Universidad Politécnica de Cartagena

Escuela Técnica Superior de Ingeniería de Telecomunicación

SEGURIDAD EN REDES DE COMUNICACIONES

Práctica 2: Autenticación. RADIUS y EAP (Extensible Authentication Protocol)

María Dolores Cano Baños

Natalio López Martínez

Objetivos

Al finalizar la práctica el alumno debe ser capaz de:

- Configurar un servidor RADIUS.
- Configurar un cliente EAP.
- Configurar un switch para ser utilizado como autenticador en un sistema de autenticación basado en EAP con servidor de autenticación RADIUS.
- Conocer el funcionamiento general del sistema de autenticación EAP con RADIUS (mensajes que se intercambian, etc.)

RADIUS

RADIUS (*Remote Authentication Dial-In User Services*) es un protocolo de autenticación ampliamente utilizado que permite tener la autenticación, la autorización y la contabilidad centralizadas para el acceso de red. Desarrollado inicialmente para acceso remoto *dial-up* (marcado manual), RADIUS es soportado actualmente por servidores VPN (*Virtual Private Network*), puntos de acceso inalámbricos, conmutadores de autenticación Ethernet, acceso DSL (*Digital Subscriber Line*) y otros tipos de redes de acceso. El protocolo RADIUS se describe en la RFC 2865 (www.ietf.org).

Un cliente RADIUS, (normalmente un servidor de acceso) envía las credenciales de usuario y la información de los parámetros de conexión en forma de mensaje RADIUS al servidor RADIUS. El servidor RADIUS comprueba las credenciales del cliente, indicando mediante un mensaje de respuesta si se autoriza o no la petición del cliente RADIUS. El cliente RADIUS también puede enviar al servidor RADIUS mensajes de contabilidad (Accounting). Adicionalmente, el estándar RADIUS soporta el uso de servidores proxy RADIUS. Un proxy RADIUS es un equipo que remite mensajes RADIUS entre clientes RADIUS, servidores RADIUS u otros proxies RADIUS. Los mensajes RADIUS nunca se envían entre el cliente de acceso y el servidor de acceso.

Los mensajes RADIUS son enviados como mensajes UDP. El puerto UDP 1812 se usa normalmente para los mensajes RADIUS de autenticacióny el puerto UDP 1813 para los mensajes RADIUS de contabilidad. Algunos servidores de acceso emplean el puerto UDP 1645 para los mensajes RADIUS de autenticación y el puerto 1646 para los mensajes RADIUS de contabilidad. Los tipos de mensajes RADIUS son: Access-Request, Access-Accept, Access-Reject, Access-Challenge, Accounting-Request y Accounting-Response.

EAPOL (Extensible Authentication Protocol over LAN)

El esquema de seguridad EAPOL permite el intercambio de información de autenticación entre cualquier equipo conectado a un switch (caso de estudio de esta práctica) y un servidor de autenticación como por ejemplo un servidor RADIUS. EAPOL se basa en EAP tal y como se especifica en el estándar 802.11x para establecer un control de acceso en redes LAN.

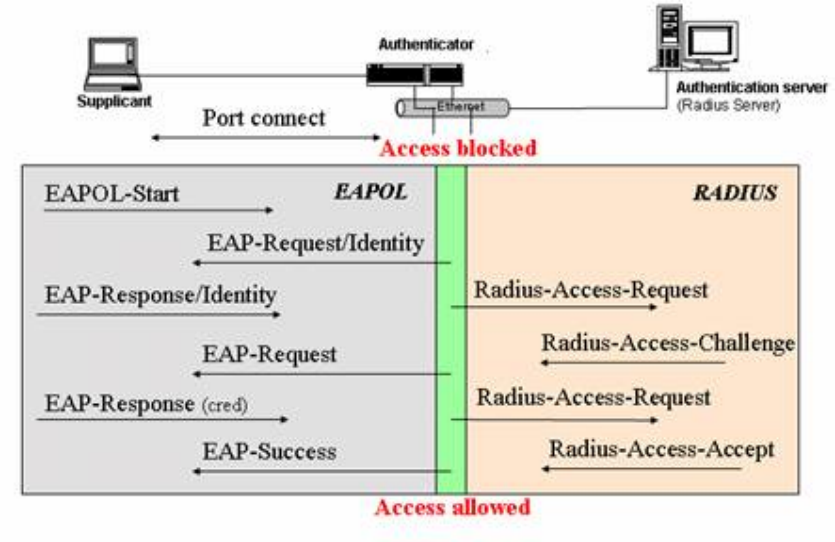
Algunos de los términos usados en EAPOL son:

- Suplicante o cliente: la máquina que solicita el acceso a la red.

- Autenticador: Software con el único propósito de autorizar a un determinado cliente. Se comunica con el suplicante haciendo uso del protocolo de encapsulación EAPOL.
- Servidor de autenticación: un servidor RADIUS que proporciona servicios de autenticación al autenticador.
- PAE (Port Access Entity): Entidad software asociada con cada puerto que soporta funcionalidad tanto de cliente como de autenticador.
- Puerto controlado: cualquier puerto del switch que tenga activada la característica de seguridad basada en EAP.

El autenticador se encarga de decidir cuál debe ser el estado (modo de funcionamiento) del puerto controlado. Dicho estado puede variar entre dos opciones:

- Reenvío o Forwarding: estado en el que se permite el paso de los paquetes a través del conmutador mediante el puerto en cuestión.
- Bloqueo o Cerrado: estado en el que no se permite el paso de paquetes a través de dicho puerto.



Desarrollo de la práctica

Instalación de servidor RADIUS

1. En primer lugar descargue el archivo FreeRadius.tar.gz desde la web oficial del FreeRadius www.freeradius.org de forma gratuita. Descargue la versión 0.9.2 para Linux.
2. Una vez descargado proceda a instalar el software:
   - gunzip FreeRadius.tar.gz
   - tar –xvf FreeRadius.tar
   - ./configure
   - ./configure –localstatedir=/var –sysconfdir=/etc

- Este comando acompañado de las opciones indicadas permite especificar cuál será la ubicación de los ficheros de configuración y de los ejecutables

- make
- make install

3. Una vez finalizado el proceso de instalación es necesario modificar algunas opciones de los archivos de configuración. Estos archivos están en el directorio: /etc/raddb

   Los archivos de configuración más importantes son:

   Clients.conf: en este archivo se guarda un listado de las máquinas que pueden actuar como clientes del servidor RADIUS.

   Users: en este archivo se almacenan una serie de entradas, cada una de las cuales se corresponde a un usuario , y donde se especifican una serie de parámetros para cada uno de ellos.

   Radius.conf: en él se configuran las opciones del propio servidor RADIUS, tales como el método de cifrado.

   El archivo que van a modificar es el **users**. En dicho archivo se incluyen todos los usuarios que pueden acceder al servidor RADIUS (a excepción de los usuarios con cuentas locales en la máquina donde se ejecuta el servidor), pudiendo especificarse multitud de parámetros para cada uno de ellos (tipo de autenticación, tipo de servicio, clave, etc.).

4. Configure el archivo **users** con las siguientes entradas:

   alum1 Auth-type:=EAP, User-Password== “alum1pass”

   Service-Type = Administrative-User

   alum2 Auth-type:=EAP, User-Password== “alum2pass”

   Service-Type = Administrative-User

   Donde Auth-type indica el tipo de autenticación para un determinado usuario. Además del protocolo EAP otras posibles opciones son: System y Local.

   La configuración del archivo **users** todavía no ha concluido. Falta proteger la interfaz de configuración y el acceso por telnet del/al switch mediante autenticación de un identificador de usuario y su correspondiente clave almacenados también en el servidor RADIUS. Para ello deberá añadir un nuevo usuario a la lista de usuarios del fichero users, con privilegio administrativo que pueda acceder al interfaz web de configuración del switch. Añada la siguiente entrada:

   admin. Auth-Type:=EAP, User-Clave == “administradorpass”

   Service-Type= Administrative-User

5. En el archivo **clients.conf** introduzca una entrada de la forma

```
Client      @IP_switch{
        Secret = alumno #secreto compartido entre radius y switch
        Shortname=switch
}
```

6. Ponga en marcha el servidor RADIUS. Dentro del directorio /usr/local/sbin ejecute el comando

   ./radiusd –X –p 1645

7. Una vez instalado RADIUS van a configurar el cliente EAP.

Configuración del Suplicante (Cliente EAP)

8. Descargue el software Odyssey Client para Windows98 de la web:

http://www.funk.com/download.asp?acg=6

9. Una vez instalado el Oddysey, arranque el Client Manager (permite configurar un cliente EAP).
10. En primer lugar desactive el cliente con la opción Settings -> Disable Oddysey.
11. A continuación, en Profiles, se configuran los perfiles de usuario. Pulse el botón Add. En la pestaña User Info introduzca el nombre de usuario (alum1) y como nombre de perfil “Alumno1”. Active las casillas *Permit Login using password* y *prompt for password*.
12. En la pestaña Authentication elimine todos los protocolos de autenticación de la misma. Pulse Add para añadir uno nuevo. Seleccione EAP/MD5 Challenge. Pulse OK, OK.
13. Cree un nuevo perfil para el usuario alum2.
14. Vaya a la opción Networks, donde se configuran las redes para las que está configurado el cliente EAP.Seleccione <any> y pulse Properties. Active las casillas Connect to any available network y Authenticate using profile alum1. Pulse OK.
15. Vaya a la opción Adapters. Compruebe que el adaptador de red de su equipo está en la lista.
16. En la opción Connection elija el adaptador de red marcándolo en el menú desplegable de Adapter. Active la casilla Connect using Profile alum1.

Configuración del autenticador (Switch)

17. Pasamos a configurar el switch (Business Policy Switch 2000 o Cisco Catalyst 2950). En el Business Policy Switch 2000, la configuración inicial consiste en asignar una dirección IP mediante la cual poder acceder al switch a través de web o telnet. Conecte el PC desde el que se desea

configurar el switch al switch mediante un cable cruzado a través del puerto serie. Una vez conectado abra el programa Hyperterminal. En el caso del Cisco catalyst 2950 se asignará una dirección IP al switch y el resto de la configuración se hará mediante la línea de comandos.

Business Policy Switch 2000

18. Cree una nueva conexión. Asigne el puerto serie correspondiente (COM1 o COM2). Establezca las siguiente propiedades:
    - Bits por segundo: 9600
    - Bits de datos: 8
    - Paridad: ninguna
    - Bits de parada: 1
    - Control de flujo: Xon/Xoff
19. Pulse aceptar.
    - Tras la secuencia de arranque pulse CTRL.+Y y accederá a la línea de comando.
    - Escriba *enable* para pasar a modo privilegiado.
    - Escriba *config* para pasar al modo de configuración global.
    - Asigne una dirección IP con el comando *ip address 192.168.4.250*

Ahora ya puede acceder al ¡nterfaz web de configuración escribiendo como URL en el navegador la dirección IP del switch.

20. Abra el interfaz de configuración web del switch. Desde esta interfaz pueden gestionarse la totalidad de las funciones del switch de modo sencillo.
21. Protección del acceso a la interfaz web:
    - Dentro del panel de la izquierda, en el apartado de Administración, entre en la opción Security y a continuación en RADIUS.
    - En Primary RADIUS Server introduzca la dirección IP del servidor RADIUS. Deje en blanco (0.0.0.0) la opción de servidor RADIUS secundario.
    - UDP RADIUS Port, puerto por el que se ejecuta el servidor RADIUS: 1645
    - RADIUS Shared Secret, secreto compartido por el servidor RADIUS y el switch: alumno
    - Pulse el botón Submit para actualizar los cambios.
    - Para proteger el acceso a la interfaz web de configuración haciendo uso del servidor RADIUS vaya al menú Administration ->Security -> Web. En la opción Web Switch Password Type seleccione RADIUS Authentication. Pulse el botón Submit para actualizar los cambios y después pulse Reset
22. Seguridad EAP en el Switch:
    - Para que el switch realice la función de autenticador es necesario configurarlo. Entre en el menú Application -> EAPOL Security.

- Para cada puerto, excepto para el puerto conectado al servidor RADIUS, se marca la opción Auto en la columna Administrative Status para que el estado del puerto dependa del resultado de la autenticación EAP.
- En la casilla EAPOL Administrative State seleccione Enabled para activar la seguridad EAP en el Switch.

Cisco Catalyst 2950

18. Cree una nueva conexión. Asigne el puerto serie correspondiente (COM1 o COM2). Establezca las siguiente propiedades:

- Bits por segundo: 9600
- Bits de datos: 8
- Paridad: ninguna
- Bits de parada: 1
- Control de flujo: Xon/Xoff

19. Inicialmente el switch aparece en modo usuario (indicado por el símbolo >). Es el modo privilegiado el que da acceso a todos los comandos del switch. Para pasar a modo privilegiado (viene indicado por el símbolo #) ejecute el comando *enable*.

- Para eliminar cualquier configuración anterior en el switch ejecute los siguientes comandos
  - Switch#**delete flash:vlan.dat**
  - Switch#**erase startup-config**
  - Switch#**reload**
- Para asignar una dirección IP al switch ejecute los siguientes comandos:
  - Switch#**configure terminal**
  - Switch(config)#**interface VLAN1**
  - Switch(config-if)#**ip address** 192.168.4.250 255.255.255.0

20. Seguridad EAP en el switch:

- Salga del modo de configuración de interfaz con el comando **exit** (el promt debe ser Switch(config)#)
- Habilite AAA y el método de autenticación:
  - Switch(config)#**aaa new-model**
  - Switch(config)#**aaa authentication dot1x default group radius**
- Active la autenticación 802.1x en los interfaces correspondientes:
  - Switch(config)#**interface fastethernet 0/1**
  - Switch(config-if)#**dot1x port-control auto**
  - Switch(config-if)#**end**
  - Switch#**copy running-config startup-config**

21. Configuración del switch como cliente del servidor RADIUS:

- Para que el switch pueda actuar como cliente del servidor RADIUS ejecute los siguientes comandos:
  - Switch#**configure terminal**

- Switch(config)#**radius-server host** 192.168.4.250 **auth-port** 1645 **key** alumno
- Switch(config)#**end**
- Switch#**copy running-config startup-config**

Comprobación

Realice un ping desde el suplicante a otro PC del laboratorio.