****

网络安全理论与技术实验

实 验 报 告

|  |  |
| --- | --- |
| **学 院** | 网络空间安全学院 |
| **专 业** | 网络工程 |
| **班 级** | 18272412 |
| **学 号** | 18041618 |
| **学生姓名** | 廖越强 |
| **教师姓名** | 高梦州 |
| **完成日期** | 2020.12.4 |
| **成 绩** |  |
| **实验一 钓鱼网站实验** | | |
| 1. **实验目的**   (1)验证伪造的DHCP服务器为终端提供网络信息配置服务的过程。  (2)验证错误的本地域名服务器地址造成的后果。  (3)验证利用网络实施钓鱼网站的过程。 | | |
| 1. **实验原理**   终端通过广播DHCP发现消息发现DHCP服务器,当DHCP服务器与终端不在同一个网络(同一个广播域)时,由路由器完成中继过程。DHCP服务器通过向终端发送DHCP提供消息表明可以为终端提供网络信息配置服务,终端选择发送第一个到达终端的DHCP提供消息的 DHCP服务器为其提供网络信息配置服务。  如图2.38所示,在终端连接的网络中接入伪造的 DHCP服务器后,终端广播的DHCP发现消息到达伪造的DHCP服务器,伪造的DHCP服务器在网络中广播DHCP提供消息,由于伪造的DHCP服务器与终端位于同一网络,伪造的DHCP服务器发送的DHCP提供消息可能先于 DHCP服务器发送的 DHCP提供消息到达终端，导致终端选择伪造的DHCP服务器为其提供网络信息配置服务﹐并将伪造的DNS服务器的IP地址192.1.3.1作为本地域名服务器地址。 | | |
| 1. **实验环境/实验拓扑图** | | |
| 1. **主要操作步骤及实验结果记录** 2. 完成拓扑图连接      1. 配置路由器接口IP地址和掩码，完成路由器RIP配置   router1路由表    router2路由表     1. 完成router1接口fastethernet0/0的中继地址配置      1. 完成3台服务器的IP地址、子网掩码和默认网关的配置          1. 开启DHCP服务器的“DHCP”功能，并配置      1. 配置DNS服务器，并添加记录      1. 配置pc0，使用DHCP模式      1. 使用pc0通过域名访问web server      1. 接入3台伪造的服务器，并完成其IP、子网掩码、默认网关的配置     伪造的DHCP配置    伪造的DNS服务器配置    伪造的Web服务器配置    使用pc0再次使用DHCP获取地址，可见DNS Server变成了192.1.3.1，表明从伪造的DHCP服务器获取网络信息     1. 使用pc0访问伪造的web Server | | |
| 1. **实验分析总结及心得** 2. **命令列表**   ip helper-address address一是配置DHCP服务器的IP地址,二是启动接口的 DHCP中继功能。参数address给出DHCP服务器的IP地址   1. **总结心得**   配置DHCP配完后记得点save，直接退出的话，配置是不会生效的。  通过这次实验，我对DHCP这方面的安全知识有了新的认识，对黑客利用DHCP服务器接入网络的攻击流程有了一个的清晰的认识。也对通过DHCP获取网络信息这个概念有了更深入的理解，意识到了需要对DHCP进行一些防护，提高网络防护安全，提高了自己的安全意识。 | | |

|  |
| --- |
| **实验一 防DHCP欺骗攻击实现** |
| 1. **实验目的**   (1)验证DHCP服务器配置过程。  (2)验证 DNS服务器配置过程。  (3)验证终端用完全合格的域名访问Web服务器的过程。  (4)验证DHCP欺骗攻击过程。  (5)验证钓鱼网站实施过程。  (6)验证交换机防DHCP欺骗攻击功能的配置过程。 |
| 1. **实验原理**   终端通过DHCP自动获取的网络信息中包含本地域名服务器地址,对于如图4.7所示的网络应用系统,DHCP服务器中给出的本地域名服务器地址是192.1.2.7,地址为192.1.2.7的域名服务器中与完全合格的域名www.bank.com 绑定的Web服务器地址是192.1.3.7。因此,终端可以用完全合格的域名www.bank.com 访问Web服务器。  一旦终端连接的网络中接入伪造的DHCP服务器,终端很可能从伪造的DHCP服务器获取网络信息,得到伪造的域名服务器的IP地址192.1.3.1 ,伪造的域名服务器中将完全合格的域名www.bank.com与伪造的Web服务器的IP地址192.1.2.5绑定在一起,导致终端用完全合格的域名www.bank.com访问伪造的Web服务器。  如果交换机启动防DHCP欺骗攻击的功能,只有连接在信任端口的 DHCP服务器才能为终端提供自动配置网络信息的服务。因此,对于如图4.7所示的实施DHCP欺骗攻击的网络应用系统,连接终端的以太网中,如果只将连接路由器Rl的交换机端口设置为信任端口,将其他交换机端口设置为非信任端口,则终端只能接收由路由器Rl转发的DHCP消息﹐使终端只能获取DHCP服务器提供的网络信息。 |
| 1. **实验环境/实验拓扑图** |
| 1. **主要操作步骤及实验结果记录** 2. 使用第2.5节的拓扑图      1. 启动交换机switch0防DHCP欺骗攻击的功能前，pc0很可能从伪造的DHCP服务器获取网络信息，如图。      1. 在switch0 CLI下启动交换机防DHCP欺骗攻击的功能     再使用pc0、pc1、pc2通过DHCP获取网络信息，可从正确的DHCP处得到网络信息，DHCP地址为192.1.2.7        使用pc0访问[www.bank.com](http://www.bank.com)域名，访问到正确的Web Server，如图     1. 显示switch0的DHCP侦听信息库，得到三者的绑定关系：pc的mac地址、DHCP分配给pc的IP地址和Switch0连接pc的交换机接口 |
| 1. **实验分析总结及心得** 2. **命令列表** 3. **ip dhcp snooping**   启动DHCP侦听功能   1. **ip dhcp snooping vlan vlan-range**   针对一个或一组 VLAN启动DHCP侦听功能。参数vlan-range可以是单个VLAN ID,或是多个用逗号分隔的VLAN ID,或是一组连续的VLAN ID   1. **ip dhcp snooping trust**   将交换机端口设置为信任端口   1. **show ip dhcp snooping binding**   显示DHCP侦听信息库中的内容,即 MAC地址,IP地址和交换机端口之间的绑定关系   1. **总结**   通过这次实验，我对DHCP这方面的安全知识有了新的认识，学会了防御伪造的DHCP服务器接入网络的基本操作，对它们的攻击流程有了一个的深刻的认识。也对通过DHCP获取网络信息这个概念有了更深入的理解，明白了做好DHCP防御，提高网络防护的重要性，提高了自己的安全意识。 |