文章编号:1672-058X(2013)07-0062-05

基于 Scapy 的网络协议分析实验室构建*

李树军
(盐城师范学院 信息与科学学院,江苏 盐城 224002)

摘　要:针对网络协议分析实验中的突出问题,提出利用 Scapy 软件来构建实验室;对 Scapy 的安装步骤、基本功能进行了介绍,在此基础上以 RIP 路由协议安全性分析实验作为案例,详细描述了 Scapy 在实验中的应用,验证了利用 Scapy 构建协议分析实验室的可行性。

关键词:Scapy;协议分析;实验室;实验室构建
中图分类号:TP393　　**文献标志码**:A

《网络协议分析》课程是针对计算机网络工程专业的本科生而设置的一门课程,该课程主要是在学习《计算机网络》课程的基础上,就网络协议的基础理论、体系结构、性能特性、技术方法和所解决的问题等方面进行学习。学生通过本课程学习,进一步掌握常用网络协议的工作原理与机制,在实践中能充分利用所学知识分析和研究协议运行过程中出现的各种现象和问题,能够利用网络协议的原理解释网络的工作过程,训练灵活运用所学知识解决计算机网络相关的综合问题的能力,为以后走向相应的工作岗位打下良好的基础。

《网络协议分析》是一门实践性很强的课程,为了让学生学好这门课程,达到课程预期的培养目标,就必须建设与之对应的协议分析实验室。条件好、资金充足的高校一般建立了专用的网络协议分析实验室,这种方法固然有不少优点,但在实际教学过程中,也暴露出不少不足的地方。比如设备的数量和型号较少,设备更新慢,难以满足学生一人一套设备的需求,对相关新技术支持不足,学生课后无法进行实验等。另外一些高校则采用 Sniffer Pro、Ethereal 等协议分析软件来进行网络协议分析。这种方法资金投入很小,解决了传统实验教学实验设备数量少、实验时间紧张、实验地点单一的弊端。不足的是学生仅能对捕获到的数据包进行分析,不能根据需要自己构造和发送各类网络数据包,更谈不上进行协议的测试了。

通过 Scapy 构建的网络协议分析实验平台,通过对网络体系各层次协议数据单元的灵活编辑、发送、捕获解析和会话分析,学生可以深入地理解和掌握网络协议的内部原理和运行机制。借助此平台还可以学习网络程序设计、网络攻防和故障性能分析等相关知识,加强学生对网络协议的理解和掌握,培养学生的动手实践和设计分析能力,培养创新型人才。

1　Scapy 安装与功能介绍[1]

Scapy 是一款强大的交互式数据包处理工具、数据包生成器、网络扫描器、网络发现工具和数据包嗅探、

收稿日期:2013-03-01;**修回日期**:2013-03-20.
* **基金项目**:江苏省高等教育教改研究课题(169).
作者简介:李树军(1980-),男,重庆潼南人,讲师,从事网络管理、网络安全研究.

分析工具。它提供多种类别的交互式生成数据包或数据包集合,能方便的对数据包进行编辑、发送、嗅探、应答和反馈匹配等,利用它可以很方便的构造各种数据包用于各种网络协议分析与测试。

1.1　Scapy 安装

Scapy 基于 Python 开发,可以运行在 Linux、FreeBSD 和 Windows 等主流操作系统平台下。考虑到实验室的实际情况,这里以 Windows XP 环境下安装 Scapy 为例进行说明。首先下载安装 Python,然后在 Scapy 的官方网站 http://www.secdev.org/projects/scapy 上下载最新版本的软件,下载完成后依次解压软件包,打开 Windows 命令行,进入到软件包的目录后执行 python setup.py install 指令进行安装,一步完成。为了让 Scapy 正常工作或者发挥全部功能,需要安装一下组件:Pywin32,Python 访问 Windows 系统 API 的运行库,推荐的版本是 2.6;WinPcap,用于支持 Scapy 捕获或者发送数据包,推荐的版本是 4.1;PypCap,用于支持 Scapy 导入其他协议分许软件捕获的数据包文件;LibdNet,用于支持支持 Scapy 发送 RAW 数据包;PyReadline,对 Scapy 提供交互式支持,推荐的版本是 1.5。

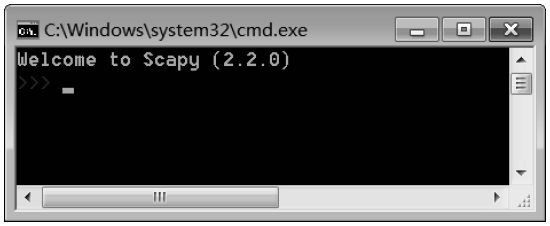

图 1　Scapy 运行初始界面

此外,还可以根据实验需要选装如下一些组件:GnuPlot、Scapy 可调用它来绘制各类统计图表;Pyx 利用它 Scapy 能把协议分析的结果导出到 pdf 文件中或者导出 ps 格式的矢量图中;VPython,提供 3D 绘图支持;PyCrypto,利用它 Scapy 可以完成 WEP 解密工作。Wireshark、Scapy 调用它来解析构造或捕获到的数据包。安装完成后,执行 Scapy 命令,如果一切正常,则出现如图 1 的界面。

1.2　Scapy 强大的数据包构造功能

利用 Scapy 可以直观灵活的构造各种网络数据包,甚至可以根据需要自定义网络协议。在构造数据包的时候,它遵循网络协议分层的思想,以参数化赋值的方式进行。比如要构造一个目的地址为192.168.10.1,TTL 为 6,源端口为 1000,目的端口为 23 的 TCP SYN 包,用指令 p=IP(dst="192.168.10.1",ttl=6)/TCP(sport=1000,dport=23,flags="S")即可简单完成。对于已经构造好的数据包 p,可以用 ls(p)指令查看它各协议单元的值,可以用 hexdump(p)指令导出为 16 进制格式的数据,可以用 p.summary()指令对数据包的功能做摘要说明。也可以在一个指令里面构造多个数据包,比如要构造 TTL 值分别为 1-6 的 6 个数据包,只需要把指令中的 ttl=6 修改为 ttl=(1,6)就可以了。类似的其他各项参数都可以用这种序列化的方式来表示,如图 2 所示。

```
>>> p=Ether()/IP(dst="192.168.10.1",ttl=6)/TCP(sport=1000,dport=23,flags="S")
>>> p
<Ether  type=0x800 |<IP  frag=0 ttl=6 proto=tcp dst=192.168.10.1 |<TCP  sport=
00 dport=telnet flags=S |>>>
>>> p.summary()
'Ether / IP / TCP 210.28.177.20:1000 > 192.168.10.1:telnet S'
>>> hexdump(p)
0000   00 0F E2 7F 3B EF 2C 41  38 B2 76 17 08 00 45 00   ....;.,A8.v...E.
0010   00 28 00 01 00 00 06 06  66 F5 D2 1C B1 14 C0 A8   .(......f.......
0020   0A 01 03 E8 00 17 00 00  00 00 00 00 00 00 50 02   ..............P.
0030   20 00 3E 09 00 00                                  .>...
```

图 2　用 Scapy 构造数据包

1.3　Scapy 强大的数据包发送与接收功能

Scapy 提供了多个指令用于数据包的发送和接收,其中 send、sendp、sr1 和 srp1 几个指令用的比较多。send 指令在网络层发送数据,sendp 在数据链路层发送数据,这两个指令仅仅发送数据包而不接收其反馈;sr1 和 srp1 分别在网络层和数据链路层发送数据,它们在发送数据包的同时接收来自网络的反馈数据包,如图 3 所示。

```
>>> send(IP(dst="www.baidu.com")/ICMP())
.
Sent 1 packets.
>>> answer=sr1(IP(dst="www.baidu.com")/ICMP())
Begin emission:
Finished to send 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
```

图3 用Scapy发送和接收数据包

1.4 Scapy其他强大的功能

除了上述功能外,Scapy还具有网络扫描、网络嗅探和协议Fuzzing测试等功能。此外,还可以通过脚本编程完成各项复杂的实验,以至于Scapy具有可编程的Wireshark的美誉。限于篇幅,这里不一一叙述。

2 RIP路由协议安全性分析与测试实验案例

2.1 实验环境搭建

实验用网络环境拓扑和设备各接口IP地址如图4。实验可以利用网络实验室里现有的路由与交换设备,也可以用GNS3软件进行仿真[2-4]。各设备按照拓扑图进行连接并做IP地址与RIP相关配置后完成实验环境的构建。配置完成后SW1的路由表如图5,R2的路由表如图6(实验真实截图)。

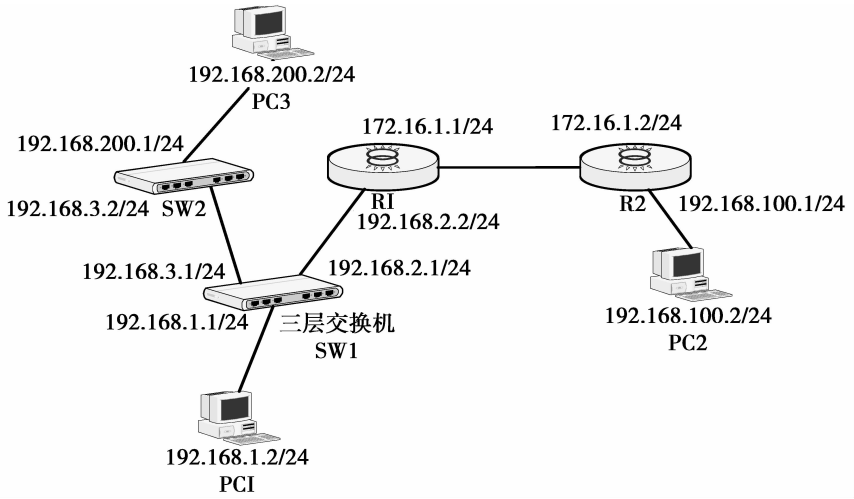

图4 RIP路由协议安全性分析实验拓扑图

```
SW1#show ip route

Type:  C - connected, S - static, R - RIP, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

Type Destination IP     Next hop        Interface Distance Metric   Status
---- ------------------ --------------- --------- -------- -------- --------
R    172.16.0.0/16      192.168.2.2     Fa0/2     120      2        Active
C    192.168.1.0/24     0.0.0.0         Fa0/1     0        0        Active
C    192.168.2.0/24     0.0.0.0         Fa0/2     0        0        Active
C    192.168.3.0/24     0.0.0.0         Fa0/3     0        0        Active
R    192.168.100.0/24   192.168.2.2     Fa0/2     120      3        Active
R    192.168.200.0/24   192.168.3.2     Fa0/3     120      2        Active
```

图5 SW1真实路由表

```
R2#show ip route

Codes:  C - connected, S - static,  R - RIP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        * - candidate default

Gateway of last resort is no set
C    172.16.1.0/24 is directly connected, FastEthernet 1/0
C    172.16.1.2/32 is local host.
R    192.168.1.0/24 [120/2] via 172.16.1.1, 00:00:21, FastEthernet 1/0
R    192.168.2.0/24 [120/1] via 172.16.1.1, 00:00:21, FastEthernet 1/0
R    192.168.3.0/24 [120/2] via 172.16.1.1, 00:00:21, FastEthernet 1/0
C    192.168.100.0/24 is directly connected, FastEthernet 1/1
C    192.168.100.1/32 is local host.
R    192.168.200.0/24 [120/3] via 172.16.1.1, 00:00:21, FastEthernet 1/0
R2#
```

图 6　R2 真实路由表

2.2　RIP 路由协议安全性测试

（1）测试 1。在 PC1 上发送欺骗数据包给 SW1,修改原有的一条路由 192.168.100.0/24 并添加一条新路由 202.16.0.0/24,测试成功(修改已有路由条目需要设置相应的 Metric 值比原来值小),新的路由表如图 7。新添加的和被修改后的条目会被传递给其他路由器,从而影响整个网络的数据流向。

测试用 Scapy 命令:

```
p=IP(dst="192.168.1.1")/UDP(dport=520,sport=520)/RIP(command=2)
px=RIPEntry(addr="202.16.0.0")/RIPEntry(addr="192.168.100.0",metric=1)
send(p/px)
```

```
SW1#show ip rou

Type:  C - connected, S - static, R - RIP, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

Type Destination IP     Next hop        Interface Distance Metric   Status
---- ------------------ --------------- --------- -------- -------- --------
R    172.16.0.0/16      192.168.2.2     Fa0/2     120      2        Active
C    192.168.1.0/24     0.0.0.0         Fa0/1     0        0        Active
C    192.168.2.0/24     0.0.0.0         Fa0/2     0        0        Active
R    192.168.2.0/24     192.168.1.2     Fa0/1     120      2        Active
C    192.168.3.0/24     0.0.0.0         Fa0/3     0        0        Active
R    192.168.3.0/24     192.168.1.2     Fa0/1     120      2        Active
R    192.168.100.0/24   192.168.1.2     Fa0/1     120      2        Active
R    192.168.200.0/24   192.168.3.2     Fa0/3     120      2        Active
R    202.16.0.0/24      192.168.1.2     Fa0/1     120      3        Active
```

图 7　SW1 被伪造数据修改后的路由表

（2）测试 2。跨网段欺骗。在 PC1 上发送欺骗数据包给 R2,直接在远程路由器(非本地子网)的路由表里添加新的条目 203.16.0.0/24,修改 192.168.3.0/24 条目的下一跳地址为一个不存在的节点 172.16.1.3。需要说明的是这里伪造的是单播包,数据包的目的地址为 R2 上的 172.16.1.2,源 IP 须为与 172.16.1.2 同一网段的地址,否则会被当作无效的数据包而被路由器丢弃,达不到欺骗的目的。另外由于 RIP 协议“水平分割”的特性,这些被修改或者新添加的路由条目不会被 R2 传播给 R1,被修改后的路由表如图 8。

测试用 Scapy 命令:

```
p=IP(src="172.16.1.3",dst="172.16.1.2")/UDP(dport=520,sport=520)/RIP(command=2)
px=RIPEntry(addr="192.168.3.0",metric=1)
send(p/px)
p=IP(src="172.16.1.1",dst="172.16.1.2")/UDP(dport=520,sport=520)/RIP(command=2)
px=RIPEntry(addr="203.16.0.0",metric=1)
send(p/px)
```

在以上的测试中,使用 Scapy 构造恶意的 RIP 路由协议数据包,并把它发送给了网络里面的指定设备,

```
R2#show ip route

Codes:  C - connected, S - static,  R - RIP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        * - candidate default

Gateway of last resort is no set
C    172.16.1.0/24 is directly connected, FastEthernet 1/0
C    172.16.1.2/32 is local host.
R    192.168.1.0/24 [120/2] via 172.16.1.1, 00:00:11, FastEthernet 1/0
R    192.168.2.0/24 [120/1] via 172.16.1.1, 00:00:11, FastEthernet 1/0
R    192.168.3.0/24 [120/1] via 172.16.1.3, 00:01:54, FastEthernet 1/0
C    192.168.100.0/24 is directly connected, FastEthernet 1/1
C    192.168.100.1/32 is local host.
R    192.168.200.0/24 [120/2] via 172.16.1.1, 00:00:11, FastEthernet 1/0
R    203.16.0.0/24 [120/1] via 172.16.1.1, 00:00:53, FastEthernet 1/0
```

图8　R2被伪造数据修改后的路由表

利用RIP路由协议的安全缺陷,篡改了目标设备的路由表,达到了实验目的。

3　结　语

由于建设专用的协议分析实验室受经费等因素的限制,利用Scapy构建基于软件的实验室就显得尤为必要。Scapy功能强大,可扩展性强,经过本在近两年在网络工程专业的应用效果良好。实践表明,在计算机网络协议分析的实验教学中,如果实验硬件条件缺乏,可以通过充分利用Scapy来突破实验条件的限制,以达到相同的或更好的教学效果。

参考文献:

[1] http://www.secdev.org/projects/scapy/doc/usage.htm.

[2] 顾春峰,李伟斌,兰秀凤.基于VMware、GNS3实现虚拟网络实验室[J]. 实验室研究与探索,2012,31(1):73-74

[3] 万润泽, 张昊. 虚拟机VMware在网络实用技术实验教学中的研究[J]. 实验室研究与探索,2010,20(6):134-135

[4] 包敬海, 周小珠, 樊东红. 基于VMWare构建虚拟网络实验室的研究[J]. 计算机技术与发展,2010(6):242-244

Construction of Network Protocol Analysis Laboratory Based on Scapy

LI Shu-jun

(School of Information and Science, Yancheng Teachers College, Jiangsu Yancheng 224002, China)

Abstract: According to projecting problems in network protocol analysis experiment, this paper proposes to use Scapy software to build a laboratory, introduces the installment steps and basic functions of Scapy, based on this, in detail describes the application of Scapy to experiment by taking RIP routing protocol security analysis experiment as a case, and tests the feasibility for using Scapy to construct protocol analysis laboratory.

Key words: Scapy; protocol analysis; laboratory; laboratory construction

责任编辑:代小红