WPA2-Enterprise

freeRADIUS

OpenLDAP

Leonardo Bernal Bueno

25/06/2013

Índice

¿Qué es Radius?

Radius (Remote Authentication Dial-In

User Server), es un protocolo de autenticación para aplicaciones de acceso a la red o movilidad IP.

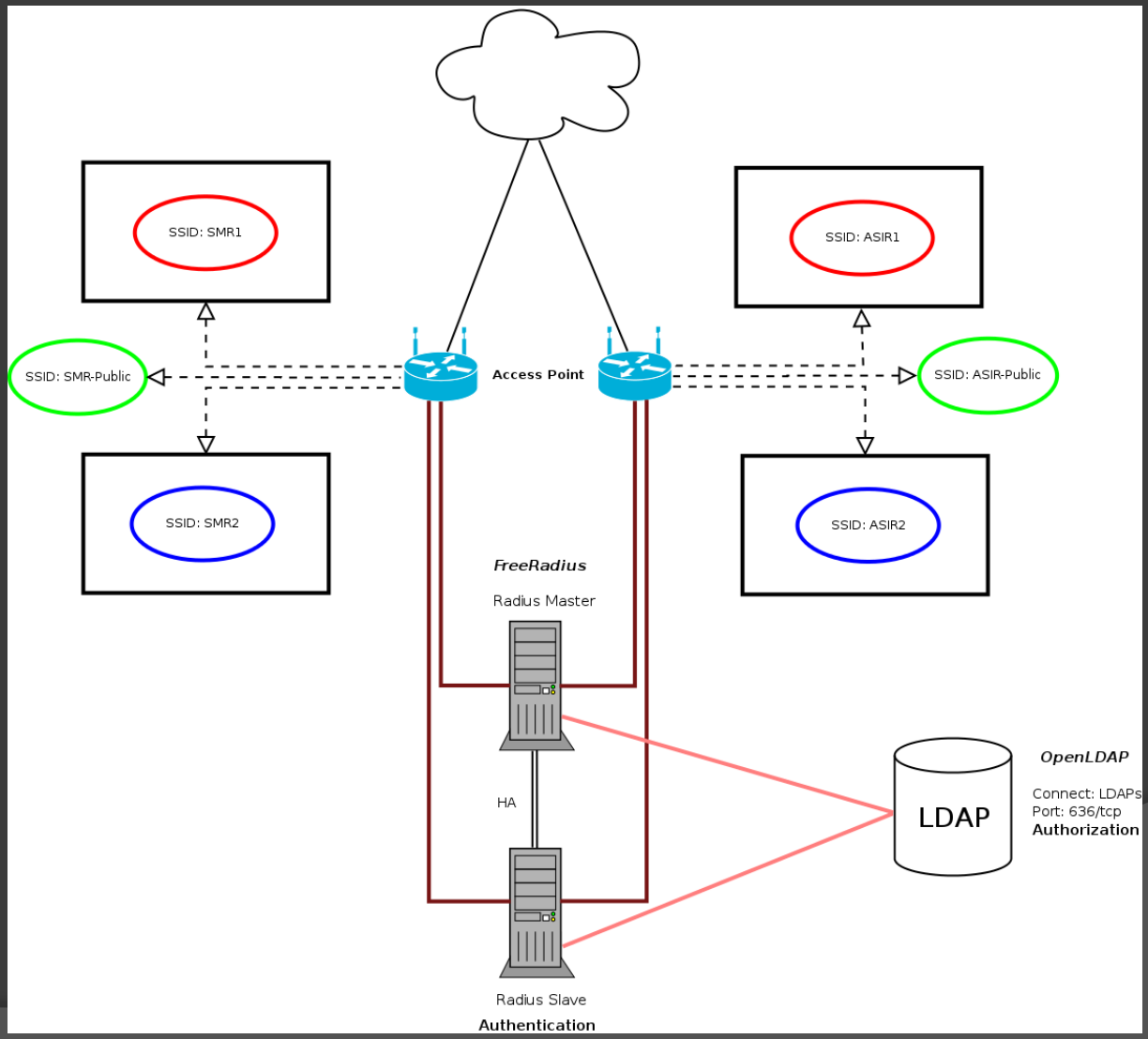
Podemos decir que más que un protocolo de autenticación, es un protocolo AAA

(Authentication, Authorization, Administration).

Objetivos

- Estudio de diferentes métodos de autenticación y protocolos.
- Conexión y configuración Radius – Ldap.
- Implantación de freeRadius en el centro.
- Toda la comunicación cifrada.
- Configuración de puntos de acceso.
- Radius en alta disponibilidad.
- Documentación para los clientes.
- Vulnerabilidades.

Infraestructura



Métodos de Autenticación

	Certificados en Servidor	Certificados en Clientes	Soporta LDAP	Compatibilidad Windows
PEAP	Obligatorio	Opcional	Si	Si
EAP-TTLS	Obligatorio	Opcional	Si	-
EAP-TLS	Obligatorio	Obligatorio	Si	-
LEAP	-	-	Sólo con MS-CHAP	-
EAP-FAST	Opcional	-	Si	Sólo en Intel

EAP-TTLS

Teniendo ahora una idea de algunos de los métodos de autenticación con los que trabaja *FreeRadius*, el método elegido es ***EAP-TTLS*** por las siguientes razones:

- *EAP-TTLS* es un método de autenticación tunelado.
- Todo el tráfico circula totalmente cifrado.
- La autenticación se realiza solo con certificados de servidor.
- EAP-TTLS tiene la capacidad de soportar una amplia variedad de métodos de autenticación interna.
- Excepto Windows 8, las demás versiones de Microsoft no dan soporte nativo a EAP-TTLS.
- *EAP-TTLS* no es vulnerable actualmente a ataques MITM ni de diccionarios.

Protocolos de autenticación

Independientemente de los métodos de autenticación que hemos visto en el apartado anterior, para la comunicación interna de los servicios podemos usar diferentes protocolos de autenticación.

	Clear-text	NTLM (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash
PAP	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x
MSCHAP	✓	✓	x	x	x	x
MSCHAPv2	✓	✓	x	x	x	x

PAP

- En nuestra infraestructura no tenemos más remedio que usar **PAP** debido a la compatibilidad con los algoritmos de cifrado de las contraseñas de LDAP.
- PAP no es recomendable usarlo independiente, pero no hay ningún problema al usarlo junto a EAPTTLS ya que éste cifra toda la comunicación cliente-servidor haciendo uso de túneles.
- En la documentación del proyecto se realizan pruebas con Wireshark para comprobar que efectivamente toda la comunicación está cifrada.

Access Point

Cisco Linksys WAP-4410N

Access Point

Cisco Linksys WAP-4410N

- Características principales:
  - WEP de 128 bits, encriptación de 64 bits WEP, WPA, WPA-PSK, WPA2-PSK, WPA-Enterprise, WPA2-Enterprise.
  - Hasta 4 SSID.
  - Hasta 2 servidores Radius (primary, backup) para mantener redundancia.
  - 3 Antenas Omnidireccionales (2dBi).
  - Velocidad de transferencia de datos 300 Mbps.
  - Un máximo de 63 usuario simultáneos.
  - Tecnología POE.

Requisitos del sistema

- Los puertos usados por RADIUS son **1812/UDP** para autenticación y **1813/UDP** para administración de cuentas.

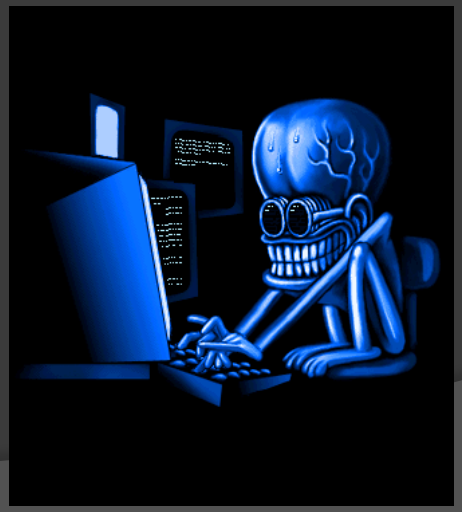
```
# Acceso desde aulas a Papion Freeradius
iptables -A FORWARD -s $AULAS -d $PAPION -p udp --dport 1812 -j  ACCEPT
iptables -A FORWARD -s $PAPION -d $AULAS -p udp --sport 1812 -j  ACCEPT
iptables -A FORWARD -s $AULAS -d $PAPION -p udp --dport 1813 -j  ACCEPT
iptables -A FORWARD -s $PAPION -d $AULAS -p udp --sport 1813 -j  ACCEPT
```

Ficheros de configuración

- FreeRadius establece su configuración en varios ficheros de configuración:
  - ***radiusd.conf***
  - ***sites-available***
  - ***Servidor virtual: iesgn***
  - ***eap.conf***
  - ***ldap***
  - ***users***
  - ***clients.conf***

Vulnerabilidades

- La infraestructura **EAP-TTLS / PAP** presenta un escenario robusto y complejo, poniendo realmente a prueba a un atacante ilícito, pero nada es perfecto.



Vulnerabilidades

- Posibles vulnerabilidades o puntos débiles:
  - ***Protocolos de autenticación.***
  - ***Que se comprometa directamente al servidor.***
  - ***Rogue AP.***

Vulnerabilidades

- ***Protocolos de autenticación:***

Todos los protocolos usados internamente están rotos. De ahí a usarlos siempre acompañados de métodos de autenticación (TTLS).

  - PAP viaja en texto plano.
  - CHAP usa MD5 como algoritmo, actualmente roto.
  - MS-CHAPv2 según la web “Una al Día” en una noticia de Septiembre de 2012, se desarrollaron métodos los cuales son capaces de descifrar cualquier contraseña MS-CHAPv2 en menos de 24 horas.

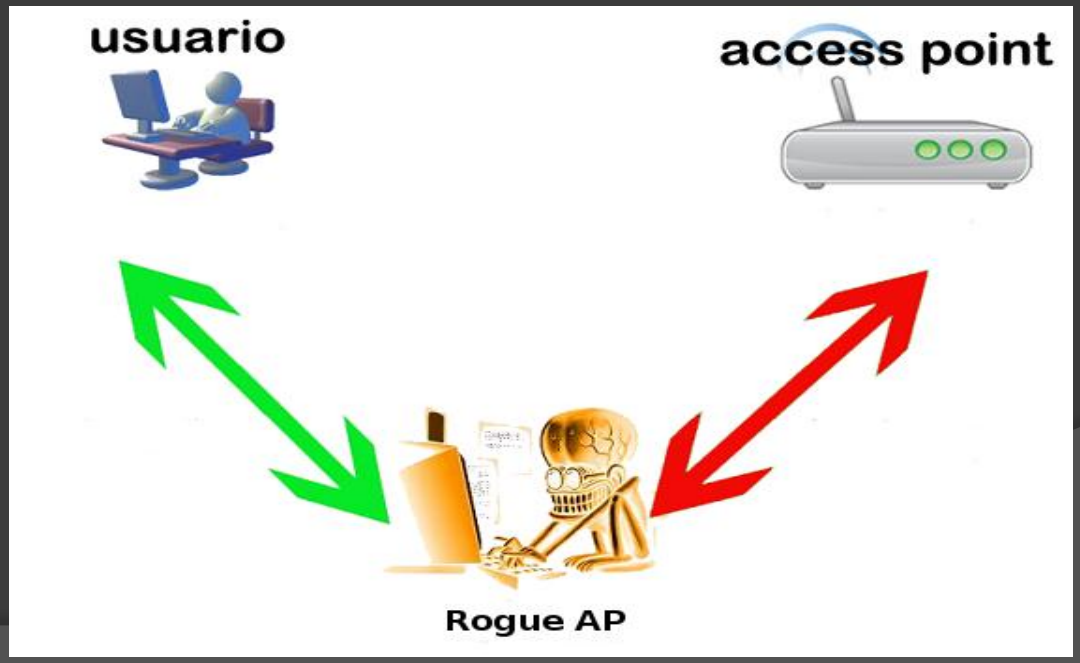
Vulnerabilidades

- ***Que se comprometa directamente al servidor.***

Si un atacante consigue acceder al servidor, aprovechando alguna vulnerabilidad no parcheada del propio sistema operativo podrá interceptar mensajes y realizar todo tipo de opciones.

Vulnerabilidades

- Rogue AP.
  - Rogue AP o suplantación del punto de acceso. La idea de esta técnica de ataque es conseguir que la víctima se conecte al equipo del atacante, que funciona como un punto de acceso legítimo, para que sea éste el que redirija el tráfico.
  - Mismo SSID y configuraciones de seguridad de la red.



Enlaces de Interés

- Slideshare

http://es.slideshare.net/leobernal91/presentaci-23407621

- Para más información visite:

http://leo-bernal.blogspot.com.es/