名服务器

域名服务器 DNS 是互联网中的核心组件,负责将易于记忆的域名转换为计算机能够识

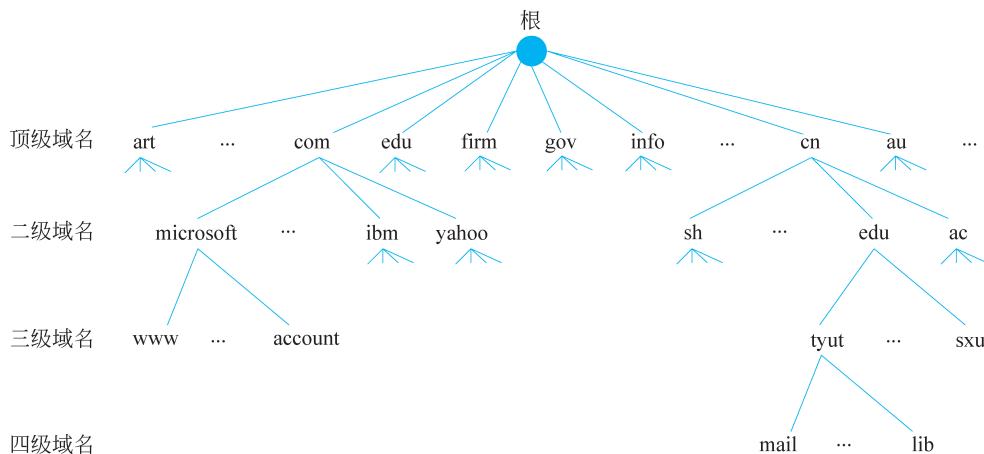


图 5-1 互联网域名体系的结构

别的 IP 地址。DNS 系统在互联网中按照层级结构组织。每个域名服务器负责管理域名体系中的特定部分。根据它们在系统中的功能,域名服务器可以分为以下四种主要类型。

(1) 根域名服务器(Root Name Server): 位于域名系统的最高层级,扮演着至关重要的角色。所有根域名服务器都存储着顶级域名服务器的域名和 IP 地址信息。无论哪个本地域名服务器,在解析互联网上的域名时,如果遇到无法直接解析的情况,都会首先向根域名服务器发起查询请求。

(2) 顶级域名服务器(Top-Level Domain, TLD Server): 该类服务器专门管理注册在其下的二级域名。当接收到 DNS 查询时,它们会提供相应的响应,它可能直接是查询结果,即域名对应的 IP 地址,或者指引查询者下一步应该联系的域名服务器的 IP 地址。

(3) 权威域名服务器(Authoritative Name Server): 该类服务器承担着存储特定域名的 DNS 记录,并提供官方认证信息的职责。当客户端发起域名解析请求,授权域名服务器将响应这些请求,提供与域名相关的详细信息。

(4) 本地域名服务器(Local Domain Name Server, LDNS): 这是用户或组织在网络内部部署的 DNS 服务器。它通常由互联网服务提供商(ISP)或企业网络管理员进行设置和配置,主要作用是为本网络内的用户设备提供域名解析服务,并且作为这些设备的首选 DNS 服务器。

为确保域名解析服务的稳定性,DNS 系统将数据在多个服务器上进行备份。其中,一个服务器作为主域名服务器(Master Name Server),负责存储和管理原始的 DNS 记录。其他服务器则作为辅助域名服务器(Secondary Name Server),用于数据备份。在主服务器发生故障时,辅助服务器能够接管服务,确保域名解析的连续性不受影响。主服务器会定期将更新后的 DNS 记录同步到辅助服务器,而所有数据的修改和更新只能在主服务器上执行,以此确保数据的准确性和一致性。

3. 域名解析过程

当主机需要查询域名对应的 IP 地址时,它会向本地域名服务器发起查询请求,这个过程通常采用如图 5-2(b)所示的递归查询的方式。递归查询的特点是:如果本地域名服务器没有存储所查询域名的 IP 地址信息,它将自动代表主机向其他上级 DNS 服务器进行查询,

而不需要主机自己进行进一步的查询操作。这种查询方式确保了主机不需要直接与多个 DNS 服务器交互,简化了查询流程。如果查询成功,本地域名服务器将返回所查询域名的 IP 地址给主机;如果查询失败,即无法找到对应的 IP 地址,本地域名服务器则会返回一个错误信息,告知主机无法解析所请求的域名。递归查询提高了查询效率,减少了主机在域名解析过程中的等待和网络通信开销。

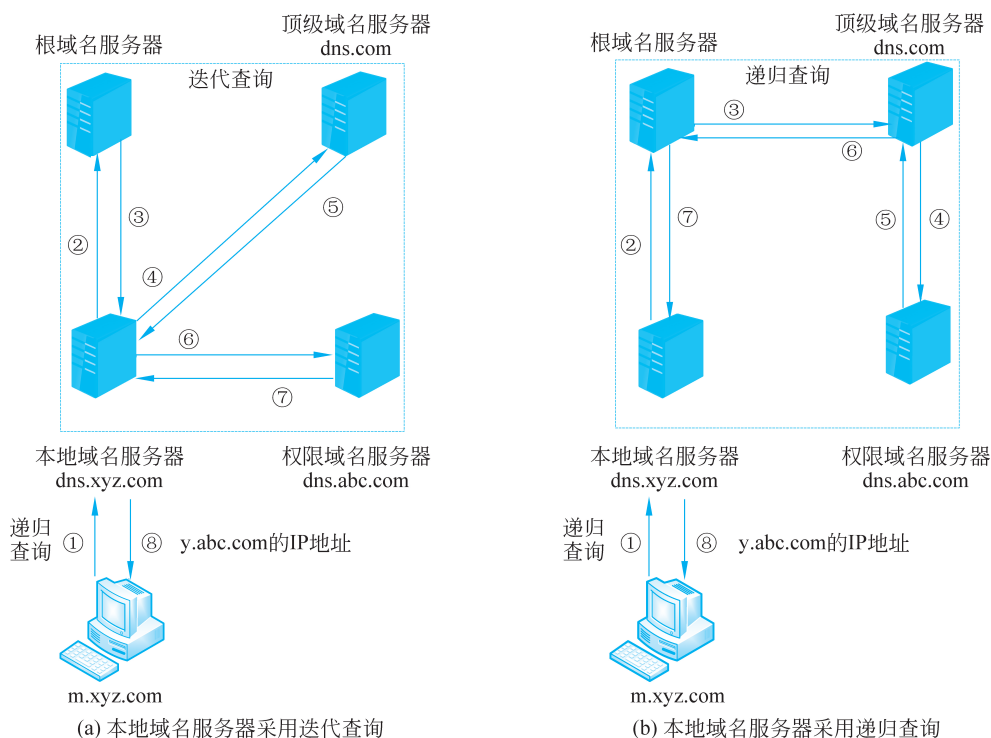


图 5-2 DNS 查询举例

本地域名服务器在进行域名解析时,通常采用如图 5-2(a)所示的迭代查询的方式向根域名服务器发起请求。迭代查询的工作原理是:当根域名服务器接收到来自本地域名服务器的迭代查询请求时,它将根据查询的域名提供相应的响应。如果根域名服务器拥有该域名的 IP 地址信息,它将直接返回这个 IP 地址;如果它没有这个信息,它将指导本地域名服务器下一步应该向哪个域名服务器发起查询。这种查询方式要求本地域名服务器在每次接收到根域名服务器或其他上级域名服务器的指引后,都要自行进行下一步的查询。根域名服务器一般会提供它所知的顶级域名服务器(TLD Servers)的 IP 地址,同理,当顶级域名服务器收到查询请求时,它也会根据情况提供 IP 地址或者指引本地域名服务器向相应的权限域名服务器(Authoritative Name Servers)进行查询。通过这一系列的迭代查询,本地域名服务器逐步深入查询过程,直到找到所要解析域名的 IP 地址,并将该结果传递回最初发起查询的主机。

图 5-2(a)描述了本地域名服务器在执行迭代 DNS 查询时的流程。在这个过程中,本地域名服务器通过连续三次迭代查询(步骤②~⑦),最终从权限域名服务器 dns.abc.com 获得了主机 y.abc.com 的 IP 地址。查询完成后,本地域名服务器将这一结果传递回最初发起查询的主机 m.xyz.com。整个查询流程共涉及 8 个 UDP 数据报,用于在服务器之间传递查

询请求和响应。图 5-2(b)展示了本地域名服务器在递归查询过程中的操作。在这种查询方式下,本地域名服务器仅需向根域名服务器发起一次查询请求。随后的查询操作则在其他域名服务器之间依次进行(步骤③~⑥)。在步骤⑦,本地域名服务器从根域名服务器获取了所需的正确地址信息。最终,在步骤⑧,本地域名服务器将查询结果反馈给主机 m.xyz.com。整个查询过程共使用了 8 个 UDP 数据报。

5.2.2 DNS 报文格式

DNS 报文是 DNS 协议中传输数据的基本单元,用于在客户端和 DNS 服务器之间传递查询请求和响应信息。DNS 报文的结构设计确保了其高效性和灵活性,如图 5-3 所示。该报文的前六个字段,即事务 ID(ID)、标志(Flags)、问题数(QDCOUNT)、回答资源记录数(ANCOUNT)、授权资源记录数(NSCOUNT)和额外资源记录数(ARCOUNT),每个字段的长度固定为 2 字节,这部分总共占用 12 字节。后四个字段,即问题区、答案区、权威区和附加信息区的记录数,它们的长度是可变的,取决于报文中实际包含的资源记录的数量和类型。

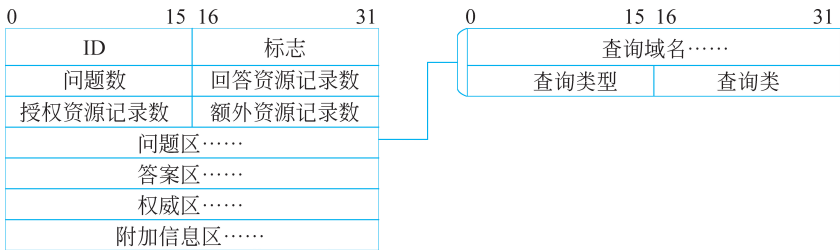


图 5-3 DNS 报文格式

DNS 报文中的四个数量指示字段分别对应报文的四个主要区域,每个区域都可能包含零个或多个资源记录,具体如下。

(1) 问题区(Question Section): 这是报文的起始部分,由查询者提供,包含以下三个基本元素。

- ① 查询域名(QNAME): 用户希望查询的域名。
- ② 查询类型(QTYPE): 指定查询的资源类型,例如 A 记录、MX 记录等。
- ③ 查询类(QCLASS): 指定查询的类别,通常为 IN,代表 Internet。

(2) 答案区(Answer Section): 这个区域通常出现在响应报文中,包含对问题区提出查询的回答。资源记录的形式与查询请求相对应,提供了查询域名的 IP 地址或其他相关信息。

(3) 权威区(Authority Section): 此区域也主要出现在响应报文中,它包括与查询域相关的权威域名服务器的信息。这些信息对于确定查询结果的权威性和进行进一步的查询非常重要。

(4) 附加信息区(Additional Information Section): 这个区域提供了与问题直接相关的一些额外信息,例如,如果查询是关于邮件服务器的 MX 记录,附加信息区可能包含指向的邮件交换服务器的 A 记录。

在 DNS 响应报文中,这四个区域共同工作,提供查询所需的全部信息,确保客户端能够

获得详尽的响应。问题区是每个 DNS 查询报文必须包含的部分,而后三个区域则根据查询的类型和响应的需要而出现。

5.2.3 DNS 报文分析

本节以访问“太原理工大学”的首页为例,采用 Wireshark 软件分析 DNS 查询报文和响应报文的构成。首先,假设主机 A 已经配置了 IP 地址 192.168.135.143,子网掩码为 24 位(即 255.255.255.0),而 DNS 服务器的 IP 地址配置为 192.168.135.141,同样使用 24 位子网掩码。请注意,实际的 IP 地址和其他配置信息可能会根据用户的网络环境而有所不同。接下来,在主机 A 上运行 Wireshark 软件,并设置一个捕获过滤器,过滤条件设置为“udp port 53”,以便只捕获 UDP 在 53 端口上的数据包,这是 DNS 协议默认使用的端口。启动数据包捕获后,在另一个命令提示符窗口中输入“nslookup www.tyut.edu.cn”命令,以发起对“太原理工大学”首页域名的 DNS 查询。查询完成后,立即停止 Wireshark 的捕获。最后,对 Wireshark 捕获到的数据包进行详细分析,以了解 DNS 查询和响应过程中的报文结构和信息传递。

1. DNS 查询报文分析

如图 5-4 所示,序号为 7 的数据包是由客户端发起的一个 DNS 查询请求,该请求被封装在 UDP 数据报中进行传输。此 UDP 数据报的目标端口设置为众所周知的 53 号端口,这是 DNS 协议进行通信的标准端口。该查询报文由报文首部和问题部分两部分组成,具体分析如下。

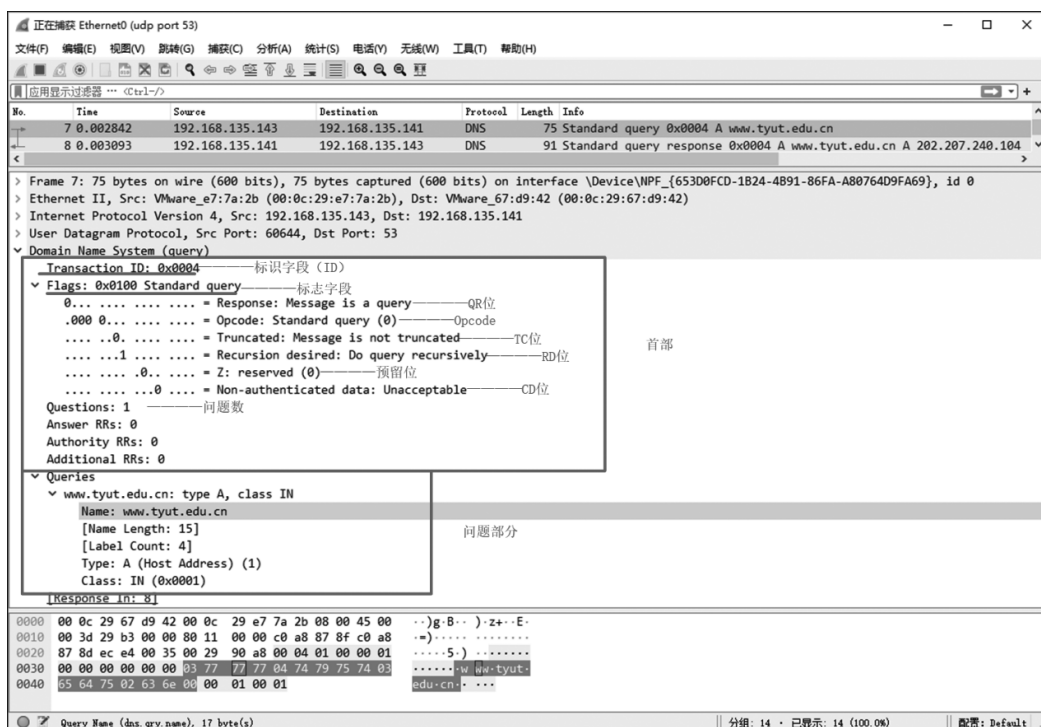


图 5-4 DNS 查询报文



(1) 首部分析。

① 标识字段：其值是 0x0004，用于唯一标识这个查询请求。

② 标志字段：包含多个比特位，其中：

- QR 位：值为 0，表明这是一个查询报文而非响应报文。
- Opcode：值为 0000，代表了一个标准查询操作，意味着客户端正在请求将域名解析为 IP 地址。
- TC 位：值为 0，表示该 DNS 报文没有被截断，即报文完整且没有超出 UDP 数据报的最大长度限制。
- RD 位：值为 1，指示 DNS 服务器应尝试进行递归查询，即服务器应尽力一次性解决查询请求，而不是提供引用或额外信息让客户端进行进一步查询。
- CD 位：值为 0，表示客户端没有要求服务器进行 DNSSEC（域名系统安全扩展）验证，即客户端不要求对响应进行安全性校验。

③ 四个数量标识字段：问题数为 1，表明客户端提出了一个查询请求。由于这是一个查询报文，回答资源记录数、授权资源记录数和额外资源记录数均为 0，表示这些部分在查询报文中不存在记录。

(2) 问题部分。

问题部分由一条问题记录构成，它详细说明了客户端所提出的查询请求。在该例子中，查询域名字段明确指出了需要解析的域名是 `www.tyut.edu.cn`。类型字段的值设置为 1，这表示查询的是 A 记录，即用于将域名转换为 IPv4 地址的资源记录类型。类字段同样被设置为 1，这指定了查询是在因特网上进行的，因为 1 代表 IN 类，即 Internet 类。这种设置确保了查询请求将在因特网的 DNS 系统中进行解析。

2. DNS 响应报文分析

如图 5-5 所示，序号 8 的数据包是由 DNS 服务器向客户端发送的 DNS 响应报文，该响应报文同样封装在 UDP 数据报中进行传输。此 UDP 数据报的源端口同样使用的是众所周知的 53 号端口，这是 DNS 协议通信的标准端口。响应报文包含首部、问题部分和回答部分，具体分析如下。

(1) 首部分析。

① 标识字段：其值是 0x0004，这个值与原始查询报文中的标识字段相匹配，确保响应能够正确关联到对应的查询请求。

② 标志字段：包含多个比特位，其中：

- QR 位：其值为 1，表明这是一个 DNS 响应报文。
- Opcode：其值为 0000，表明响应是针对一个标准查询操作，即查询请求是正向解析域名以获取 IP 地址。
- AA 位：其值为 0，表明提供响应的服务器不是权威服务器，也就是说，它可能不是最终解析域名的服务器。
- TC 位：其值为 0，表示响应报文完整，没有因为超过 UDP 数据报大小限制而被截断。
- RD 位：其值为 1，表明客户端请求服务器进行递归解析，即服务器应尽力一次性完成查询请求。

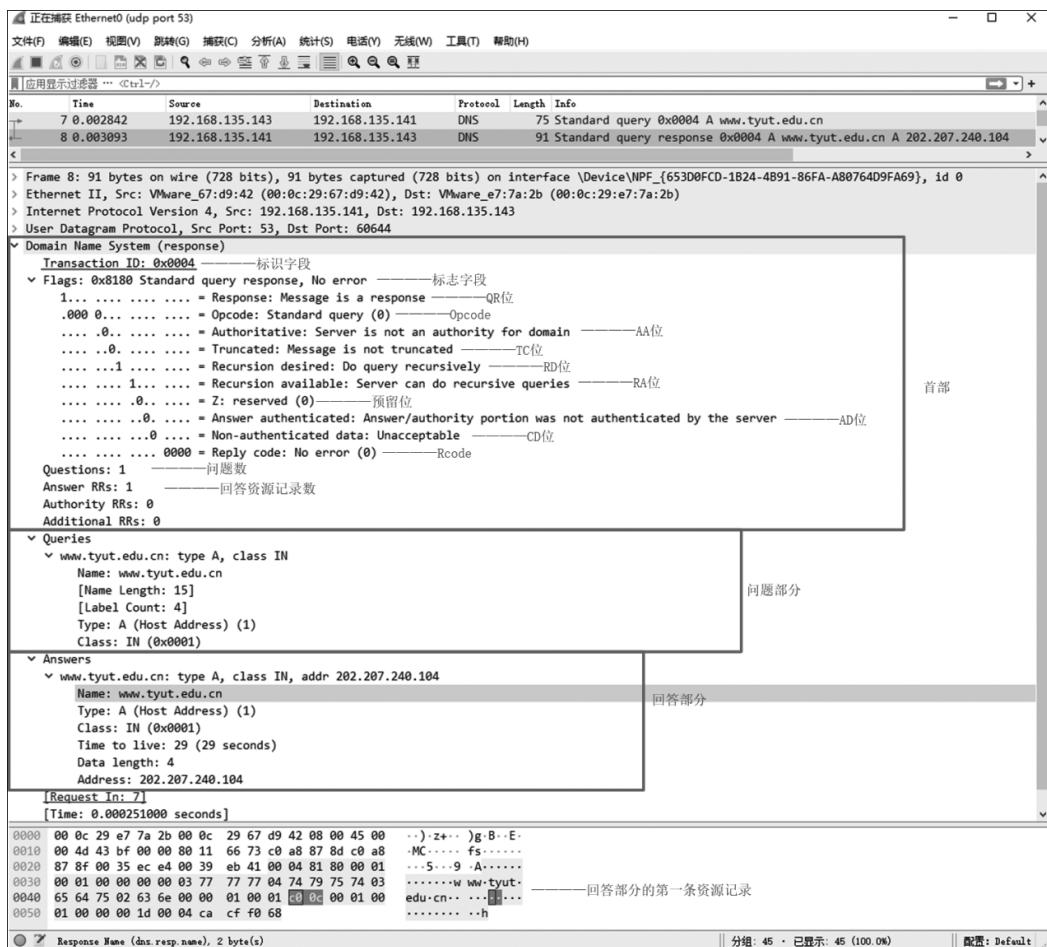


图 5-5 DNS 响应报文

- RA 位：其值为 1，表示服务器支持递归查询，即服务器能够代表客户端完成查询过程。
- AD 位：其值为 0，表示服务器在生成响应时没有对 DNSSEC 签名进行验证。
- RCode 位：其值为 0000，表示查询请求已被成功处理，没有遇到错误。

③ 四个数量标识字段：问题数为 1，表明报文中包含一个查询请求；回答资源记录数为 1，表明报文中包含一个回答该查询的资源记录；授权资源记录数和附加资源记录数的值均为 0，这可能意味着没有提供额外的权威信息或附加信息。

(2) 问题部分。

问题部分详细说明了查询的具体要求，包括要查询的域名、所需的资源类型以及查询的类别。这些信息与 DNS 查询报文中的相应部分具有相同的含义和目的。

(3) 回答部分。

在 DNS 响应报文中，各字段提供了关于资源记录的详细信息，以下是对这些字段的描述和分析。

① 域名字段：该字段的值是 0xC00C。转换成二进制表示为 1100000000001100。这里



的前两位“11”表明这是一个指针偏移值。接下来的 14 位(二进制的“00000000001100”)转换成十进制为 12,这意味着这个偏移指向问题部分中的某字节位置,从该位置开始的字节序列构成了域名“www.tyut.edu.cn”。

② 类型字段: 值为 0x0001,表明资源记录的类型是 A 记录,用于将域名映射到 IPv4 地址。

③ 类字段: 同样设置为 0x0001,表明查询和响应是在因特网类别中进行的。

④ 生存时间字段(TTL): 值为 0x001D,通常表示资源记录在 DNS 缓存中的有效时间为 29s。

⑤ 资源数据长度字段: 值为 0x0004,表明资源记录中的数据部分长度为 4 字节。

⑥ 资源数据字段: 包含一个 IPv4 地址,以十六进制表示为 0xCACFF068。转换为点分十进制形式,即域名“www.tyut.edu.cn”对应的 IP 地址是 192.207.240.104。

这些字段共同构成了 DNS 响应报文中的一个完整的资源记录,提供了域名到 IP 地址的映射信息,以及其他相关的记录元数据。

5.2.4 DNS 面临的安全威胁

DNS 作为互联网上最关键的服务之一,其安全性对于整个网络环境的稳定 and 用户数据的保护至关重要。然而,DNS 基于请求和响应的交互模式运行机制若被攻击者利用,通过篡改 DNS 响应,将域名的解析结果恶意指向攻击者控制的服务器或网站,就可能对用户造成严重的安全威胁。以下是 DNS 欺骗攻击的一些具体威胁细节。

1. 数据窃听和篡改

DNS 协议在传输过程中不加密,使得数据容易被截获和修改。由于 DNS 查询和响应通常使用 UDP,且 UDP 不保证数据包的完整性和安全性,攻击者可以轻易地通过网络嗅探工具捕获 DNS 流量,进而进行数据篡改,破坏数据的机密性和完整性。

2. ID 猜测和请求预测

攻击者通过预测技术构造假冒的响应。DNS 查询和响应报文中的 ID 字段用于匹配,且仅为 2 字节长,给攻击者提供了通过穷举法尝试 16384 种可能值来预测正确 ID 的理论机会。此外,尽管域名服务器通常监听 53 号端口,客户端端口号的随机性为预测增加了难度,但如果攻击者能预测客户端端口号,伪造响应的成功率将大大增加。在最坏情况下,攻击者可能需要尝试 65536 次(2^{16})来同时猜测 ID 和端口号。

3. 名字连锁攻击

名字连锁攻击,也称为 DNS 链式解析攻击,是一种利用 DNS 协议特性的复杂攻击手段。这种攻击可能依赖其他类型的 DNS 攻击,如 ID 预测和端口号猜测,来增加其成功率。名字连锁攻击依赖构造恶意的 DNS 资源记录,如 CNAME 和 NS 记录,这些记录通常用于指定域名的别名或权威域名服务器。攻击者通过在 DNS 响应的权威区或附加信息区插入这些构造的记录,企图使查询者的 DNS 缓存被错误信息充斥。当查询者执行 DNS 查询时,可能会被误导至攻击者控制的域名,进而可能遭受钓鱼攻击、恶意软件分发或其他形式的网络攻击。

4. 信任服务器背叛

DNS 客户端普遍设置有默认的域名服务器,这些服务器被客户端视为可信赖的来源以

解析域名。对于大多数用户来说,他们的 DNS 服务器配置往往来自互联网服务提供商 (ISP),在很多情况下,当用户使用 DHCP 自动获取网络配置时,ISP 会自动分配 DNS 服务器的地址。然而,如果 ISP 提供的 DNS 服务器遭受故障或被恶意攻击者掌控,攻击者就有可能利用这个信任关系的漏洞,向用户提供非法或错误的 DNS 响应。这种情形被称为信任服务器背叛,它为攻击者打开了进一步进行网络攻击的大门,例如,引导用户访问假冒的网站或分发恶意软件。

5. 否认域名的存在

当客户端发起 DNS 查询请求时,攻击者可能会采用策略来操纵响应,例如,通过发送一个表明查询失败的响应,或者在响应中故意省略某些资源记录。这种做法可以误导客户端,使其认为所查询的域名不存在,这种攻击方式被称为拒绝服务攻击 (DoS) 或域名存在性否认攻击。这种手段可能被用来隐藏网络资源的真实位置,妨碍正常的网络导航和通信。

6. 通配符

DNS 协议支持使用星号 (*) 作为通配符,以简化对多个子域名的统一管理。例如,如果定义了一个如下的 MX 记录:

```
*.example.com.      IN      MX      10      mailserver.example.com.
```

该条记录表示所有子域名如 a.example.com、b.example.com、c.example.com 等的电子邮件都将被路由至 mailserver.example.com 进行处理。这种使用通配符的方法虽然提高了配置的灵活性和效率,但也引入了一定的不确定性,因为它允许对任意子域名的邮件流量进行统一的指向。这不仅可能隐藏邮件流量的真实来源,还可能使得对邮件来源的验证变得更加复杂,增加了邮件欺诈和钓鱼攻击的风险。

5.2.5 常见的 DNS 攻击

常见的 DNS 攻击方式、攻击原理及攻击后果如表 5-1 所示。

表 5-1 DNS 攻击对比分析

攻 击 方 式	攻 击 原 理	攻 击 后 果
DNS 欺骗	修改 DNS 缓存、劫持 DNS 请求	网络钓鱼、信息窃取
DNS 隐蔽信道	利用 DNS 数据包封装信息	发送恶意指令,窃取隐私信息
DNS DDoS 攻击	直接耗尽服务器带宽资源	丧失网络服务能力
DNS 反射放大攻击	间接耗尽服务器带宽资源	丧失网络服务能力
恶意 DGA 域名	使用 DGA 生成大量恶意域名	存在大量恶意域名,破坏安全性

1. DNS 欺骗

DNS 欺骗,也被称为域名劫持,是一种网络攻击手段,它通过篡改用户请求的域名对应的 IP 地址,将用户引导到一个伪造的、恶意的网站。这种攻击可以让用户在不知情的情况下泄露个人信息。DNS 欺骗通常通过两种主要方式实施: DNS 缓存中毒和 DNS 信息劫持。这些攻击手段可以导致用户被误导至钓鱼网站,从而增加信息被盗取的风险。

在如图 5-6(a)所示的 DNS 缓存中毒攻击中,攻击者通过非法手段篡改 DNS 服务器的缓存记录,将合法域名本应指向的 IP 地址更改为一个恶意 IP 地址,诱使用户访问到一个仿