“Python+仿真平台”IPv6地址管理安全实验技术

汪小琦[1],胡曦明[1,2*],李 鹏[1,2],马 苗[1,2]
(1.陕西师范大学 计算机科学学院,陕西 西安 710119;
2.现代教学技术教育部重点实验室,陕西 西安 710119)

摘 要:“互联网+”深入推进所催生的高密度、大规模端系统互联对IPv6地址管理安全性提出新的挑战。在产教融合发展背景下,聚焦IPv6网络安全实验技术创新驱动教学改革,针对性地分析了IPv6地址管理协议体系结构和地址管理机制,提出了“Python+仿真平台”的IPv6地址管理安全实验新技术,并进一步详细论述了Python开发层、实验运行层、测量分析层的总体架构和交互接口、过程控制、攻击模式、数据源生成等关键技术。在此基础上,实际应用“Python+仿真平台”完成了链路本地重复地址检测攻击和地址前缀欺骗等针对IPv6无状态地址自动配置管理的安全实验,通过实验教学示例表明“Python+仿真平台”具有可开发性与仿真平台工具性相融合的特点,为面向一流本科课程建设的综合性实验教学改革提供了技术途径。

关键词:IPv6;实验教学;无状态地址自动配置;重复地址检测;地址前缀欺骗
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2021)04-0125-06
doi:10.3969/j.issn.1673-629X.2021.04.021

"Python + Simulation Platform" IPv6 Address Management Security Experimental Technology

WANG Xiao-qi[1],HU Xi-ming[1,2*],LI Peng[1,2],MA Miao[1,2]
(1.School of Computer Science,Shaanxi Normal University,Xi'an 710119,China;
2.Key Laboratory of Modern Teaching Technology of Ministry of Education,Xi'an 710119,China)

Abstract:The high density and large-scale end system interconnection generated by the in-depth promotion of "Internet Plus" has posed new challenges to the security of IPv6 address management. Under the background of the integrated development of industry and education,focusing on the teaching reform driven by IPv6 network security experiment technology innovation,the IPv6 address management protocol architecture and address management mechanism are analyzed,a new technology of IPv6 address management security experiment based on "Python+simulation platform" is proposed,and the overall architecture and key technologies including interactive interface,process control,attack mode,data source generation in Python development layer,experiment operation layer,measurement and analysis layer are further discussed in detail. On this basis,the "Python+simulation platform" is applied to complete the security experiment of IPv6 stateless address auto configuration management,such as link local duplicate address detection attack and address prefix spoofing. The experimental teaching example shows that "Python+simulation platform" has the characteristic of integrating development with simulation platform tool,which provides a technical way for the comprehensive experimental teaching reform facing the construction of first-class undergraduate courses.

Key words:IPv6;experimental teaching;stateless address auto configuration;duplicate address detection;address prefix spoofing

0 引 言

在物联网、云计算和人工智能等新一轮信息科技革命的热潮中,个人上网加速向万物互联纵深推进成为“互联网+”战略推动新兴产业转型升级的标志性和基础性的重要驱动力。然而,面对互联网医疗、智能家居和智慧校园等新行业新场景催生的高密度、大规模

收稿日期:2020-05-29 **修回日期**:2020-09-30
基金项目:国家自然科学基金面上项目(61877037);中央高校基本科研业务费专项资金资助项目(GK201503065);陕西师范大学2020年教师教学模式创新与实践研究专项基金项目(JSJX2020Z28);陕西师范大学2019年教师教学模式创新与实践研究专项基金项目(JSJX2019Z47)
作者简介:汪小琦(1999-),女,研究方向为计算机科学与技术;胡曦明,通讯作者,博士,讲师,教育硕士导师,研究方向为智慧教育、计算机教育;李 鹏,博士,副教授,硕导,研究方向为移动计算、教育信息化;马 苗,博士,教授,博导,研究方向为人工智能、智能系统。

端系统互联需求,传统 IPv4 地址体系在可分配地址空间不足、地址管理机制不完备和地址安全性保障缺失等关键技术性能方面存在制约性短板的问题日益凸显。

IPv6 作为全球公认的下一代互联网技术[1],能够以充足的网络地址、先进的管理机制和新颖的安全性保障为新一代信息技术发展提供广阔的创新空间。相对于 IPv4 体系,IPv6 地址管理技术既是最具代表性的革新与进步,又是整个 IPv6 体系中最为基础和关键的技术之一。面向未来物联网、云计算、人工智能等新技术产生的巨大变革,IPv6 地址管理在协议、机制等方面不可避免地将面临新的安全性挑战[2]。在进一步深化产教融合,加强教育链与产业链有机衔接的背景下,该文聚焦 IPv6 网络安全实验技术创新驱动课程教学改革和人才培养高质量发展,在分析 IPv6 地址管理协议的基础上,针对当前 IPv6 地址管理安全实验技术亟待发展的现实需求,提出了“Python+仿真平台”的创新设计并在教学实践中具体应用。

1 IPv6 地址管理原理

1.1 协议体系结构

IPv6 地址管理协议体系由两部分组成,一部分是对 IPv4 地址管理方式的继承,包括基于手动分配的地址静态配置与基于 DHCPv6 的有状态地址自动配置[3];另一部分是新增的 IPv6 无状态地址自动配置 SLAAC(stateless address auto configuration)方式。这样的设计既能够兼容原有 IPv4 地址体系[4],又能够让 IPv6 地址分配和管理更加高效。

IPv6 无状态地址自动配置是通过网络层的邻居发现协议 NDP(neighbor discovery protocol)实现的,地址信息分配与管理基于四种类型的 ICMPv6 协议报文,分别是:路由请求报文 RS(router solicitation)、邻居请求报文 NS(neighbor solicitation)、路由通告报文 RA(router advertisement)、邻居通告报文 NA(neighbor advertisement)。NDP 发现链路上彼此连接的邻居节点和地址配置信息[5],在实时维护与邻居节点之间的链路可达性与可达路径等链路状态的基础上,实现对邻居节点的 IPv6 地址自动分配与跟踪管理。

1.2 地址管理机制

邻居发现协议 NDP 实现了 IPv6 无状态地址自动配置机制[6],机制分为用户发送 RS 报文请求前缀和网关路由器周期性发送携带配置信息的 RA 报文两种方式,具体报文交互过程如下:

①终端用户根据一定规则生成临时链路本地地址,并在局域网内发送该地址的 NS 报文,进行链路本地地址重复地址检测 DAD(duplicate address detection)。

②网关发送包含地址前缀等配置信息的 RA 报文,使终端用户成功配置全球单播地址;如果终端用户未接收到 RA 报文,可主动发送 RS 报文,请求网关的 RA 报文配置全球单播地址。

③终端用户发送包含全球单播地址的 NS 报文,进行全球单播地址重复地址检测。

此后,位于 IPv6 局域网链路上的终端用户成功配置链路本地地址和全球单播地址两类地址。从上述过程可以看到,邻居发现协议 NDP 通过 RS、NS、RA 和 NA 报文自动交互,实现了 IPv6 无状态地址自动配置,可极大地缓解地址配置过程中人工和服务器压力,具有全自动和即插即用等优势,非常有利于未来智能化应用的发展,但 DAD 过程对移动节点地址切换具有一定时延[7]。

2 基于“Python+仿真平台”的实验技术

2.1 总体架构

由于 IPv6 网络实验室设备投入大、建设周期长,目前主要依赖仿真平台开展 IPv6 实验教学。仿真平台具有技术成熟、运行稳定和便于操作等优势,但在面向大规模学生群体的探究性实验中,仿真平台往往表现出可开发性、可拓展性不足[8],常局限于单一的攻击和防御模式[9]。因此该文提出 Python 开发与仿真平台融合的 IPv6 安全性实验新技术,如图 1 所示,既可有效利用仿真平台成熟、稳定的优势,又可融入自主开发实验要素,满足开展创新性、高阶性和具有挑战度的个性化探究实验。

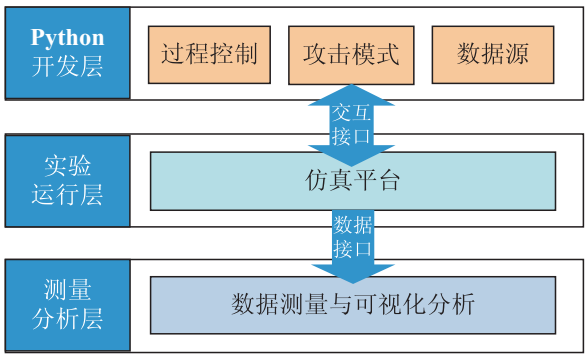

图 1 “Python+仿真平台”实验技术

(1)Python 开发层。

开发层可向上为实验人员提供个性化、开放式的实验定制开发接口,向下通过输入输出接口与实验运行模块实现过程交互。

开发人员可通过 Python 内置 scapy 模块或自主编程等多种方式开发实验插件,实现探测、路由跟踪等网络行为,数据包组包发包等数据源对象以及控制逻辑等功能。

(2)实验运行层。

仿真平台可采用华为、华三等主流模拟器,用来实现路由器、交换机等设备的虚拟仿真[10],为开发层提供支撑实验的基础网络结构和仿真运行环境。Python 程序与仿真平台既相互协同工作,又相对独立,相互之间通过通道式的双向接口进行数据和控制的交互。

(3)测量分析层。

测量分析层通过数据接口实时接收实验运行模块输出的实验数据,通过协议分析工具如 Wireshark 等实现对实验的过程性分析。

2.2　关键技术

如何基于 Python 实现可编程攻击方,控制报文生成并发送到仿真平台中与输入仿真过程是“Python+仿真平台”的关键,具体可分为四个部分。

(1)创建交互接口。

交互接口是一种通道式的双向接口,连接着 Python 开发层与实验运行层,负责 Python 程序与仿真软件之间的运行交互。通过本地主机搜寻并激活本地“环回适配器”后,仿真平台创建“云对象”桥接本地环回网络,从而完成 Python 程序与仿真软件的接口创建。该方法提高了仿真平台的可操作性,节省了创建虚拟网卡等繁琐工作,并且避免了绑定真实网络网卡导致实验操作引起的公共网络故障。

(2)过程控制。

Python 开发层通过交互接口实现对仿真平台实验运行报文的实时监听,然后嗅探、过滤出目标类型的报文,实现对实验状态的侦听监控。Python 程序实现示例如下:

示例一:监听本地环回网卡功能实现需要开发层确定接受链路层数据帧类型的协议和实验网卡名称,具体程序为:listen_socket = conf. L2listen(type = ETH_P_ALL, iface = " Microsoft KM-TEST 环回适配器")。

示例二:获取仿真平台运行的网卡,然后确定过滤报文的类型和数量,可以实现嗅探过滤报文(如 icmpv6 报文)的同时对报文调用响应方法,并返回响应结果。具体程序为:package = sniff(iface = " Microsoft KM-TEST 环回适配器", filter = " ICMPv6", count = 20, prn = pack_callback)。

(3)攻击模式。

攻击模式具体包括单线程攻击和多线程攻击。处于开发层的 Python 程序实时监控实验运行层中主机的地址配置信息,如果有新的主机加入实验,Python 程序则对应新建主机控制线程,并将线程号与该主机的 MAC 地址绑定之后存储形成字典数据。

(4)数据源生成。

开发层的 Python 程序可以与实验运行层的仿真软件交互实验数据,通过 Python 开发自主设计报文类型并赋值,可以实现伪造、错造和窃取报文等攻击操作,其中伪造报文的关键实现如表 1 所示。

表 1　伪造报文关键技术

关键步骤	程序实现
步骤一:填充 NA 或 RA 攻击报文内容参数,确定攻击对象自动配置的 IPv6 地址或全局地址前缀	NA: b = ICMPv6ND_NA( ) c = ICMPv6NDOptSrcLLAddr( ) RA: b = ICMPv6ND_RA( ) c = ICMPv6NDOptSrcLLAddr( ) d = ICMPv6NDOptPrefixInfo( )
步骤二:将报文按照 IPv6 协议的标准封装格式进行封装	e = Ether(dst, src) a = IPv6(src, dst, plen, tc) pack = e/a/b/c/d
步骤三:将数据包按指定网卡发出	sendp(pack, count = 1, iface = " Microsoft KM-TEST 环回适配器")

开发 Python 可编程攻击方可以根据具体实验需要,自主设计报文类型和赋值,并可根据整个实验进程自动调整发包种类和报文值,具有个性化、智能化的技术优点。

3　IPv6 地址管理攻击与防御实验

基于上述“Python+仿真平台”实验技术,通过链路本地 DAD 和地址前缀欺骗的攻击与防御实例研究,进一步丰富 IPv6 实验教学内容和提升 IPv6 网络安全性。

3.1　实验环境与流程设计

(1)环境搭建。

实验运行层部署华为 eNSP 模拟器为仿真平台,建立的网络拓扑如图 2 所示,其中以基于 Python 开发的“云对象”为攻击方,以路由器 UserA 和 UserB 为被攻击方。

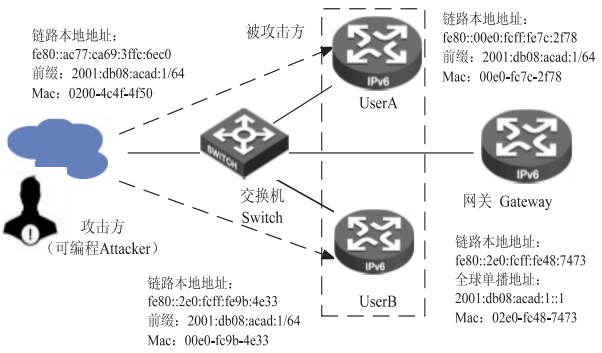

图 2　实验拓扑

(2)环境配置。

首先在实验运行层的仿真平台进行无状态地址自动配置实验,作为后续攻击与防御实验的基础,具体配

置如表 2 所示。

表 2 实验设备配置

设备名称	配置及相关命令
网关 Gateway	ipv6 interfaceGigabitEthernet 0/0/4 ipv6 enable ipv6 address 2001:db08:acad:1::1/64 undo ipv6nd ra halt //开启使能 RA
攻击方（可编程 Attacker）	Port1:Ethernet UDP 9429 Port2:Microsoft KM-TEST(环回适配器网卡)(192.168.10.2) ipv6 stateless address auto configuration//配置网卡自动获取 IPv6 地址
被攻击方 UserA、UserB	ipv6 interface g0/0/3 ipv6 enableipv6 address auto global //开启无状态地址自动配置 display ipv6 interface g0/0/3 //显示地址配置信息

开启 Attacker、UserA 和 UserB 无状态地址自动配置功能，查看本地主机网卡信息和 UserA、UserB 地址，由图 2 设备信息可以看到，Gateway 等路由器的链路本地地址采用基于 MAC 地址的 EUI-64 规则生成[11-12]，相比之下 Attacker 的链路本地地址是随机生成，与 MAC 地址无关。其主要原因是防止 PC 机的 MAC 地址泄露带来安全隐患。

(3)流程设计。

IPv6 无状态地址自动配置在实现地址管理功能的过程中，也带来新的网络安全漏洞。以下基于“Python+仿真平台”技术，提出 IPv6 地址管理攻击实验流程设计(见图 3)，有效促进 IPv6 实验教学发展。

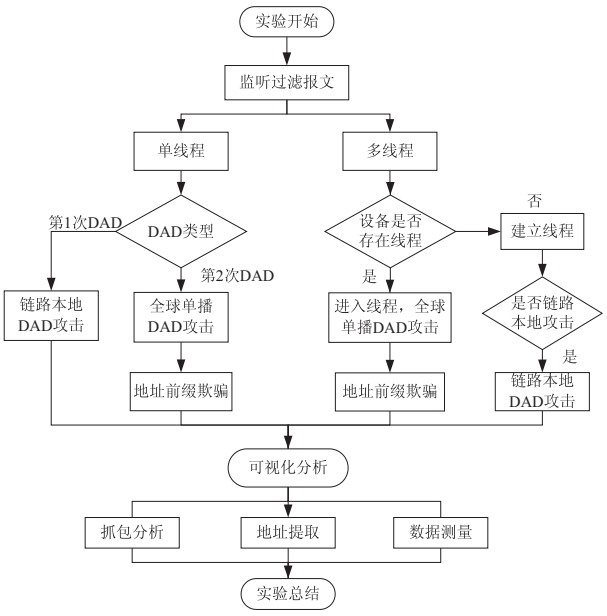

图 3 IPv6 地址管理攻击实验流程

3.2 链路本地 DAD 攻击

3.2.1 攻击原理

由 IPv6 地址管理机制可知，在无状态地址自动配置过程中，有两次 DAD 过程，并且是在网段内广播地址检测报文[13]。攻击方可以在接收报文后，发送包含相同 IPv6 地址的 NA 报文来响应 NS 报文，声称该 IP 地址已经在使用，造成大量的 IP 地址和网络资源浪费，形成网络攻击[14]。

3.2.2 攻击实验

(1)单线程攻击。

首先，实验运行层的仿真平台开启 UserA 无状态地址自动配置，广播发送 NS 报文进行链路本地地址唯一性检查，攻击方 Attacker 自主检测到节点配置地址。然后，Python 程序分析 NS 报文，提取其声明的地址 fe80::2e0:fcff:fe7c:2f78 添加至伪造 NA 报文的 Target Address 字段并作为网络层的源地址，同时将攻击方的 MAC 地址填入地址解析选项字段，完善各标志位，逐层封装，过程如图 4 所示。随后，Python 程序控制攻击方发送伪造报文，进行 DAD 攻击。此时，被攻击方 UserA 查看地址配置信息可发现节点地址末尾显示“DUPLICATE”字样，表示 IPv6 地址在局域网内重复，地址配置失败。

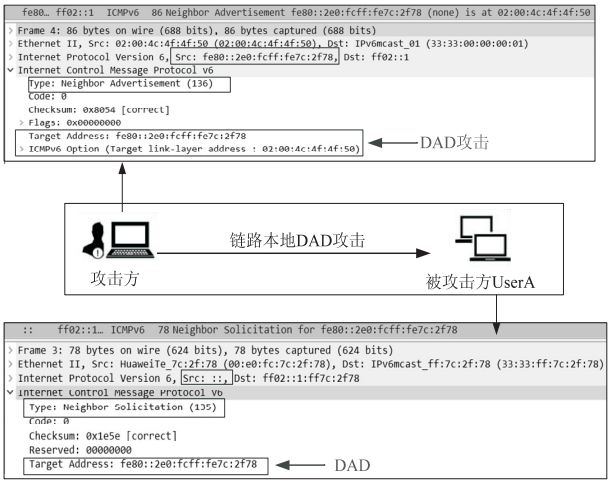

图 4 链路本地 DAD 攻击

(2)多线程攻击。

在实验拓扑(图 2)中启用 UserB 作为新设备与 UserA 一起加入网络，当 Python 开发层检测到新设备加入时，根据攻击模式对不同新节点建立对应线程，在字典数据结构中以键值对“Key:Value”形式存储 MAC 地址和线程号，例如存储节点 UserA、UserB 信息为：{"00e0-fc7c-2f78":"Thread1","00e0-fc9b-4e33":"Thread2"}。

在此基础上，Python 程序传送不同设备 NS 报文中的 MAC、IPv6 字段至数据源，用以伪造链路 NA 报文并发送，从而实现多线程条件下链路本地 DAD 攻

击。Attacker 接口抓包获得攻击过程如图 5 所示。

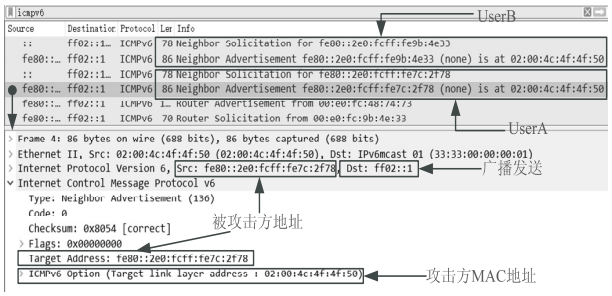

图 5　链路本地 DAD 攻击

3.3　基于全球单播 DAD 的地址前缀欺骗

3.3.1　攻击原理

在配置全球单播地址过程中,链路内的节点依据接收到的 RA 报文进行地址配置,且不对发送方进行网关身份验证。攻击方利用该漏洞,自行发送包含无效地址前缀的路由通告 RA 报文,被攻击方自动使用该前缀进行全球单播地址配置得到的地址是无效的,从而实现拒绝服务攻击[15]。

3.3.2　攻击实验

在实验教学中,为了避免节点配置过程中无法区分网关和攻击方发送的 RA 报文正确性,使得攻击实验存在偶然性,攻击方可以选择将全球单播 DAD 攻击同地址前缀欺骗攻击结合,具体过程如图 6 所示。

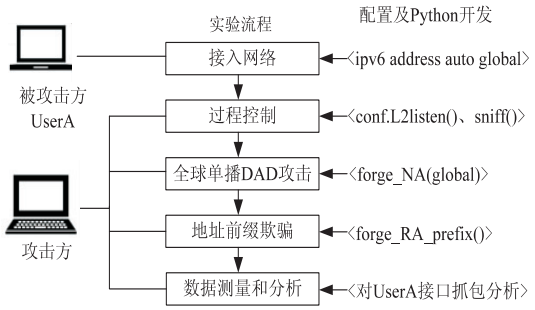

图 6　实验教学过程

(1)全球单播 DAD 攻击。

UserA 链路本地地址配置成功后,接收网关 RA 报文获取前缀信息,配置全球单播地址为 2001:db08:acad:1:2e0:fcff:fe7c:2f78,并发送 NS 报文对该地址进行声明。Python 开发的攻击方读取该 NS 报文,伪造类似上述链路本地 DAD 攻击的 NA 报文使节点声明全球单播地址失效,导致 UserA 配置全球单播地址失败。经局域网内 ping 实验验证,UserA 此时虽然拥有本地链路地址,可在局域网内正常通信,但由于全球单播地址缺失无法跨网段通信。

(2)地址前缀欺骗。

由于针对 UserA 的全球单播 DAD 攻击造成真实网关发布的前缀信息对 UserA 不可用。此时,Python 开发的攻击方伪造 RA 报文,添加相应的前缀选项字段包含虚假前缀:2001:db08:acad:2::/64,同时携带链路 MAC 地址解析选项字段,将报文广播至实验运行层的所有网段。由于 UserA 完全信任网段内的报文,因此在收到伪造的 RA 报文后,将按其配置全球单播地址,导致地址前缀被欺骗。

(3)抓包分析。

如图 7 所示,使用 Wireshark 软件对 UserA 接口上的报文进行抓包。UserA 成功配置无效的全球单播地址 2001:db08:acad:2:2e0:fcff:fe7c:2f78。另外,通过仿真平台地址查看命令,发现原本拥有正确全球单播地址的 UserB 主机也另外获得了前缀为 2001:db08:acad:2::/64 的新 IPv6 地址。此时的 UserA 仅可以使用虚假全球单播地址与 UserB 通信。

图 7　基于全球单播 DAD 的前缀欺骗

3.4　攻击防御

为了防范 IPv6 地址管理的安全漏洞,抵御恶意主机对 IPv6 网络的攻击,可以在用户终端、局域网内和二层交换设备处分别通过改进 NDP 协议、建立邻居控制服务器以及配置控制信息交互命令等方式综合提升网络安全性能,具体可采取以下三种有效措施。

(1)安全邻居发现协议(SEND)。

通过加密地址生成技术(CGA)、数字签名等方法对通信过程进行加密,可有效防止 IP 地址被盗用。当经过重复地址检测发现存在冲突地址时,CGA 能够通过重新计算生成新的地址[16],有效实现 DAD 攻击防御。

(2)安全邻居发现协议(IPSec-SEND)。

在邻居发现协议的基础上,IPSec-SEND 采用 IPsec 认证头 AH(authentication header)作为节点间通信的安全协议,提供 IP 和 MAC 绑定认证,能有效解决由伪造 IP 地址、路由信息等攻击行为造成的各种网络安全问题[17]。

(3)ND Snooping 技术。

华为[18]与华三[19]等公司二层交换机具有 ND Snooping 机制,可防御利用邻居发现协议进行的网络攻击。ND Snooping 通过自动的 ND 监控模式监听 DAD 交互过程,通过获取合法用户的 IP-MAC 对应关系,建立起邻居信任表,从面可以对端口输入报文进行合法性检测,放行匹配绑定的报文,丢弃不匹配的报

文,有效实现 IPv6 节点接入控制。

4 结束语

《教育部关于一流本科课程建设的实施意见》明确提出高阶性、创新性和挑战度的“两性一度”一流本科课程发展导向,如何以教育技术创新支撑优质课程教学在高水平本科教育建设中的基础性地位成为新时代高等教育教学改革的热点。该文着眼于实验技术创新驱动课程教学改革,提出了“Python+仿真平台”的 IPv6 网络安全实验新技术,通过无状态地址自动配置过程中的链路本地 DAD 和地址前缀欺骗的攻防实验,深入而细致地论述了“Python+仿真平台”教学应用的方法与过程。经过多年级多班次的实验教学实践表明,“Python+仿真平台”将 Python 可开发性与仿真平台的工具性有机融合,为面向“两性一度”导向的综合性实验教学改革提供了切实可行的技术途径。

参考文献:

[1] 郭 威,常艳生,时利鹏,等. LTE 终端 IPv6 地址无状态自动分配研究[J]. 电信技术,2019(2):34-38.

[2] 张连成,郭 毅. IPv6 网络安全威胁分析[J]. 信息通信技术,2019(6):7-14.

[3] AL-ANI A,ANBAR M,HASBULLAH I H,et al. Authentication and privacy approach for DHCPv6[J]. IEEE Access,7:73144-73156.

[4] 李晓杰. 基于双栈网络的 IPv4/IPv6 校园过渡方案研究[J]. 计算机技术与发展,2016,26(8):171-173.

[5] AL-ANI A,ANBAR M,AL-ANI A,et al. Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network[J]. IEEE Access,2020,8:27122-27138.

[6] SONG Guangjia,WANG Hui,WANG Hangjun. Using multi-address generation and duplicate address detection to prevent DoS in IPv6[J]. IET Communications,2019,13(10):1390-1396.

[7] 房家保,王振兴,张连成. 免重复地址检测移动 IPv6 快速切换方案[J]. 计算机应用研究,2017,34(5):1455-1458.

[8] 张 宁,赵毅强,兰馗博,等. “新工科”背景下关于虚拟仿真实验的几点思考和建议[J]. 实验技术与管理,2020,37(3):185-188.

[9] 叶福玲,张 栋,林为伟. 基于软件定义网络的安全攻防虚拟仿真实战平台[J]. 实验技术与管理,2018,35(11):125-129.

[10] 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.

[11] ROHRER J P,LAFEVER B,BEVERLY R. Empirical study of router IPv6 interface address distributions[J]. IEEE Internet Computing,2016,20(4):36-45.

[12] 张千里,姜彩萍,王继龙,等. IPv6 地址结构标准化研究综述[J]. 计算机学报,2019,42(6):1384-1405.

[13] WANG X,CHENG H,YAO Y. Addressing with an improved DAD for 6LoWPAN[J]. IEEE Communications Letters,2016,20(1):73-76.

[14] 苗慧宇,陈 勇,孙知信. 一种抗攻击的 6Lowpan 地址注册的算法[J]. 计算机技术与发展,2017,27(9):110-115.

[15] AHMED A S A M S,HASSAN R,OTHMAN N E. IPv6 neighbor discovery protocol specifications,threats and countermeasures:a survey[J]. IEEE Access,2017,5:18187-18210.

[16] 宋广佳,季振洲,王 晖. 一种在无状态地址自动配置中 DAD 攻击的防御方法[J]. 电信科学,2014,30(4):54-60.

[17] 刘华春,戴庆光,蒋志平. 基于 IPsec 的 IPv6 安全邻居发现协议[J]. 计算机工程与设计,2011,32(2):513-516.

[18] 华为. ND Snooping 配置命令(S600-E V200R013C00 命令参考)[EB/OL]. (2019-04-04)[2020-04-25]. https://support.huawei.com/enterprise/zh/doc/EDOC1100066233/7788d141.

[19] 华三. IPv6 解决方案 ND 防攻击技术白皮书[EB/OL]. (2009-07-14)[2020-04-25]. http://www.h3c.com/cn/d_200907/642189_30004_0.htm.