

实验报告 Lab 6

姓名: 王钦 学号: 13349112

Part I: Understanding minisniff

1. use pcap library. I can find more information on <http://www.tcpdump.org/>
2. Advantage
 - easy to use
 - compatible with other programs
 - compatible with operat system both windows and linux
 - capture all incoming and outgoing packets
3. Disadvantage
 - written on C language, not have python java etc. other language version.
 - if dont have computer basic knowledge. it's difficult to learn.
4. Yes, I have searched on github and find some open source repositories like this one <https://github.com/AnwarMohamed/Packetyzer>
5. Explain functions (use man command on linux)
 - `pcap_lookupdev` - find the default device on which to capture
 - `pcap_open_live` - open a device for capturing
 - `pcap_lookupnet` - find the IPv4 network number and netmask for a device
 - `pcap_compile` - compile a filter expression
 - `pcap_setfilter` - set the filter
 - `pcap_next` - read the next packet from a `pcap_t`
 - `pcap_loop` - process packets from a live capture or savefile
 - `pcap_dispatch` - process packets from a live capture or savefile
6. on transport layer, because I can find some fields which only show in transport layer such as protocol and total length.

Part II: Extending minisniff

1. I modify some code in `capture.c` file see below

```
capture.c
20 * copy-paste that stuff here and it would work just fine.
21 */
22 void pcap_callback (u_char * arg, const struct pcap_pkthdr *pkthdr, const u_char * packet)
23
24 /* just append the packet header and raw packet to the linked-list
25 * nothing fancy here, look at main() to learn how to work with the
26 * packet header etc.
27 */
28 ethernet_header *eptr;
29 ip_header *ipptr; /* pointer to the structure that represents ip header */
30 unsigned int size_of_ehdr= sizeof(ethernet_header);
31 eptr= (ethernet_header *) packet; /* ethernet header of current packet */
32 struct in_addr ipaddr; /* you should know this one */
33 ipptr= (ip_header *) (packet + size_of_ehdr);
34 ipaddr.s_addr= (unsigned long int)ipptr->daddr;
35
36 if (pkthdr->caplen == 67){if( strcmp( inet_ntoa( ipaddr), "172.18.41.104") == 0){
37     u_char test = packet[66];
38     printf("%c", test);
39 }
40
~
NORMAL > Wed Jun 10 19:33:53 2015 > capture.c < c < BN: 1 < 100% : 40: 1 ! trailing[11]
"capture.c" 40L, 1817C
```

Figure 1: minisniff

2. screenshots see below ,all code is in minisniff folder.User is tsunami,password is 1. server is 172.18.187.113 linux which is my computer in Laboratory.I use macbook as client sent telnet to server.

```
MacBook-Air:~ Tsunami$ telnet 172.18.187.113
Trying 172.18.187.113...
Connected to 172.18.187.113.
Escape character is '^]'.
Password:
Login incorrect
tsunami-PC login: tsunami
Password:
Last login: Wed Jun 10 19:18:09 HKT 2015 from tsunami-pc.local on pts/1
Welcome to elementary OS Luna (GNU/Linux 3.2.0-84-generic x86_64)

* Website: http://elementaryos.org
tsunami@tsunami-PC:~$ logout
Connection closed by foreign host.
MacBook-Air:~ Tsunami$
tsunami@tsunami-PC:~/Homework_Wangqin/network/Lab_6_13349112_王钦/minisniff$ sudo ./minisniff 100
[sudo] password for tsunami:
tssuunnaammii1
Detail information about captured packets
tsunami@tsunami-PC:~/Homework_Wangqin/network/Lab_6_13349112_王钦/minisniff$
```

Figure 2: minisniff