Wireless Authentication, Authorization and Accounting-2 Without AP version

Speaker: Chia-Peng Lee

Date: 2019/3/20

Mobile Communications Networking Lab, NTU

注意事項

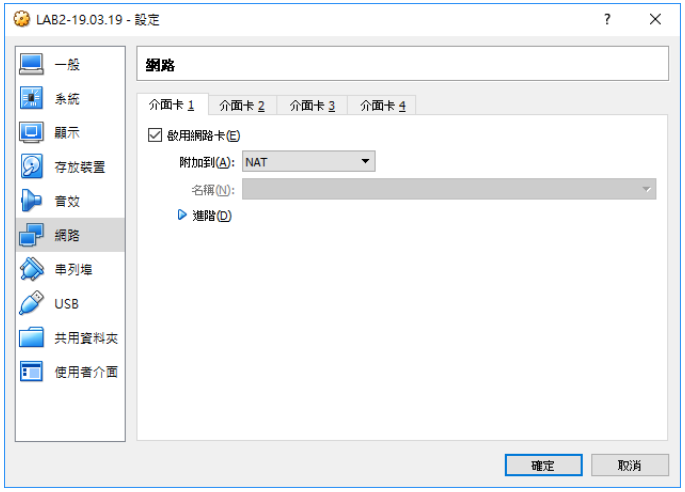
- 實驗(二)上機實驗時間 (@ R204)
  - 時間: 2019/3/27 14:20~17:10
- 實驗(二)展演及實驗結報繳交 (@ R204)
  - 時間: 2019/4/10 14:20~17:20
  - 實驗結報繳交方式:
    - 一律使用電子郵件繳交電子檔 (一組只要繳交一份)，
    - 郵件主旨範例如 [CNL實驗(二)結報繳交_組別], 最晚當天繳交完畢。
- 下次上課 (@ R204)
  - 時間: 2019/4/24 14:20~17:10

實驗說明

- 設計一無線區域網路使用者認證機制，可供使用者認證之用，並且統計每個使用者使用此無線區域網路之流量與時間，進以實作流量控管與流量監測。同時也要為這兩項功能寫個供管理者控管及供使用者操作的網頁介面。
- 本次實驗完成下列事項
  - 完成WLAN認證功能
  - 撰寫一個網頁管理介面完成下列功能
    - 流量監測
    - 流量控管
    - 使用者註冊、登入與登出

實驗環境網路架構


Internet


LAB2-19.03.19 - 設定
一般
系統
顯示
存放裝置
音效
網路
串列埠
USB
共用資料夾
使用者介面
網路
介面卡 1
介面卡 2
介面卡 3
介面卡 4
啟用網路卡(E)
附加到(A):
NAT
名稱(N):
進階(D)
確定
取消

實驗環境軟體安裝

- 電腦A with wireless card
  - RADIUS server
  - MySQL server
  - CoovaChilli
- 電腦B (NoteBook)
  - NoteBook
  - PC with wireless card
- 作業系統
  - Ubuntu 18.04.2

實驗環境架設

- **Upgrade**
  - #sudo apt update
  - #sudo apt upgrade
- **Install MariaDB FreeRADIUS**
  - #sudo apt install default-jre-headless
    - If fails
      - #sudo apt purge openjdk-8-jre-headless
  - #sudo apt install mariadb-server
  - #sudo apt install freeradius freeradius-mysql

https://wiki.freeradius.org/guide/SQL-HOWTO-for-freeradius-3.x-on-Debian-Ubuntu

實驗環境架設
Configuring FreeRADIUS

- **Configuring FreeRADIUS**
  - #sudo -s
  - #mysql -u root
    - CREATE DATABASE radius;
    - quit;
  - #cd /etc/freeradius/3.0/
  - #mysql -u root radius < mods-config/sql/main/mysql/schema.sql
  - #mysql -u root radius < mods-config/sql/main/mysql/setup.sql
  - #mysql -u root
    - use radius;
    - insert into radcheck (username,attribute,op,value) values("test", "Cleartext-Password", ":=", "testpwd");
    - quit;

實驗環境架設
Configuring FreeRADIUS

- **Configuring FreeRADIUS**
  - #cd mods-enabled
  - #ln -s ../mods-available/sql sql
  - #cd ..
  - #cd sites-available
  - #gedit default
    - (uncomment sql under authorize {} & accounting{})
  - #gedit inner-tunnel
    - (uncomment sql under authorize {})
  - #cd ..
  - #gedit mods-enabled/sql
    - change driver = "rlm_sql_null" to driver = "rlm_sql_mysql"
    - also uncomment and result like this:

```
# Connection info:
#
server = "localhost"
port = 3306
login = "radius"
password = "radpass"
```

實驗環境架設
Configuring FreeRADIUS

- **Configuring FreeRADIUS**
  - #systemctl stop freeradius
  - #systemctl start freeradius
  - #radtest test testpwd localhost 0 testing123
  - should get Access-Accept

```
root@raspberrypi:/etc/freeradius/3.0# radtest test testpwd localhost 0 testing12
3
Sent Access-Request Id 39 from 0.0.0.0:60195 to 127.0.0.1:1812 length 74
        User-Name = "test"
        User-Password = "testpwd"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "testpwd"
Received Access-Accept Id 39 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
root@raspberrypi:/etc/freeradius/3.0#
```

  - #exit

實驗環境架設
Install&Configuring CoovaChilli

- **Install CoovaChilli**
  - #wget https://github.com/coova/coova-chilli/archive/1.4.tar.gz
  - #tar -zxvf 1.4.tar.gz
  - #cd coova-chilli-1.4
  - #sudo apt install devscripts gengetopt libjson-c-dev
  - #sudo apt install libssl1.0-dev debhelper
  - #gedit debian/control
    - change Build-Depends:…libssl-dev to libssl1.0-dev

```
Priority: optional
Maintainer: David Bird (Coova Technologies) <support@coova.com>
Build-Depends: debhelper (>= 7), libc6-dev | libc6-dev-amd64, gengetopt, libtool, automake,
libssl1.0-dev
Standards-Version: 3.8.1
```

  - #debuild -b
  - (will see no secret key)
  - #cd ..

```
gpg: /tmp/debsign.1f19Mnfr/coova-chilli_1.3.0_armhf.buildinfo: clear-sign failed
: No secret key
debsign: gpg error occurred!  Aborting....
debuild: fatal error at line 1045:
running debsign failed
pi@raspberrypi:~/coova-chilli-1.4 $
```

實驗環境架設

Install&Configuring CoovaChilli

- **Install CoovaChilli**
  - #sudo apt install haserl
  - #sudo dpkg --install coova-chilli_1.3.0_amd64.deb
- **Configuring CoovaChilli**
  - #sudo gedit /etc/chilli/defaults
    - (HS_WANIF=enp0s3)
    - (HS_LANIF=enp0s8)
  - #sudo gedit /etc/default/chilli
    - START_CHILLI=1
  - #cd /etc/NetworkManager
  - #sudo gedit NetworkManager.conf
    - unmanaged-devices=interface-name:enp0s8
  - #sudo systemctl restart NetworkManager
  - #cd ..
  - #cd network

實驗環境架設
Install&Configuring CoovaChilli

- **Configuring CoovaChilli**
  - #sudo gedit interfaces
    - add following

      #access point

      iface enp0s8 inet static

      address 10.1.0.1

      Netmask 255.255.255.0

      Gateway 10.1.0.1

      Wireless-mode Master

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

#access point
iface enp0s8 inet static
address 10.1.0.1
Netmask 255.255.255.0
Gateway 10.1.0.1
Wireless-mode Master
```

  - #sudo systemctl restart networking
  - #sudo gedit /etc/chilli/up.sh ADD
    - iptables -I POSTROUTING -t nat -o $HS_WANIF -j MASQUERADE

實驗環境架設

Install&Configuring CoovaChilli

- **Configuring CoovaChilli**
  - #sudo apt install hostapd
  - #cd /etc/hostapd
  - #sudo gedit hostapd.conf

    interface= enp0s8

    driver=nl80211

    ssid=PIAP

    hw_mode=g

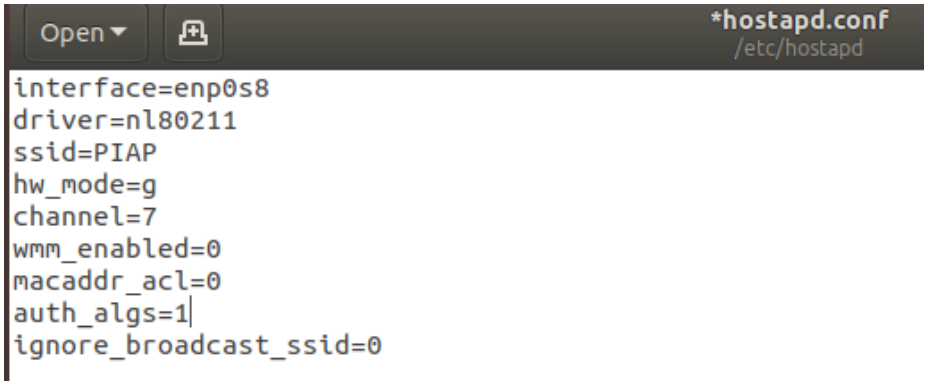
    channel=7

    wmm_enabled=0

    macaddr_acl=0

    auth_algs=1

    ignore_broadcast_ssid=0



實驗環境架設
Install&Configuring CoovaChilli

- **Configuring CoovaChilli**
  - #cd /etc/default
  - #sudo gedit hostapd
    - uncommand
    - DAEMON_CONF="/etc/hostapd/hostapd.conf“

```
# file can be found at /usr/share/doc/hostapd/e
#
DAEMON_CONF="/etc/hostapd/hostapd.conf"

# Additional daemon options to be appended to h
#       -d   show more debug messages (-dd for
```

  - #cd /etc
  - #sudo gedit sysctl.conf

    net.ipv4.ip_forward=1

```
# See http://lwn.net/Articles/277.
# Note: This may impact IPv6 TCP s
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enabl
net.ipv4.ip_forward=1
```

- #sudo systemctl start freeradius
- #sudo systemctl start chilli
- #sudo systemctl unmask hostapd (第一次啟動才需要)
- #sudo systemctl start hostapd

實驗二展演要求

- 架設CoovaChilli (20%)。
- 實作以下功能:
  - 使用者註冊(3%)
  - 使用者登出(3%)
  - 顯示使用者流量與使用時間的功能(7%)
  - 根據不同的使用者限制流量與使用時間的功能(7%)
    - 超過時間或是超過流量，即時踢掉使用者
- 展示資料庫內容並說明各張 tables 負責的功能，請刪除不需要用到的 table (10%)。

實驗二結報要求

- WLAN Authentication Mechanism (30%)
  1. 說明目前市面上對於無線區域網路所提出之認證機制其優缺點。
  2. 說明提出之認證機制的運作原理。
  3. 說明對於所提出之認證機制其漏洞預防措施為何。
- 網頁介面 (20%)
  1. 說明使用之web介面技術。
  2. 說明你們設計的網頁的運作方式。