Skill 2

Install Aircrack-ng 3

使用Aircrack-ng破解无线密码 3

开启monitor mode 4

Eclipse 4

MPI 4

FileZilla 4

Usage of g++ 4

MySQL 5

Tcpdump 7

PCAP 7

Wireshark 7

Pthread 7

RSSI 8

Geany 8

Socket Programming 8

Libsvm 8

Wireless 8

PHP 9

Skill

1) system中command若有双引号，双引号之前加\

Reference: http://stackoverflow.com/questions/16004913/executing-terminal-command-from-c-program-doesnt-behave-as-i-would-expect

2) login as root

root is the default username of superuser, thus change the password means change the root password

sudo passwd

sudo nano /etc/ssh/sshd_config

PermitRootLogin yes

sudo service ssh restart

3) manage time in ubuntu through command line

http://codeghar.wordpress.com/2007/12/06/manage-time-in-ubuntu-through-command-line/

http://my.oschina.net/jackguo/blog/94707

4) Memory debugging

-- cd ./workspace/Sniffer/Debug/

-- sudo valgrind --tool=memcheck --leak-check=yes --show-reachable=yes --num-callers=20 --track-fds=yes ./Sniffer

5) still reachable: 99,148 bytes in 29 blocks

explanation:

http://stackoverflow.com/questions/3840582/still-reachable-leak-detected-by-valgrind

solution:

http://blog.csdn.net/weihua1984/article/details/5835731

6) open() read() write() close()

http://gd.tuwien.ac.at/languages/c/programming-bbrown/c_075.htm

7) stack，heap

http://blog.csdn.net/hairetz/article/details/4141043

http://www.cnblogs.com/buddy/archive/2012/09/28/2706787.html

8) 如何让程序优雅地退出 ctrl+c

http://stackoverflow.com/questions/1641182/how-can-i-catch-a-ctrl-c-event-c

9) 图片文件格式

gif文件格式

http://blog.csdn.net/friendwaters/article/details/2737328

jpg文件格式

http://www.cnblogs.com/RobotTech/archive/2008/07/21/1247721.html

http://blog.csdn.net/lpt19832003/article/details/1713718

png文件格式

http://blog.csdn.net/bisword/article/details/2777121

http://dev.gameres.com/Program/Visual/Other/PNGFormat.htm

bmp文件格式
http://wojiaolongyinong.iteye.com/blog/1896092

10) change date zone
sudo dpkg-reconfigure tzdata

Install Aircrack-ng

Reference: http://www.maybe520.net/blog/1744/

1) 首先安装两个扩展

sudo apt-get install build-essential
sudo apt-get install libssl-dev

2) 然后到http://download.aircrack-ng.org/aircrack-ng-1.1.tar.gz 下载最新版的aircrack-ng，解压它

tar -xvf aircrack-ng-1.1.tar.gz

3) cd aircrack-ng-1.1

gedit common.mak

找到 CFLAGS ?= -g -W -Wall -Werror -O3 并把它改为

CFLAGS ?= -g -W -Wall -O3

保存好后，开始编译安装

make
sudo make install

4) 完了之后它会提示 Run ‘airodump-ng-oui-update’ as root (or with sudo) to install or update Airodump-ng OUI file (Internet connection required).

于是输入

sudo airodump-ng-oui-update

更新好后即可。

使用Aircrack-ng破解无线密码

Reference: http://www.maybe520.net/blog/1744/

1) 启动无线网卡的监控模式，在终端中输入：sudo airmon-ng start wlan0
（wlan0是无线网卡的端口,可用命令 ifconfig 查看）

2) 查看无线AP在终端中输入：
sudo airodump-ng mon0
（mon0 是启动监控模式后无线网的端口）
查看有哪些采用wep加密的AP在线，然后按 ctrl+c 中止，不要关闭终端。

3) 抓包
打开另一个终端，输入：
sudo airodump-ng -c 6 –bssid AP’s MAC -w wep mon0 （此处有误，-bssid 改为 --bssid）

(-c 后面跟着的6是要破解的AP工作频道，–bissid后面跟着的AP'sMAC是要欲破解AP的MAC地址，-w后面跟着wep的是抓下来的数据包DATA保存的文件名，具体情况根据步骤2里面的在线AP更改频道和MAC地址，DATA保存的文件名可随便命名）
// to be checked
sudo airmon-ng start wlan0
sudo airodump-ng mon0
sudo airodump-ng --channel 1 --bssid C8:D3:A3:63:63:D1 -w dlink mon0
sudo aireplay-ng -1 0 -a C8:D3:A3:63:63:D1 -h c0:4a:00:10:54:40 mon0

开启monitor mode

sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ifconfig wlan0 up

Eclipse

1) Installation
sudo apt-get install eclipse-cdt eclipse
sudo apt-get install eclipse-platform
2) add -lpcap in eclipse library
properties --> c/c++ build --> settings --> Cross G++ Linker --> Libraries --> add pcap
3) how to debug application as root in eclipse in Ubuntu?
http://stackoverflow.com/questions/2891356/how-to-debug-application-as-root-in-eclipse-in-ubuntu
gksu eclipse
4) uninstall eclipse
sudo apt-get autoremove eclipse*
rm -r ~/.eclipse/

MPI

1) Installation
sudo apt-get install libcr-dev mpich2 mpich2-doc
2) ssh configure
https://source.ggy.bris.ac.uk/wiki/Configure_ssh_for_MPI

FileZilla

1) Installation
sudo add-apt-respository ppa:n-muench/programs-ppa
sudo apt-get update
sudo apt-get install filezilla

Usage of g++

-c 只激活预处理，编译和汇编，只把程序做成obj文件（将生成.o的obj文件）
-O by using this flag, the executable file should execute more quickly although compilation may take longer
-Wall a contraction of warning all, will warn us of anything unexpected that is not actually an error, but will still create an executable file

-Werror to treat anything unexpected as error and, therefore, not to create an executable file when this occurs

-lm to link to a library of mathematical routines

MySQL

1) Installation

sudo apt-get install mysql-server mysql-client

2) libmysqlclient Installation

sudo apt-get install libmysqlclient-dev

3) mysql_query() -- mysql_real_query()

https://dev.mysql.com/doc/refman/5.0/en/mysql-query.html

https://dev.mysql.com/doc/refman/5.0/en/mysql-real-query.html

4) mysql_store_result() mysql_fetch_row() mysql_free_result()

http://dev.mysql.com/doc/refman/5.0/en/mysql-store-result.html

http://dev.mysql.com/doc/refman/5.0/en/mysql-fetch-row.html

http://dev.mysql.com/doc/refman/5.0/en/mysql-free-result.html

5) load data into sql from documents

References: http://www3.ntu.edu.sg/home/ehchua/programming/sql/MySQL_Beginner.html#zz-2.4

http://dev.mysql.com/doc/refman/5.1/en/load-data.html

```
-> LOAD DATA LOCAL INFILE 'd:/path-to/products_in.csv' INTO TABLE products
-> COLUMNS TERMINATED BY ','
-> LINES TERMINATED BY '\r\n';
```

6) MySQL多行合并

http://bbs.csdn.net/topics/110005890

```
-> select id,group_concat(re_id order by re_id separator ", ") as re_id
-> from tablename
-> group by id
```

7) MySQL取平均值合并

```
-> SELECT student_name, AVG(test_score)
->       FROM student
->       GROUP BY student_name;
```

8) 从已知table选取数据建立新table

```
-> create table t2 select name, avg(id) as id from t1 group by name;
```

9) 清空表中所有数据

```
-> truncate table t3
```

10) 从已建立表格中选择数据建立新表格，新表格规定格式

```
-> create table t4(MACAdd varchar(17), AvgRSSI int)
-> select MACAdd, avg(RSSI) as AvgRSSI
-> from t3
-> group by MACAdd;
```

11) MySQL add new column “Time”
-> drop table MACRecord;
-> create table if not exists MACRecord(MACAdd varchar(17), RSSI TINYINT, Record SMALLINT, Timestamp timestamp default current_timestamp on update current_timestamp);

12) delete mobile add if it has been in the db for more than 3 days
-> select * from MACRecord where date_sub(curdate(),interval 2 day) = Timestamp;
which means that curdate - timestamp > 3 days
-> delete from MACRecord where date_sub(curdate(),interval 2 day) >= Timestamp and Record = 1;
-> update MACRecord set Record = Record + 1 where timestampdiff(hour,Timestamp,curtime()) > 1 and Record < 6;

13) mysql restart
http://superuser.com/questions/282115/how-to-restart-mysql
Start:
sudo /etc/init.d/mysql start
Stop:
sudo /etc/init.d/mysql stop
Restart / reload configs:
sudo /etc/init.d/mysql restart
Check run status:
sudo /etc/init.d/mysql status

14) how to connect to sql server from other computers
/etc/mysql/my.cnf
bind-address = 127.0.0.1
-- sudo /etc/init.d/mysql restart
(for connecting)

->grant all privileges on *.* to ‘root’@’ip’ identified by ‘root’;
->flush privileges;
->grant all privileges on *.* to ‘root’@’%’ identified by ‘root’;
->flush privileges;
(privileges allow connect)

for client
-- mysql -u username -p -h ip

15) insert if not exists update if exists
http://dev.mysql.com/doc/refman/5.0/en/insert-on-duplicate.html

16) Alter table
http://www.tech-recipes.com/rx/378/add-a-column-to-an-existing-mysql-table/
ALTER TABLE contacts ADD email VARCHAR(60);
ALTER TABLE contacts ADD email VARCHAR(60) AFTER name;
ALTER TABLE contacts ADD email VARCHAR(60) FIRST;

17) update table according to time

-> UPDATE MACRecord SET RSSI2 = IF(timestampdiff(minute,Timestamp,now()) < 2,-77,-90) WHERE MACAdd = "80-EA-96-C6-7C-7A";

-> INSERT INTO MACRecord(MACAdd,RSSI2,Record) values ("80-EA-96-C6-7C-7A",-90,1) on duplicate key update RSSI1 = IF(timestampdiff(minute,Timestamp,now()) < 2,RSSI1,0), RSSI2 = VALUES(RSSI2), Record = IF(Record = 25, 25, VALUES(Record));

18) copy mysql from one server to another
http://www.cyberciti.biz/tips/howto-copy-mysql-database-remote-server.html
-- for old server
-> mysqldump -u root -p -h 172.22.189.152 HAS MACTrain > MACTrain.sql;
-- for new server
-> mysql -u root -p HAS < MACTrain.sql;

Tcpdump

1) Installation
sudo apt-get install tcpdump

PCAP

1) Installation
sudo apt-get install libpcap-dev

2) callback function writing in pcap
http://yuba.stanford.edu/~casado/pcap/section3.html

3) radiotap
http://www.radiotap.org/defined-fields/Flags

4) 80211
http://www.technologyuk.net/telecommunications/networks/wireless_networks.shtml

Wireshark

1) Installation
cause: rawshark: not found
apt-get install wireshark
-- cd /usr/share/wireshark
-- nano init.lua
> line #29 change to: disable_lua = true

Pthread

1) pthread编程 ubuntu c++多线编程
http://blog.csdn.net/hitwengqi/article/details/8015646

2) pthread_cond_wait()用法
http://blog.csdn.net/hairetz/article/details/4535920

3) pthread 执行顺序

http://blog.csdn.net/harry_lyc/article/details/6055734

4) Install mpi on ubuntu
http://jetcracker.wordpress.com/2012/03/01/how-to-install-mpi-in-ubuntu/
sudo apt-get install libcr-dev mpich2 mpich2-doc
mpicc mpi_hello.c -o hello
mpirun -np 2 ./hello

5) pthread_create
http://man7.org/linux/man-pages/man3/pthread_create.3.html
#include <pthread.h>
int pthread_create(pthread_t *thread, const pthread_attr_t *attr, void *(*start_routine) (void *), void *arg);
Compile and link with -pthread.

RSSI

1) why wifi worse on smartphone than on laptops and computers
http://pocketnow.com/2013/06/28/smartphone-wifi-performance

Geany

1) Installation
sudo get-install geany

Socket Programming

1) Socket Programming in C on Linux
http://www.binarytides.com/socket-programming-c-linux-tutorial/

Libsvm

1) Usage

http://blog.csdn.net/meredith_leaf/article/details/6714144

Wireless

1) change the display name of wireless card
http://hi.baidu.com/tian___tian/item/86aa541c50ace313e3f986fd
sudo gedit /etc/udev/rules.d/70-persistent-net.rules

2) check wireless driver version
http://askubuntu.com/questions/333424/how-can-i-check-the-information-of-currently-installed-wifi-drivers
sudo lshw -C network
lshw lists information on your hardware
C network filters the output to only show the network class.
modinfo <driver-name>

find /lib/modules/$(uname -r)/kernel/drivers/net/wireless -name '*.ko'

3) to get encrypted pass phrase
wpa_passphrase [ssid] [passphrase]

PHP

1) install
fatal error: call to undefined function mysqli_connect()

```
sudo apt-get install apache2
sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt
sudo apt-get install php5-mysql
sudo apt-get install php5-cli
```

2) allow access
sudo chown -R www-data:www-data /var/www/test_folder