·实验技术·

基于 eNSP、VirtualBox 和 Kali 的 DHCP 多层次闯关实验设计

贾　楠，石　磊，郭静霞，徐　立，白金牛*

（内蒙古科技大学 包头医学院，包头 014040）

摘要：动态主机配置协议(DHCP)是管理和分配 IP 地址的协议，在企业网中广泛使用。针对学生在学习过程中缺乏动手实践能力的训练以及计算机网络设备硬件有限的问题，提出了一种综合使用 eNSP、VirtualBox、Kali 软件搭建 DHCP 多层次实验项目。实验项目的设计涵盖了常见 DHCP 服务器的配置、DHCP 中继、DHCP 攻击与防御方面的内容。通过本实验项目的设计能够提升学生的网络工程实践能力，方便教师开展线上教学，提升教学质量。

关　键　词：动态主机配置协议；eNSP；VirtualBox；Kali

中图分类号：TP391.9　　**文献标志码：**A　　DOI: 10.12179/1672-4550.20220659

Design of DHCP Multi-level Experiment Based on eNSP, VirtualBox and Kali

JIA Nan, SHI Lei, GUO Jingxia, XU Li, BAI Jinniu*

（Baotou Medical College, Inner Mongolia University of Science and Technology, Baotou 014040, China）

Abstract: Dynamic host configuration protocol (DHCP) is a protocol for managing and assigning IP addresses and is widely used in enterprise networks. Considering the problems of students' lack of practical ability and the limited hardware of computer network equipment in the learning process, this paper proposes a kind of integrated use of eNSP, VirtualBox and Kali software to build a DHCP multi-level experimental project. The design of the experiment project covers the configuration of common DHCP servers, DHCP relay, and DHCP attack and defense. The design of this experimental project can improve students' practical ability of network engineering, facilitate teachers to carry out online teaching, and improve teaching quality.

Key words: DHCP; eNSP; VirtualBox; Kali

DHCP 是计算机网络应用层中的重点内容，它能实现自动分配 IP 地址、网关、子网掩码等信息，提升地址的使用效率[1−3]。为了使学生深入地掌握该部分内容，同时具备 DHCP 工程实践能力，以符合新工科背景下对人才培养的要求[4−6]，本文将通过 3 款 eNSP、VirtualBox、Kali Linux 软件构建 DHCP 实验项目。eNSP 是华为公司开发的免费的、可扩展的、图形化计算机网络仿真平台，它可以模拟 PC、交换机、路由器、无线设备、防火墙等设备[7−10]。VirtualBox 是甲骨文公司的一款开源虚拟机软件，它能够很好地和 eNSP 适配实现对真实服务器的模拟[11−12]。Kali Linux 是一种基于 Debian 的 Linux 发行版，通常应用在高级渗透测试和安全审计场景中。Kail Linux 系统中内置了数百种工具，适用于各种信息安全任务，如渗透测试、安全研究、计算机取证和逆向工程[13−15]。利用以上 3 款软件可以搭建非常丰富且有深度的 DHCP 实验，缓解部分高校实验设备有限、学生缺乏动手实践的问题。

1　DHCP 实验设计

本文设计了 3 个层次的 DHCP 实验项目，由

收稿日期：2022−11−20；**修回日期：**2024−01−12

基金项目：内蒙古自然科学基金(2023QN06007)；内蒙古自治区高等学校科学研究项目(NJZY22050)；包头医学院“问学计划”“为学计划”“践学计划”研究项目(2023BYWWJ-YB-12)；包头医学院研究基金(BYJJ-ZRQM202206)。

作者简介：贾楠(1984−)，男，硕士，讲师，主要从事计算机网络与医学大数据处理方面的研究。

***通信作者：**白金牛(1967−)，男，硕士，教授，主要从事计算机网络与人工智能方面的研究。E-mail: baijinniu@163.com

简入难分别为初窥门径、登堂入室、小有所成。

1）初窥门径阶段即 DHCP 服务器和客户机在同一广播域内，该阶段包含 3 个实验，分别是利用 eNSP 中的路由器作为 DHCP 服务器(细分为全局地址池和接口地址池)，以及利用 VirtualBox 搭建 Windows Server DHCP 服务器，然后将其接入 eNSP 虚拟网络中。该阶段实验较为简单，通过该阶段实验让学生明白 DHCP 工作过程即报文交互的 4 个阶段——发现阶段、提供阶段、选择阶段、确认阶段，使学生掌握基本的 DHCP 配置，筑牢基础。

2）登堂入室阶段即 DHCP 服务器和客户机不在同一广播域，该阶段包含两个实验(路由器作为 DHCP 服务器和 Windows Server 作为 DHCP 服务器)，这两个实验相较于前一阶段的实验更贴近现实应用场景。该阶段实验使学生掌握 DHCP 中继概念以及 DHCP 中继相关配置，提升学生动手能力。

3）小有所成阶段即 DHCP 攻击与防御，该阶段设计了两个常见的 DHCP 攻击与防御实验，一个是 DHCP Sever 仿冒攻击，另一个是 DHCP 饿死攻击。为了演示 DHCP 饿死攻击，搭建了 Kali Linux 服务器，让学生掌握 DHCP Snooping 的功能和相关配置，该实验能够极大地提升学生的学习兴趣，因为大部分学生对黑客技术充满好奇。3 个阶段的详细实验方案、配置代码以及实验结果介绍如下。

2　DHCP 实验实现与验证

2.1　DHCP 服务器与客户机在同一广播域(初窥门径)

[实验 1]

将路由器 R1 作为 DHCP 服务器，使用 R1 的接口 G0/0/0 所在网段作为 DHCP服务器的地址池，并且将该接口地址作为 DHCP Server 地址，租期设置为 8 天，最终实现 PC1 自动获得 IP 地址，实验拓扑如图 1 所示。

图 1　DHCP 接口地址池拓扑图

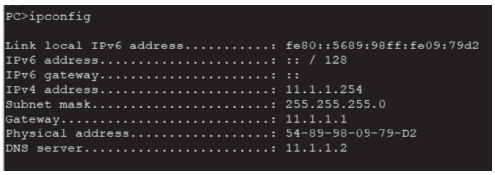
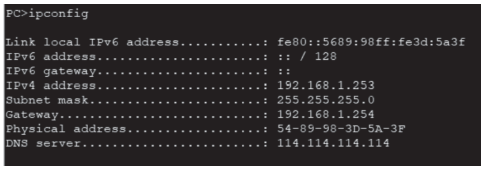
[实验 2]

将路由器 R2 作为 DHCP 服务器，配置全局地址池 192.168.1.0/24，排除 IP 地址 192.168.1.10，网关为 192.168.1.254，DNS 为 114.114.114.114，租期设置为 8 天，最终实现 PC2 自动获得 IP 地址，实验拓扑如图 2 所示。

图 2　DHCP 全局地址池拓扑图

详细实验配置以及实验结果如表 1 所示。

表 1　实验 1、实验 2 核心配置与实验结果

实验项目	核心配置	实验结果
实验1	dhcp enable interface GigabitEthernet0/0/0 　ip address 11.1.1.1 255.255.255.0 　dhcp select interface 　dhcp server excluded-ip-address 11.1.1.2 　dhcp server lease day 8 hour 0 minute 0 　dhcp server dns-list 11.1.1.2	
实验2	dhcp enable ip pool dhcp1 　gateway-list 192.168.1.254 　network 192.168.1.0 mask 255.255.255.0 　excluded-ip-address 192.168.1.10 　lease day 8 hour 0 minute 0 　dns-list 114.114.114.114 interface GigabitEthernet0/0/0 　ip address 192.168.1.1 255.255.255.0 　dhcp select global	

[实验 3]

用 VirtualBox 构建一台 Windows Server 虚拟机作为 DHCP 服务器，将其 IP 地址设置为 192.168.2.2/24，DHCP 地址池范围为 192.168.2.10/24~192.168.2.200/24，默认网关为 192.168.2.254，DNS 为 192.168.2.2 和 114.114.114.114。通过 eNSP 中的

Cloud 设备将该 DHCP 服务器接入虚拟网络中，实现 PC3 自动获取 IP 地址，实验拓扑如图 3 所示。

图 3　Windows Server DHCP 服务器实验拓扑图

具体实现有以下 4 个步骤。

1）使用 VirtualBox 新建一台虚拟机，并安装 Windows Server 操作系统。

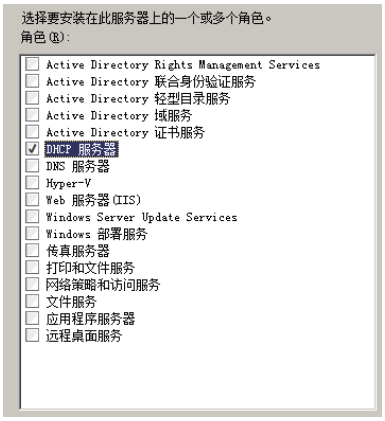
2）将网络设置为 VirtualBox Host-Only 模式，物理机上多出一块虚拟网卡 VirtualBox Host-Only Network，设置该网卡的 IP 地址为 192.168.2.1。

3）进行 Windows Server DHCP 服务器配置，具体步骤如下：

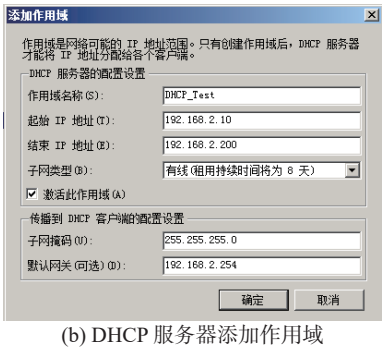
① 关闭防火墙，设置 DHCP 服务器 IP 地址；

② 安装 DHCP 服务器；

③ 新建 DHCP 作用域，并进行相关配置，如图 4 所示。



(a) DHCP 服务器安装



(b) DHCP 服务器添加作用域

图 4　Windows Server DHCP 服务器配置

4）在 eNSP 中的 Cloud 中添加 2 个端口，一个端口绑定信息为 UDP，一个端口绑定信息为 VirtualBox Host-Only Network(192.168.2.1)。Cloud 配置以及实验结果分别如图 5 和图 6 所示。

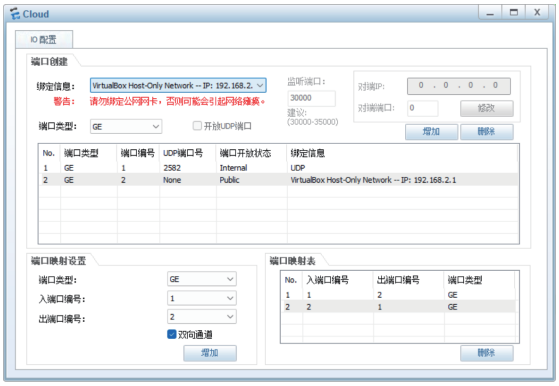


图 5　eNSP Cloud 配置

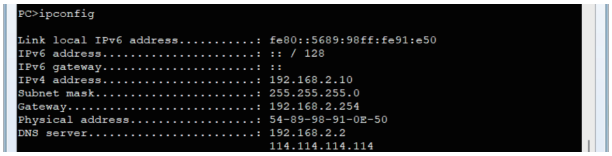


图 6　实验结果

2.2　DHCP 服务器与客户机在不同广播域(登堂入室)[实验 4]

1）将路由器 R3 作为 DHCP 服务器，配置全局地址池：

dhcp_vlan10，IP 范围为 192.168.10.0/24，网关为 192.168.10.254；

dhcp_vlan20，IP 范围为 192.168.20.0/24；网关为 192.168.20.254；

主 DNS 为 8.8.8.8，备用 DNS 为 114.114.114.114，租期设置为 8 天。

2）在交换机 LSW3 上创建 VLAN 10 和 VLAN 20 以及互连 VLAN 100，VLAN 10 的虚接口 IP 地址为 192.168.10.254，VLAN 20 的虚接口 IP 地址为 192.168.20.254，VLAN 100 的虚接口 IP 地址为 192.168.100.2；将 G0/0/1 口、G0/0/3 口分别划入 VLAN10 和 VLAN20；

3）最终实现 PC3 自动获取到 192.168.10.X/24 范围的地址，PC4 自动获取到 192.168.20.X/24 范围的地址，实验拓扑如图 7 所示。

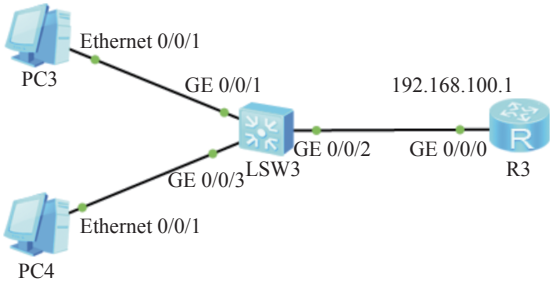


图 7　DHCP 中继(路由器作为 DHCP 服务器)拓扑图

[实验 5]

1）用 VirtualBox 构建一台 Windows Server 虚拟机作为 DHCP 服务器，将其 IP 地址设置为 192.168.56.2/24，创建 2 个作用域：

dhcp_vlan30，IP 范围为 192.168.30.0/24，网关为 192.168.30.254；

dhcp_vlan40，IP 范围为 192.168.40.0/24，网关为 192.168.40.254；

主 DNS 为 8.8.8.8，备用 DNS 为 114.114.114.114，租期设置为 8 天。

通过 eNSP 中的 cloud 设备将该 DHCP 服务器接入交换机 LSW4。

2）在交换机 LSW4 上创建 VLAN 30 和 VLAN 40 以及互连 VLAN 56，VLAN 30 的虚接口 IP 地址为 192.168.30.254，VLAN 40 的虚接口 IP 地址为 192.168.40.254，VLAN 56 的虚接口 IP 地址为 192.168.56.2；将 G0/0/1 口、G0/0/2 口分别划入 VLAN30 和 VLAN40。

3）最终实现 PC3 自动获取到 192.168.30.X/24 范围的地址，PC4 自动获取到 192.168.40.X/24 范围的地址。实验拓扑如图 8 所示。实验配置、实验结果如表 2 所示。

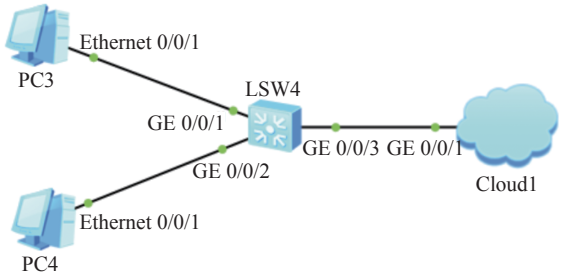


图 8　DHCP 中继(虚拟机做服务器)拓扑图

表 2　实验 4、实验 5 核心配置与实验结果

实验项目	核心配置	实验结果
实验4	#路由器R1配置： dhcp enable ip pool dhcp_vlan10 　gateway-list 192.168.10.254 　network 192.168.10.0 mask 255.255.255.0 #dhcp_vlan20地址池配置与dhcp_vlan10类似 interface GigabitEthernet0/0/0 　ip address 192.168.100.1 255.255.255.0 　dhcp select global ip route-static 192.168.10.0 255.255.255.0 192.168.100.2 ip route-static 192.168.20.0 255.255.255.0 192.168.100.2 #交换机LSW3配置： interface Vlanif10 　ip address 192.168.10.254 255.255.255.0 　dhcp select relay 　dhcp relay server-ip 192.168.100.1 #虚接口Vlanif20的配置与Vlanif10类似 interface Vlanif100 　ip address 192.168.100.2 255.255.255.0 interface GigabitEthernet0/0/1 　port link-type access 　port default vlan 10 #GigabitEthernet0/0/2与GigabitEthernet0/0/1配置类似	PC3： PC>ipconfig Link local IPv6 address.....: fe80::5689:98ff:feaa:6885 IPv6 address.....: :: / 128 IPv6 gateway.....: :: IPv4 address.....: 192.168.10.253 Subnet mask.....: 255.255.255.0 Gateway.....: 192.168.10.254 Physical address.....: 54-89-98-AA-68-85 DNS server.....: 8.8.8.8 114.114.114.114
实验5	WindowsServer服务器配置和前面类似，本项目需要建2个作用域；作用域[192.168.30.0] dhcp_vlan30、作用域[192.168.40.0] dhcp_vlan40 #交换机LSW4配置： interface Vlanif30 　ip address 192.168.30.254 255.255.255.0 　dhcp select relay 　dhcp relay server-ip 192.168.56.2 #虚接口Vlanif40配置与Vlanif30类似 interface GigabitEthernet0/0/1 　port link-type access 　port default vlan 10 #GigabitEthernet0/0/2、GigabitEthernet0/0/3的配置与#GigabitEthernet0/0/1类似	PC4： PC>ipconfig Link local IPv6 address.....: fe80::5689:98ff:fe84:3f9 IPv6 address.....: :: / 128 IPv6 gateway.....: :: IPv4 address.....: 192.168.40.1 Subnet mask.....: 255.255.255.0 Gateway.....: 192.168.40.254 Physical address.....: 54-89-98-84-03-F9 DNS server.....: 8.8.8.8 114.114.114.114

2.3　DHCP 攻击与防御(小有所成)

2.3.1　DHCP Server 仿冒攻击

DHCP 仿冒攻击是利用非法的 DHCP 服务器接入计算机网络中，导致正常的用户获取到错误的网络参数，对个人的信息安全及财产安全造成损失。

[实验 6]

1）将一台路由器作为 DHCP 服务器，配置全局地址池为 dhcp_vlan10，IP 范围为 192.168.10.0/24，网关为 192.168.10.254，DNS 地址为 8.8.8.8，租期设置为 8 天。

2）将另一台路由器作为 DHCP 仿冒服务器，配置全局地址池为 dhcp_vlan10，IP 范围为 192.168.10.0/24，网关为 192.168.10.253，DNS 地址为 1.1.1.1，租期设置为 8 天。

3）LSW5 为接入交换机，在该交换机上创建 VLAN 10，并将 e0/0/1、g0/0/1、g0/0/2 都划入 VLAN10；LSW6 为核心交换机，在该交换机上创建 VLAN 10 和 VLAN100 并创建其虚拟接口 192.168.10.254 和 192.168.100.2，将 g0/0/1 划入 VLAN10，将 g0/0/2 划入 VLAN100，实验拓扑如图 9 所示。

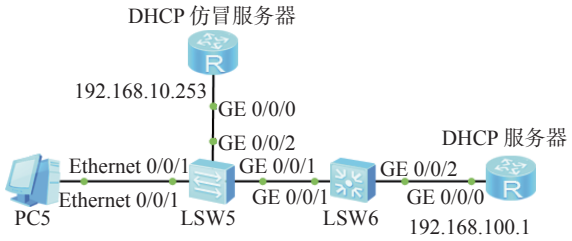


图 9　DHCP Server 仿冒攻击拓扑图

如果此时 DHCP 仿冒服务器没有接入，DHCP 服务器、LSW5、LSW6 参照前面 DHCP 中继实验的配置，PC5 可以正常获取到 DHCP 分配的 IP 地址及相关网络参数。但如果此时将 DHCP 仿冒服务器接入到交换机 LSW5 中，由于 DHCP 仿冒服务器与 PC5 在同一个 VLAN 中，所以 PC5 会优先选用仿冒服务器提供的 IP 地址及相关网络参数，此时 PC5 已遭到攻击。实验配置、实验结果如表 3 所示。

表 3　实验 6 核心配置与实验结果

	核心配置	实验结果
合法	#LSW5、LSW6配置省略，可参见实验4 #合法DHCP服务器配置代码： dhcp enable ip pool dhcp_vlan10 　gateway-list 192.168.10.254 　network 192.168.10.0 mask 255.255.255.0 　excluded-ip-address 192.168.10.253 　lease day 8 hour 0 minute 0 　dns-list 8.8.8.8 interface GigabitEthernet0/0/0 　ip address 192.168.100.1 255.255.255.0 　dhcp select global ip route-static 192.168.10.0 24 192.168.100.2	PC5获得合法DHCP服务器分配地址： PC>ipconfig Link local IPv6 address.....: fe80::5689:98ff:fe77:6a4b IPv6 address.....: :: / 128 IPv6 gateway.....: :: IPv4 address.....: 192.168.10.252 Subnet mask.....: 255.255.255.0 Gateway.....: 192.168.10.254 Physical address.....: 54-89-98-77-6A-4B DNS server.....: 8.8.8.8
非法	#仿冒服务器配置代码： dhcp enable ip pool dhcp_vlan10 　gateway-list 192.168.10.253 　network 192.168.10.0 mask 255.255.255.0 　excluded-ip-address 192.168.10.254 　lease day 8 hour 0 minute 0 　dns-list 1.1.1.1 interface GigabitEthernet0/0/0 　ip address 192.168.10.253 255.255.255.0 　dhcp select global	PC5获得非法DHCP服务器分配地址： PC>ipconfig Link local IPv6 address.....: fe80::5689:98ff:fe77:6a4b IPv6 address.....: :: / 128 IPv6 gateway.....: :: IPv4 address.....: 192.168.10.252 Subnet mask.....: 255.255.255.0 Gateway.....: 192.168.10.253 Physical address.....: 54-89-98-77-6A-4B DNS server.....: 1.1.1.1

2.3.2　DHCP 饿死攻击

DHCP 饿死攻击是指攻击者伪造 chaddr 字段不同的 DHCP 请求报文，向 DHCP 服务器申请大量的 IP 地址，导致 DHCP 服务器地址池很快被耗尽，使得合法的客户端获取不到正确的 IP 地址。

Kali Linux 中常用到的 DHCP 饿死攻击工具有 dhcpstarv 和 yersinia。其中 dhcpstarv 在攻击时伪造的数据包中源 mac 地址一直不变，不断变化的是 DHCP 报文中的 chaddr 字段。yersinia 攻击则更为高级一些，伪造的数据包中源 MAC 地址和 DHCP 报文中的 chaddr 字段同时会发生变化，本实验采用了 yersinia 攻击，具体实验如下。

[实验 7]

1）将一台路由器作为 DHCP 服务器，配置全局

地址池为 dhcp_vlan56，IP 范围为 192.168.56.0/24，网关为 192.168.56.254，DNS 地址为 8.8.8.8，租期设置为 8 天。

2）LSW7 为接入交换机，在该交换机上创建 VLAN 56，并将 e0/0/1、e0/0/2 都划入 VLAN 56，接口类型为 access，g0/0/1 接口为 trunk 类型，LSW6 为核心交换机，在该交换机上创建 VLAN 56 和 VLAN 100 并创建其虚拟接口 192.168.56.254 和 192.168.100.2，g0/0/1 为 trunk 口，将 g0/0/2 划入 VLAN100。

3）Kail 攻击机是一台 VirtualBox 虚拟机，将其接入到交换机中实施攻击，实验拓扑如图 10 所示，交换机、路由器的详细配置省略，可参考实验 4。

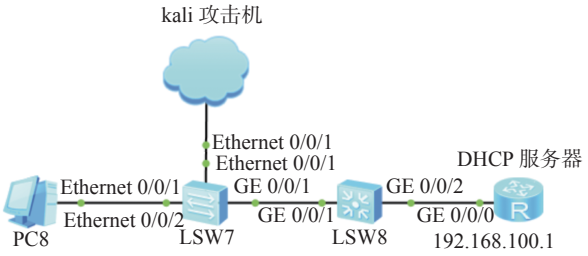
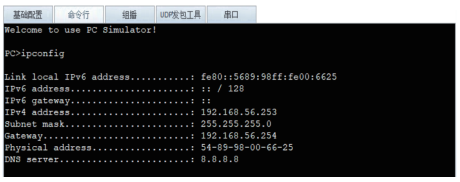
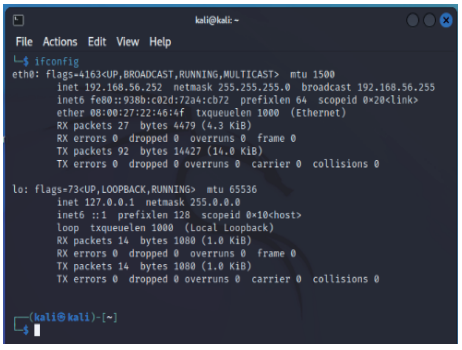


图 10　DHCP 饿死攻击实验拓扑

正常情况下，PC8 和 kail 攻击机可以获得到 DHCP 分配的 IP 地址如图 11 所示。



(a) PC8



(b) Kali

图 11　服务器获得 DHCP 分配的 IP 地址

如果在 Kali 服务器运用 yersinia 工具对 DHCP 服务器发起攻击，yersinia 操作如图 12 所示，可以看到 DHCP 服务器的地址池中的 IP 地址很快被耗光，此时让 PC8 再重新获取 IP 地址，PC8 已经无法再重新获得正常的 IP 地址，实验结果如图 13 所示。

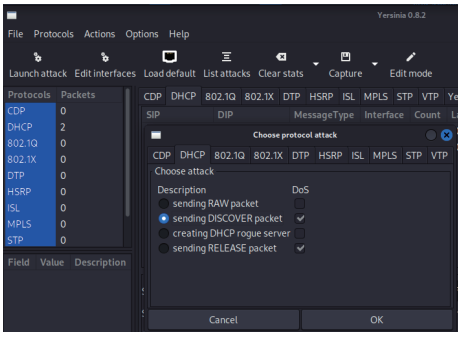
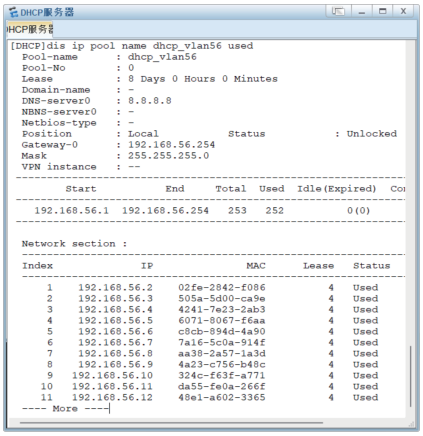
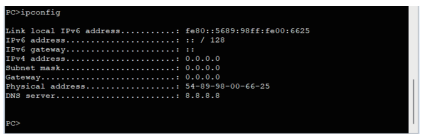


图 12　yersinia 攻击操作



(a) DHCP 地址池的信息查询



(b) PC 无法自动获取 IP 地址

图 13　yersinia 攻击实验结果

2.3.3　DHCP 安全防御

1）针对 DHCP 仿冒攻击，解决方案为配置 DHCP Snooping 功能。具体分为以下 3 步：

① 在相关交换机上全局使能 DHCP；

② 在相关交换机上全局使能 dhcp snooping；

③ 在交换机的下行接口使能 dhcp snooping，上行接口设置 dhcp snooping 信任。

2）针对饿死攻击中的 dhcpstarv，该攻击只需要在交换机上配置 DHCP Snooping 功能并在攻击端口（Kali 接入的交换机端口）下配置如下命令 dhcp snooping check dhcp-chaddr enable，就能实现对 DHCP Request 报文的源 MAC 地址与 chaddr 字段的一致性检查，如果不一致则认为是伪造的报文，直接将其丢弃。而 yersinia 在攻击时，伪造的

数据包中源 MAC 地址和 DHCP 报文中的 chaddr 字段同时会发生变化，所以前述的防御方法将失效。只能通过限制接口允许接入的最大用户数。具体防御配置如表 4 所示。

表 4　防御配置

实验名称	DHCP	
	仿冒攻击的防御	饿死攻击的防御
核心配置	#LSW5配置 dhcp snooping enable interface Ethernet0/0/1 　dhcp snooping enable interface GigabitEthernet0/0/1 　dhcp snooping trusted #LSW6配置与LSW5类似	#LSW7配置 #在可能攻击的交换机端口上进行相应配置，以Ethernet0/0/1为例 interface Ethernet0/0/1 　dhcp snooping enable 　#解决dhcpstarv攻击 　dhcp snooping check dhcp-chadd enable 　#解决yersinia攻击 　port-security enable 　port-security max-mac-num 5 　port-security protect-action shutdown

3　闯关考核

计算机网络实验传统的考核方式存在的弊端是学生之间可以相互抄袭，教师很难对学生的动手能力做出正确的评价，同时逐个查看学生实验配置代码也将耗费大量的时间。针对本文设计的 3 个层次的 DHCP 实验，可利用 eNSP 自带的考试功能分层次设计试卷，只有成绩达到规定的下限才可以进入下一测试环节。eNSP 考试功能的使用流程如图 14 所示。

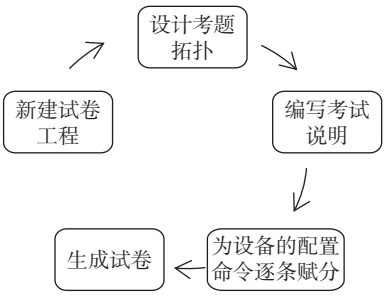


图 14　eNSP 考试功能使用流程

4　结束语

本文提出了一种整合 eNSP、VirtualBox、Kali 来搭建 DHCP 分层仿真实验项目。该实验项目的设计有助于学生更好地掌握 DHCP 相关的理论知识，提升学生的动手实践能力，同时也能够有效解决部分高校实验室硬件设备不足的情况，极大降低学生的学习成本。

参 考 文 献

[1] 李勇, 范全润, 张顺吉, 等. 动态主机配置协议分析及其在模拟器中的实验设计与仿真[J]. 实验室研究与探索, 2020, 39(3): 128−131.

[2] 邹承明, 刘攀文, 唐星. 动态主机配置协议泛洪攻击在软件定义网络中的实时防御[J]. 计算机应用, 2019, 39(4): 1066−1072.

[3] 李晓佳, 李楠, 刘萍. 基于 DHCP 的虚拟主机应用研究[J]. 智能计算机与应用, 2022, 12(5): 98−101.

[4] 谢逸, 王盛邦. 面向新工科的计算机网络教学现状分析与改革[J]. 计算机教育, 2022 (6): 203−207.

[5] 符发, 杨厚群, 黎才茂, 等. 新工科背景下计算机网络实验教学改革探索[J]. 计算机教育, 2022 (3): 39−42.

[6] 陈劲新, 张德成. 新工科背景下计算机实践教学模型的构建与应用[J]. 实验室研究与探索, 2022, 41(1): 235−240.

[7] 叶涛, 王思齐, 杨建彪. 基于 eNSP 的大规模路由综合设计与仿真实验[J]. 实验室研究与探索, 2019, 38(4): 109−114.

[8] 时晨, 赵洪钢, 余瑞丰, 等. 基于 eNSP 的高可靠性企业园区网设计与仿真[J]. 实验室研究与探索, 2020, 39(2): 112−117.

[9] 唐灯平, 凌兴宏, 魏慧. EVE-NG 与 eNSP 整合搭建跨平台仿真实验环境[J]. 实验技术与管理, 2018, 35(11): 117−120.

[10] 郭文普, 陈天豪, 杨百龙. 基于 eNSP 的中小型企业组网实验设计[J]. 实验室研究与探索, 2022, 41(2): 125−129.

[11] 李林林, 孙良旭, 吴建胜, 等. 基于 GNS3 与 VirtualBox 构建虚拟网络工程实验室研究[J]. 实验技术与管理, 2015, 32(9): 144−148.

[12] 周雄庆. 基于 VirtualBox 的 DHCP 服务器仿真实验平台的设计与实现[J]. 智能计算机与应用, 2015, 5(4): 111−112.

[13] 郭川. 基于 Kali Linux 的渗透测试平台的研究[D]. 包头: 内蒙古科技大学, 2019.

[14] 贺义君. 基于 Kali Linux 的渗透测试研究[D]. 长沙: 中南林业科技大学, 2019.

[15] 陈楠. 高校网络攻防仿真教学平台设计[J]. 现代信息科 技, 2021, 5(3): 28−31.

编辑　张俊