

# **Práctica**

# **Seguridad Servidor Radius**

**Franco Larrea**

2º SMR-A

(Prof. Fernando Albert González)

Instituto IES SAN VICENTE

# Índice

Teoría.....	Pag. 3
Tareas y cuestiones.....	Pag. 4-7
Problemas encontrados.....	Pag. 8
Fuentes.....	Pag. 9
Alumnos participantes.....	Pag. 9

# Teoría

Para realizar esta practica es conveniente saber algunos conceptos:

## **Servidor Radius**

### **¿Que es?**

RADIUS es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc. Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuándo comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

## **WPA Enterprise**

### **¿Que es?**

Este modo proporciona la seguridad necesaria para las redes inalámbricas en el mundo empresarial. Es más complicado configurar, y ofrece control individualizado y centralizado sobre el acceso a su red Wi-Fi. Cuando los usuarios tratan de conectarse a la red, necesitan presentar sus credenciales de acceso al sistema. Este modo soporta la autenticación de 802.1x RADIUS y es adecuado en los casos donde se utiliza un servidor RADIUS. WPA-Enterprise sólo debe ser usado cuando un servidor RADIUS está conectado para la autenticación de cliente.

Los usuarios nunca tratan con los códigos de encriptado. Son creados y asignados de manera segura por sesión del usuario en un segundo plano después que un usuario presenta sus credenciales de acceso al sistema. Esto evita que la gente obtenga las claves de la red de las computadoras.

## **freeRadius**

### **¿Que es?**

FreeRADIUS es un conjunto de RADIUS gratuito modular de alto rendimiento desarrollado y distribuido bajo la Licencia Pública General de GNU, versión 2, y es gratuito para descargar y usar.

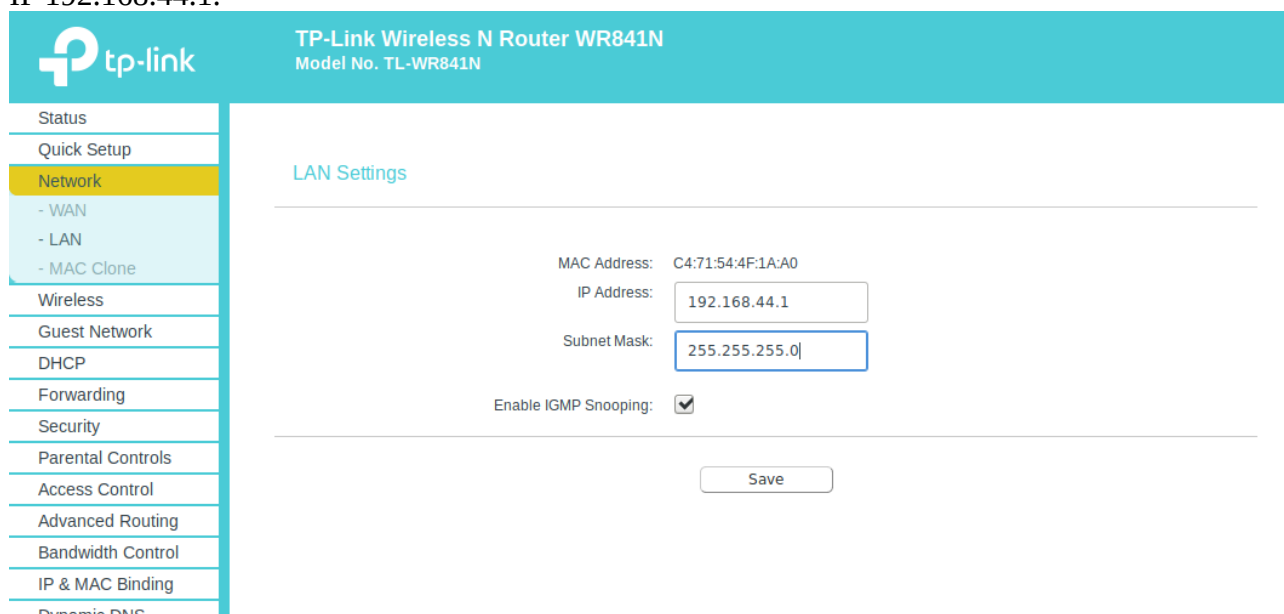
## En esta práctica aprenderemos como instalar y configurar un Servidor Radius.

*Esta práctica se ha realizado con un router “TP-LINK” y con una maquina Ubuntu 18.04.*

Primero conectaremos el router al ordenador mediante un cable Ethernet para cofigurarlo. Una vez conectado y encendido el router accederemos a la configuración de este mediante algún navegador.

Simplemente pondremos la IP del router en la barra de búsqueda y nos debería aparecer un login. Tras autenticarnos con el usuario “admin” y la contraseña “admin” podremos configurar el router.

En el apartado “Network-LAN” modificaremos el apartado “IP Address”, nosotros hemos puesto la IP 192.168.44.1.

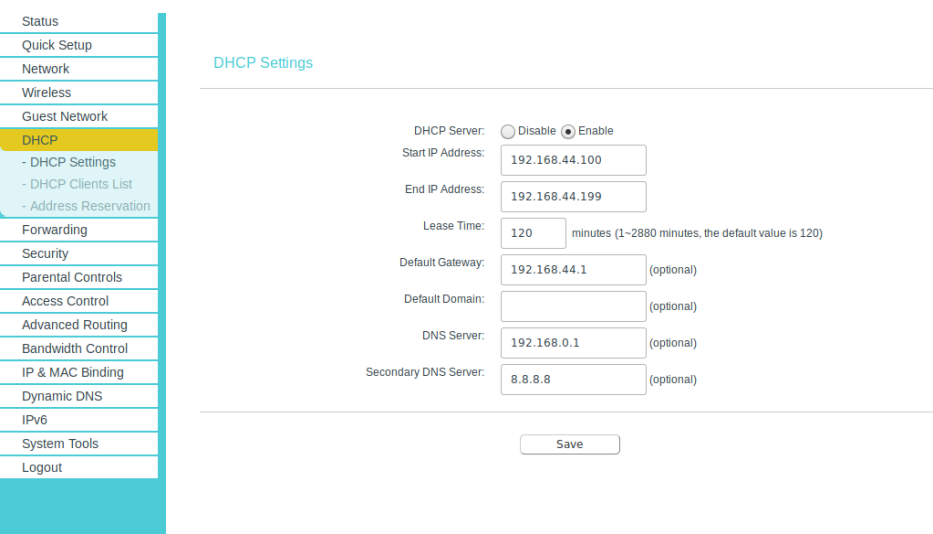


TP-Link Wireless N Router WR841N  
Model No. TL-WR841N

LAN Settings

MAC Address: C4:71:54:4F:1A:A0  
IP Address: 192.168.44.1  
Subnet Mask: 255.255.255.0  
Enable IGMP Snooping: ☒

Save



DHCP Settings

DHCP Server: ☐ Disable ☒ Enable  
Start IP Address: 192.168.44.100  
End IP Address: 192.168.44.199  
Lease Time: 120 minutes (1~2880 minutes, the default value is 120)  
Default Gateway: 192.168.44.1 (optional)  
Default Domain: (optional)  
DNS Server: 192.168.0.1 (optional)  
Secondary DNS Server: 8.8.8.8 (optional)

Save

A continuación configuraremos el rango de IPs asignadas mediante DHCP.

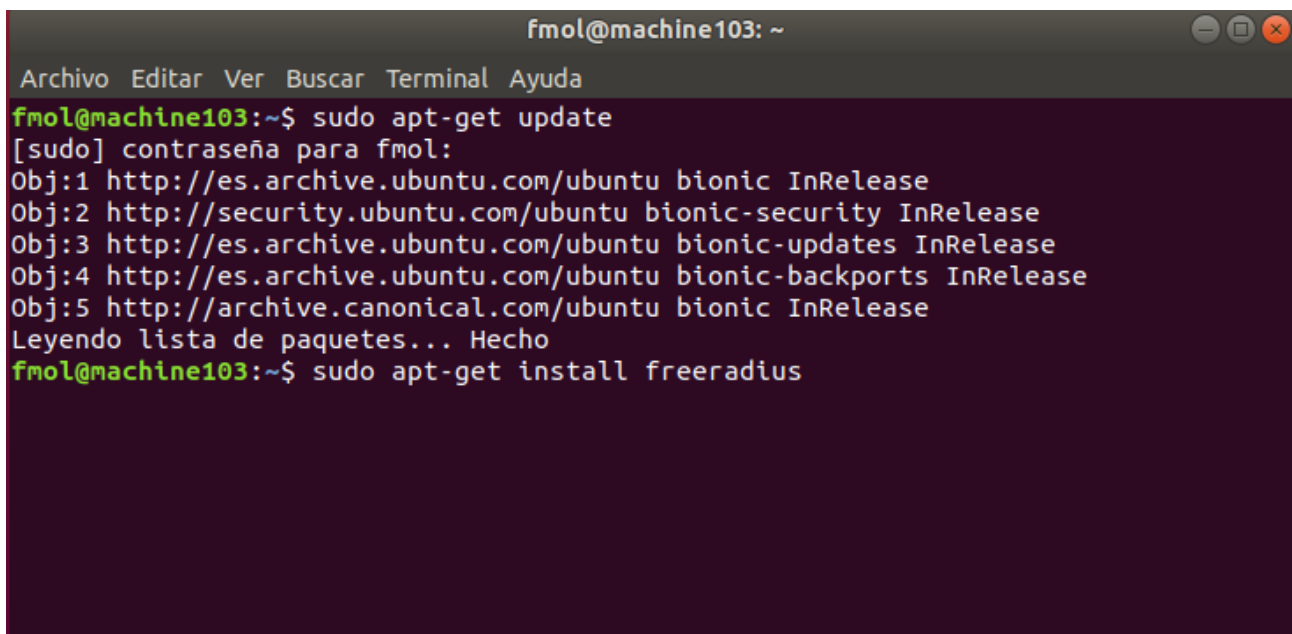
Iremos al apartado “Guest Network – DHCP Settings” y pondremos la IP 192.168.44.100 en el campo “Start IP Address” y la IP 192.168.44.199 en el campo “End IP Address”.

Ahora el router asignara a los equipos que se conecten IPs entre 192.168.37.100 y 192.168.37.199.

Antes de terminar de configurar el router configuraremos freeradius en alguna maquina linux. En este caso hemos usado una maquina Ubuntu 18.04.

Abriremos un terminal y teclearemos los siguientes comandos:

- `sudo apt-get update`
- `sudo apt-get install freeradius`



```
fmol@machine103: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
fmol@machine103:~$ sudo apt-get update  
[sudo] contraseña para fmol:  
Obj:1 http://es.archive.ubuntu.com/ubuntu bionic InRelease  
Obj:2 http://security.ubuntu.com/ubuntu bionic-security InRelease  
Obj:3 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease  
Obj:4 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease  
Obj:5 http://archive.canonical.com/ubuntu bionic InRelease  
Leyendo lista de paquetes... Hecho  
fmol@machine103:~$ sudo apt-get install freeradius
```

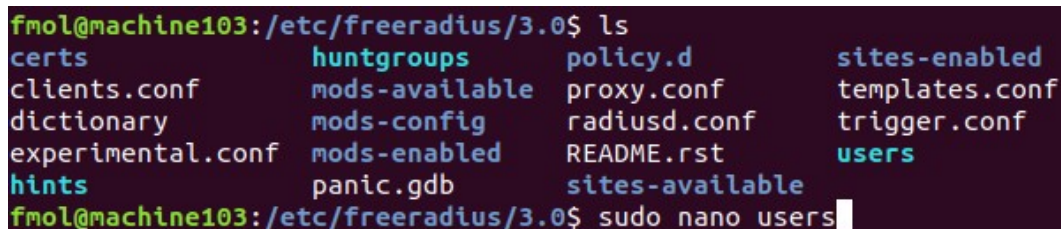
Después de esto se comenzará a instalar freeradius.

Una vez se haya instalado el programa iremos a `/etc/freeradius/3.0/`.

Dentro de este directorio modificamos el fichero `users` indicando en cada linea el usuario que queremos añadir al servidor Radius.

Para esto he empleado el editor *nano* desde la terminal con el siguiente comando:

- `sudo nano users`



```
fmol@machine103:/etc/freeradius/3.0$ ls  
certs          huntgroups     policy.d       sites-enabled  
clients.conf   mods-available proxy.conf     templates.conf  
dictionary     mods-config    radiusd.conf  trigger.conf  
experimental.conf mods-enabled    README.rst    users  
hints          panic.gdb      sites-available  
fmol@machine103:/etc/freeradius/3.0$ sudo nano users
```

He añadido cuatro líneas al fichero *users* una para cada usuario que quería crear.

Todas las líneas tenían que seguir la misma sintaxis:

- `<nombreusuario> Cleartext-Password := "<contraseña>"`

En la siguiente captura podemos ver cada usuario con sus respectivas contraseñas:

```
GNU nano 2.9.3 users Modificado
#
# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name.  If you have
# users with spaces in their names, you must also change
# the "filter_username" policy to allow spaces.
#
# See raddb/policy.d/filter, filter_username {} section.
#
#"John Doe"      Cleartext-Password := "hello"
#                Reply-Message = "Hello, %{User-Name}"

fran             Cleartext-Password := "elite"
pablo            Cleartext-Password := "holaxd"
franco           Cleartext-Password := "machine"
fernando         Cleartext-Password := "1111"

#
# Dial user back and telnet to the default host for that port
#

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir     ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Después de esto deberemos configurar el fichero *clients.conf* añadiendo al final de este unas líneas.

El párrafo que he añadido tenía la siguiente sintaxis:

```
client <iprouter> {
    secret = <contraseñarouter>
    shortname = <nombrerouter>
}
```

Aquí podemos ver el fichero *client.conf* configurado:

```
#
# }
#}
client 192.168.44.1 {
    secret = admin
    shortname = gorrocoptero
}

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir     ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Solo nos quedaría reiniciar el servicio freeradius y ya lo tendríamos activo y configurado.  
Con el siguiente comando reiniciamos el servicio:

- `sudo service freeradius restart`

```
fmol@machine103:/etc/freeradius/3.0$ sudo service freeradius restart
fmol@machine103:/etc/freeradius/3.0$
```

Vamos a acabar de configurar el router. Iremos a “Wireless > Wireless Security”

Marcaremos la casilla “WPA/WPA2 – Enterprise”.

Pondremos en “RADIUS Server IP” la ip de nuestro servidor radius(192.168.44.101).

(Esta ip es la de la maquina donde tengamos instalada freeradius. Con un **ip address** lo podemos ver.)

```
fmol@machine103:/etc/freeradius/3.0$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f8:dd:06 brd ff:ff:ff:ff:ff:ff
    inet 192.168.44.101/24 brd 192.168.44.255 scope global dynamic noprefixroute enp0s3
        valid_lft 6340sec preferred_lft 6340sec
    inet6 fe80::bba0:abd5:6132:8996/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Por ultimo en “RADIUS Server Password” pondremos la contraseña “admin”.

The screenshot shows the 'Wireless Security' configuration page. On the left, a sidebar lists various settings, with 'Wireless Security' selected. The main area shows the 'WPA/WPA2 - Enterprise' configuration. The 'Authentication Type' is set to 'Auto', and the 'Encryption' is also set to 'Auto'. The 'RADIUS Server IP' is entered as '192.168.44.101'. The 'RADIUS Server Port' is set to '1812', with a note indicating that 0 stands for the default port 1812. The 'RADIUS Server Password' is entered as 'admin'. The 'Group Key Update Period' is set to '0'.

Con esto ya tendríamos configurado el servidor radius y el router.

## Problemas encontrados:

- He intentado cifrar las contraseñas del archivo de configuración *users*. No he podido realizar esta tarea. Tras una extensa investigación he concluido que la documentación de freeradius es pésima.

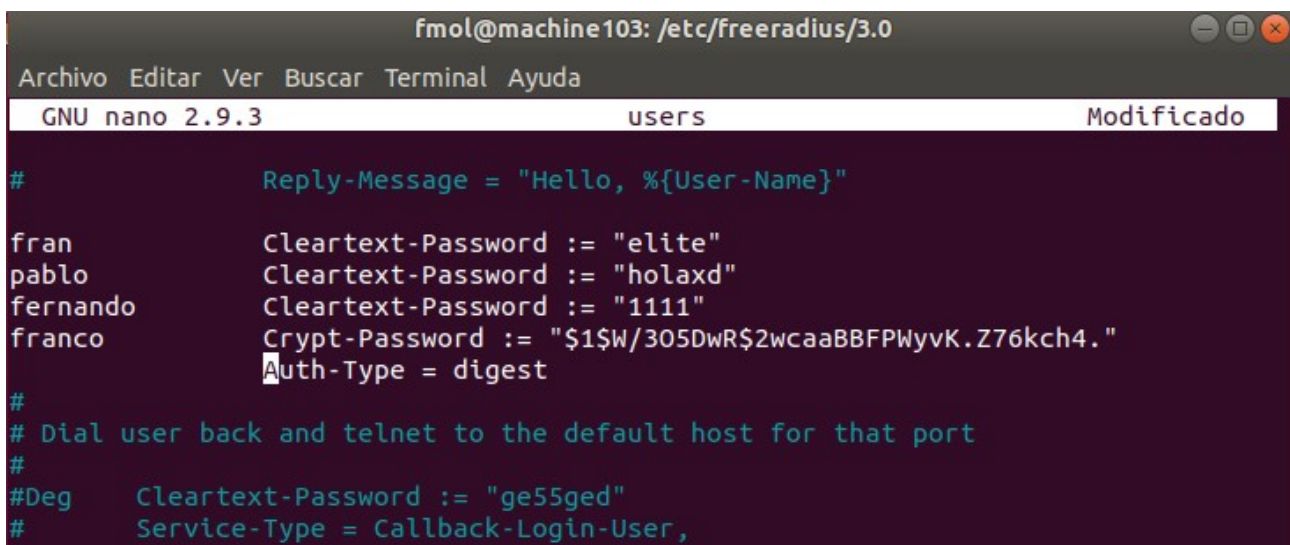
Cuando instalamos freeradius en un entorno linux también se instalan unas herramientas, entre ellas radcrypt.

Esta herramienta te permite encriptar contraseñas a md5 y comprobar las mismas.

El siguiente comando encriptaba la contraseña “machine” con md5:

```
fmol@machine103:~$ radcrypt --md5 machine
$1$W/305DwR$2wcaaBBFPWyvK.Z76kch4.
```

He intentado incluir la contraseña cifrada al archivo **users** con distintas sintaxis. He concluido que si la sintaxis es incorrecta salta un error al reiniciar el servicio con **sudo systemctl restart freeradius**.



```
fmol@machine103: /etc/freeradius/3.0
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.9.3      users      Modificado
#          Reply-Message = "Hello, %{User-Name}"

fran      Cleartext-Password := "elite"
pablo     Cleartext-Password := "holaxd"
fernando  Cleartext-Password := "1111"
franco    Crypt-Password := "$1$W/305DwR$2wcaaBBFPWyvK.Z76kch4."
          Auth-Type = digest
#
# Dial user back and telnet to the default host for that port
#
#Deg      Cleartext-Password := "ge55ged"
#         Service-Type = Callback-Login-User,
```



## Fuentes:

- <https://es.wikipedia.org/wiki/RADIUS>
- [https://www.gnu.org/software/radius/manual/html\\_node/Encrypted-Password-Auth.html](https://www.gnu.org/software/radius/manual/html_node/Encrypted-Password-Auth.html)
- <https://hub.packtpub.com/storing-passwords-using-freeradius-authentication/>
- [https://wiki.freeradius.org/modules/Rlm\\_digest#Clear\\_text\\_password\\_storage](https://wiki.freeradius.org/modules/Rlm_digest#Clear_text_password_storage)
- <https://www.dslreports.com/forum/r26973260-FreeRADIUS-encrypted-passwords>
- <http://lists.freeradius.org/pipermail/freeradius-users/2012-April/060271.html>
- <https://freeradius.org/radiusd/man/users.html>
- <http://manpages.ubuntu.com/manpages/bionic/man8/radcrypt.8.html>
- <https://freeradius.org/radiusd/man/radcrypt.html>
- <http://deployingradius.com/documents/configuration/pap.html>

## Alumnos participantes:

- Franco Matias Oscar Larrea
- Francisco Gomez Benimeli
- Pablo Diaz Rueda