实验二　packet sniffing and spoofing 实验

一. 实验目的

通过此次实验，了解包嗅探和欺骗的方法，使自己对包嗅探及欺骗有一定的认识和了解，同时学会使用 SEEDLABS 网站进行网络安全的网上学习，提高自主学习的能力。

二. 实验环境及过程

实验环境为在 VM 虚拟机中运行的 SEEDUbuntu12.04 系统（系统已经由实验室配置好环境）。

实验过程参考该实验下提供的 PDF 的实验指导书完成。

详细过程略

三. 实验结果

```
[sudo] password for seed:
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth0
Number of packets: 10
Filter expression: ip

Packet number 1:
       From: 192.168.129.132
         To: 128.230.208.76
   Protocol: TCP
   Src port: 40021
   Dst port: 80

Packet number 2:
       From: 192.168.129.132
         To: 128.230.208.76
   Protocol: TCP
   Src port: 40022
```

```
[sudo] password for seed:
socket() - Using SOCK_RAW socket and UDP protocol is OK.
setsockopt() is OK.
Trying...
Using raw socket and UDP protocol
Using Source IP: 127.1.1.1 port: 234, Target IP: 193.123.123.11 port: 80.
Count #1 - sendto() is OK.
Count #2 - sendto() is OK.
Count #3 - sendto() is OK.
Count #4 - sendto() is OK.
Count #5 - sendto() is OK.
Count #6 - sendto() is OK.
```

```
Packet number 5:
       From: 192.168.129.132
         To: 128.230.208.76
   Protocol: TCP
   Src port: 40021
   Dst port: 80
   Payload (369 bytes):
00000   47 45 54 20 2f 7e 77 65  64 75 2f 73 65 65 64 2f    GET /~wedu/seed/
00016   6c 61 62 5f 65 6e 76 2e  68 74 6d 6c 20 48 54 54    lab_env.html HTT
00032   50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 77 77 77    P/1.1..Host: www
00048   2e 63 69 73 2e 73 79 72  2e 65 64 75 0d 0a 55 73    .cis.syr.edu..Us
00064   65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c    er-Agent: Mozill
00080   61 2f 35 2e 30 20 28 58  31 31 3b 20 55 62 75 6e    a/5.0 (X11; Ubun
00096   74 75 3b 20 4c 69 6e 75  78 20 69 36 38 36 3b 20    tu; Linux i686;
00112   72 76 3a 32 33 2e 30 29  20 47 65 63 6b 6f 2f 32    rv:23.0) Gecko/2
00128   30 31 30 30 31 30 31 20  46 69 72 65 66 6f 78 2f    0100101 Firefox/
00144   32 33 2e 30 0d 0a 41 63  63 65 70 74 3a 20 74 65    23.0..Accept: te
00160   78 74 2f 68 74 6d 6c 2c  61 70 70 6c 69 63 61 74    xt/html,applicat
00176   69 6f 6e 2f 78 68 74 6d  6c 2b 78 6d 6c 2c 61 70    ion/xhtml+xml,ap
00192   70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 3b 71 3d    plication/xml;q=
00208   30 2e 39 2c 2a 2f 2a 3b  71 3d 30 2e 38 0d 0a 41    0.9,*/*;q=0.8..A
00224   63 63 65 70 74 2d 4c 61  6e 67 75 61 67 65 3a 20    ccept-Language:
00240   65 6e 2d 55 53 2c 65 6e  3b 71 3d 30 2e 35 0d 0a    en-US,en;q=0.5..
```

实验总结

通过此次实验,我了解了 Heartbleed 攻击的危害,方式及解决方法,使自己对网络安全有一方面的认识和了解,同时学会了使用 SEEDLABS 网站进行网络安全的网上学习，提高自主学习的能力。

在包嗅探及欺骗上，我也了解了其基本工作原理，当然，还存在一些不足的地方，比如对包嗅探的一些深入探索，对于包嗅探的危害，我有了很直接的了解，这对以后面对此类问题有很好的帮助。

其次，在本次试验中也暴露了我的一些不足，比如对于 Linux 系统方面的理解，以及对于一些专业名词的英文不太熟悉等。这些都会促使我在信息安全道路上不断前行，这些将使我受益终生。