DHCP 安全问题及其防范措施研究

王舒艳

（山东协和学院　山东 济南　250107）

摘要：随着网络接入用户数量的增加，静态 IP 地址资源紧缺，已无法满足网络接入需求。动态主机配置协议 DHCP 为用户的上网提供了极大的便利，也为负责 IP 地址分配的网络管理员减轻了负担。本文的主要介绍了 DHCP 系统工作原理，分析了 DHCP 中继工作方式，针对 DHCP 存在的安全问题，分析了各种攻击行为，并引用了 DHCP Snooping 防范技术应对攻击，以确保用户的网络安全。

关键词：IP 地址；DHCP；网络安全

1 研究背景和意义

1.1 研究背景

当前时代网络已成为生活中不可或缺的一大部分，也是企业重要的生产工具之一。网络管理是构成大型计算机网络的重要因素。传统的手工静态分配网络参数方法需要每个用户都手动配置 IP address，subnet mask、gateway 以及 DNS 等多个参数。手动修改效率低下，加上有些新手技术操作水平不高，配置不够灵活导致现在的状况已经无法满足需求。为了解决上述手工静态分配网络参数的问题，出现了动态主机配置协议 DHCP（Dynamic Host Configuration Protocl），实现可动态分配网络参数，达到 IP 地址资源利用最大化

1.2 研究意义

分析 DHCP 的安全漏洞，找到应对方法，维护 DHCP 的正常运作。同时也为个人日后的发展打下一定的基础，如果能保证 DHCP 的安全，对于企业的网络安全将会有重大的意义。

2 DHCP 技术

DHCP 是动态主机配置协议,主要应用于给局域网内的主机动态分配 IP Address 的网络参数。

2.1 DHCP 工作原理

DHCP 是一个局域网的网络协议。传输配置参数由主要由两部分信息组成：一是传送专用的配置信息给网络主机；二是给主机分配网络地址。DHCP 的组成结构是基于 Client/Server 的，具有三种 DHCP 支持 IP 地址分配方法： 一是自动分配 IP 方式，没有时间的限制，一旦有用户成功获取到 IP 地址，那么 DHCP 将永久的把这个 IP 地址分配给该用户。二是动态分配 IP 方式，有时间限制，用户可在 DHCP server 获得一个有租约期限的 IP Address，期限一到便要归还。三是手工分配 IP 方式，管理员指定好一个 IP Address 给某一个用户，其他用户无法获取这个 IP；在这种情况下，DHCP Server 会将这个指定好的 IP Address 传送到给用户。

2.2 DHCP 中继

DHCP 中继又叫 DHCP Relay，可以实现在不同子网和物理网段之间处理和转发 DHCP 信息的功能。用 DHCP Relay 代理可以去掉在每个物理网段都要有 DHCP 服务器的必要,它可以传递消息到不在同一个物理子网的 DHCP 服务器，也可以将服务器的消息传回给不在同一个物理子网的 DHCP 客户机。

3 DHCP 面临的安全威胁

网络攻击行为无处不在，针对 DHCP 的攻击行为也不例外。例如，某公司突然出现了大面积用户无法上网的情况，经检查用户终端均未获取到 IP 地址，且 DHCP Server 地址池中的地址已经全部被分配出去了，这种情况很有可能就是 DHCP 受到了某种攻击而导致的。实际网络中,针对 DHCP 的攻击行为主要有以下三种：一是 DHCP 饿死攻击；二是仿冒 DHCP Server 攻击；三是 DHCP 中间人攻击。

3.1 DHCP 饿死攻击

DHCP 饿死攻击，指攻击者通过持续大量地向 DHCP Server 发送申请 IP 地址的消息，直到地址池中的 IP 地址会被申请耗尽时，DHCP Server 将没有剩余 IP 地址分配给正常的用户使用。

3.2 仿冒 DHCP Server 攻击

DHCP Server 程序被攻击者私自安装并运行后，攻击者便可以把自己乔装成一个合法的 DHCP Server，所谓的仿冒 DHCP Server 也就是这样形成的。仿冒 DHCP Server 与合法的 DHCP Server 在工作原理上是完全一样的，而不同的部分是，错误的 IP 地址及提供错误的网关地址等参数会被仿冒 DHCP Server 向客户端分配，会导致客户端不能正常地访问网络。

3.3 DHCP 中间人攻击

攻击者利用 ARP 机制，使所有经过它的往来于 PC-A 与 DHCP Server 之间的 IP 报文进行中转，这些 IP 报文中的某些信息很容易被攻击者窃取，并且其他的破坏行为会基于 IP 报文中的某些信息进行。往来于 PC-A 与 DHCP Server 之间的 DHCP 消息（这些消息是封装在 UDP 报文中的，而 UDP 报文又是封装在 IP 报文中的）很容易被攻击者进行篡改，达到直接攻击 DHCP 的目的。

4 防范措施

为了增强网络安全，防止 DHCP 受到攻击，DHCP Snooping 的技术应运而生。DHCP Snooping 部署在交换机上，其作用类似于在 DHCP 客户端与 DHCP 服务器端之间构筑了一道虚拟的防火墙。

4.1 DHCP Snooping 技术

交换机开启 DHCP Snooping 目的是对来往 DHCP 报文进行侦听，并可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息的对应关系，通过建立或维护的 DHCP Snooping 绑定表过滤不被信任的 DHCP 消息，绑定表信息包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息。

4.2 工作过程

4.2.1 防止 DHCP 饿死攻击

为了解决 DHCP 饿死攻击这个风险极大的漏洞，抵挡饿死攻击，在 DHCP Snooping 技术支持下，DHCP Request 报文的源 MAC 地址与 CHADDR 会在端口下会被进行一致性检查。如果二者相同，则转发报文；如果二者不相同，则丢弃。如果要在某端口下一致性检查施源 MAC 地址与 CHADDR，可以在该端口下使用命令 dhcp snooping check dhcp-chaddr enable。

4.2.2 防止仿冒 DHCP Server 攻击

交换机上的端口被 DHCP Snooping 分为两种类型，也就是 Trusted 端口和 Untrusted 端口；与合法的 DHCP Server 相连接的端口应配置为 Trusted 端口，其他端口应配置为 Untrusted 端口。

例如 DHCP Offer 报文、DHCP Ack 报文等等，这些 DHCP 响应报文会被交换机从 Trusted 端口接收到，会转发这些报文，从而保证 IP 地址及提供其他网络参数可以被合法的 DHCP Server 正常地分配；如 DHCP Offer 报文、DHCP Ack 报文等等，这些 DHCP 响应报文被交换机从 Untrusted 端口接收到，会丢掉这些报文，从而阻止 IP 地址及提供其他网络参数被仿冒的 DHCP Server 进行分配。

4.2.3 防止 DHCP 中间人攻击

DHCP 中间人攻击，实质是一种 Spoofing IP/MAC 攻击。要想阻止 DHCP 中间人攻击，其实就是要阻止 Spoofing IP/MAC 攻击。运行

（下转第 115 页）

（上接第 124 页）
了 DHCP Snooping 的交换机会“侦听（Snooping）”往来于用户与 DHCP Server 之间的 DHCP 消息，并从中收集用户的 MAC 地址（这里的 MAC 地址是指 DHCP 消息中 CHADDR 字段的值）、用户的 IP 地址（这里的 IP 地址是指 DHCP Server 分配给相应 CHADDR 的 IP 地址）等信息，这些信息会集中存放在一个数据库中，该数据库也被称为 DHCP Snooping 绑定表。运行了 DHCP Snooping 的交换机会建立并动态维护 DHCP Snooping 绑定表，绑定表中除了包含了用户的 MAC 地址、用户的 IP 地址外，还包括 IP 地址租用期、VLAN-ID 等等信息。

5 结束语

虽然 DHCP 技术有很大的安全隐患，但是它的自身优势远远大于它的缺点，所以 DHCP 技术才会在网络中已经被广泛应用。本文重点论述了 DHCP 技术，及提出其面临的安全问题，并且分析了 DHCP Snooping 技术，如何利用该技术实现对 DHCP 服务器的保护。基于 DHCP 中继和 DHCP Snooping 的安全特性也为接入层设备防止常见的二层攻击提供了优秀的解决方案。

参考文献：

[1]李泰.计算机网络安全问题及其防范措施研究[J].通讯世界,2019,26(09):183-184.

[2]卢翔,徐小杰.浅析计算机网络安全问题及其防范措施[J].中国新通信,2020,22(05):129.

[3]李军军.计算机网络安全问题及其防范措施[J].网络安全技术与应用,2018(11):1+3.

作者简介：王舒艳(1984-），女，菏泽人，副教授，硕士，主要研究方向网络工程。