ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

INFORME DE PROYECTO DE GRADUACIÓN

"AUDITORÍA DE SEGURIDAD EN REDES INALÁMBRICAS, SOLUCIONES Y RECOMENDACIONES"

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

Presentado por:

DIEGO ANDRES CHOEZ CAJAMARCA

JAVIER ANTONIO BENITES BARREIRO

GUAYAQUIL – ECUADOR

2015

AGRADECIMIENTO

A todas las personas que hicieron posible la realización de este proyecto. A mis padres por su apoyo moral y económico durante toda mi carrera universitaria. Finalmente a mi compañero de tesis, Javier Benites, cuyo esfuerzo y dedicación hicieron posible completar este trabajo exitosamente.

Diego Chóez Cajamarca

En primer lugar agradezco a Dios por darme fuerza para cumplir una meta más en mi vida académica.

A la señorita Karen Aguirre y sus padres por todo ese apoyo incondicional que me brindaron para la culminación de este trabajo.

A mis padres por todo el sacrificio hecho, durante toda mi vida académica.

A mi director de tesis el Ing. Albert Espinal, a mi compañero de tesis, Diego Chóez, por toda la ayuda brindada.

Finalmente agradezco a todos mis profesores de la carrera de LICRED cuyas enseñanzas han sido de gran ayuda para el desarrollo de este proyecto.

Javier Benites Barreiro

DEDICATORIA

A mis padres, por su apoyo y esfuerzo que me han permitido alcanzar este nivel de estudios, por confiar en mi capacidad e impulsarme a seguir adelante en mi carrera universitaria.

Diego Chóez Cajamarca

Este trabajo está dedicado de manera muy especial a la señorita Karen Aguirre, quien ha estado a mi lado durante todo el desarrollo de este proyecto, brindándome su compresión, ayuda y amor, lo cual ha sido mi más grande fuente de inspiración, fortaleza y alegría.

A Dios, a mi familia y compañeros que han sido un pilar fundamental en mi vida.

Javier Benites Barreiro

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Albert Espinal

DIRECTOR DE PROYECTO DE GRADUACIÓN

_____

Ing. Patricia Chávez.

PROFESOR DELEGADO POR LA UNIDAD ACADEMICA

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este informe, me corresponde exclusivamente; y el patrimonio intelectual del mismo a la Escuela Superior Politécnica del Litoral"

_____

Diego Andrés Chóez Cajamarca

_____

Javier Antonio Benites Barreiro

RESUMEN

El presente trabajo tiene como objetivo mostrar las debilidades que se pueden encontrar en una red local inalámbrica, para esto se demostrará como operan algunas herramientas de auditoria de seguridad y la facilidad con que ciertos métodos de seguridad poco confiables pueden ser eludidos o vulnerados. Se analizarán y propondrán algunas soluciones de seguridad más complejas orientadas a optimizar la seguridad y el control de acceso en redes inalámbricas. Finalmente, se mostrará el diseño e implementación de una solución de seguridad basada en VPN + RADIUS EAP-TLS.

El capítulo 1 describe el proyecto, sus antecedentes, objetivos y metodología. El capítulo 2 explica de manera teórica conceptos de seguridad en redes inalámbricas. En el capítulo 3 se describe el proceso de un test de penetración y sus diferentes fases. En el capítulo 4 se muestra el funcionamiento de varias herramientas de auditoría y procesos específicos para vulnerar algunos métodos de seguridad usando un escenario de pruebas. El capítulo 5 da algunas recomendaciones para mejorar la seguridad en un ambiente personal o de hogar y propone algunas de las soluciones más confiables de seguridad a nivel empresarial. Finalmente, en el capítulo 6 se muestra el diseño e implementación de un modelo de seguridad usando VPN para el cifrado y certificados digitales para la autenticación de los usuarios.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS

AES: Estándar de Cifrado Avanzado (Advanced Encryption Standard).

AFS: Sistema de Archivos Andrew (Andrew File System).

AP: Punto de Acceso. (Access Point).

BSSID: Identificador del Conjunto de Servicios Básicos (Basic Service Set Identifier).

CA: Entidad de Certificación (Certification Authority).

CCMP: Modo de Contador con Cifrado de Mensajes de Encadenamiento de Bloques de Código de Autenticación de Protocolo (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

CH: Canal (Channel).

CHAP: Protocolo de Autenticación por Desafío Mutuo (Challenge Handshake Authentication Protocol).

CRL: Lista de Revocación de Certificados (Certificate Revocation List).

DDR2: Tasa de Datos Doble de Tipo Dos (Double Data Rate type two).

DNS: Sistema de Nombres de Dominio (Domain Name System).

DSL: Línea de Abonado Digital (Digital Subscriber Line).

EAP: Protocolo de Autenticación Extensible (Extensible Authentication Protocol).

EAP-GTC: Protocolo de Autenticación Extensible - Tarjeta Token Genérica (Extensible Authentication Protocol - Generic Token Card)

ENC: Cifrado (Encryption).

ESSID: Identificador del Conjunto de Servicio Extendido (Extended Service Set Identifier).

EP: Punto Final (End Point)

GB: Gigabyte

GHz: Gigahertz

GPO: Objeto de Directiva de Grupo (Group Policy Object).

HTTP: Protocolo de Transfernecia de Hipertexto (Hypertext Transfer Protocol).

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers).

IETF: Fuerza de Trabajo de Ingeniería de Internet (Internet Engineering Task Force).

IP: Protocolo de Internet (Internet Protocol.

IV: Vector de Inicialización (Initialization Vector).

LAN: Red de Area Local (Local Area Network).

LEAP: Protocolo Ligero de Autenticación Extensible (Lightweight Extensible Authentication Protocol).

LM: Administrador de LAN (Lan Manager)

LST: Lista (List).

MAC: Control de Acceso al Medio (Media Access Control).

MB: Megabyte

MD4: Algoritmo de Resumen del Mensaje 4 (Message-Digest Algorithm 4).

MD5: Algoritmo de Resumen del Mensaje 5 (Message-Digest Algorithm 5)

MON: Monitor

MS-CHAP: Microsoft - Protocolo de Autenticación por Desafío Mutuo (Microsoft - Challenge Handshake Authentication Protocol)

NAC: Control de Acceso a la Red (Network Access Control).

NAP: Proteccion de Acceso a la Red (Network Access Protection).

NPS: Servidor de Directivas de Redes (Network Policy Server).

OPN: Abierta (Open).

PAP: Protocolo de Autenticación de Contraseña (Password Authentication Protocol).

PDP: Punto de Decisión de Políticas (Policy Decision Point).

PEAP: Protocolo de Autenticación Extensible Protegido (Protected Extensible Authentication Protocol).

PEP: Punto de Aplicación de Políticas (Policy Enforcement Point).

PKI: Infraestructura de Clave Pública (Public Key Infrastructure).

PPTP: Protocolo de túnel punto a punto (Point to Point Tunneling Protocol).

PSK: Clave precompartida (Pre-shared key).

PSTN: Red Telefónica Pública Conmutada (Public Switched Telephone Network).

PWR: Nivel de Señal

RADIUS: Servicio de autenticación remota telefónica de usuario (Remote Authentication Dial-In User Service).

RRAS: Servicio de enrutamiento y acceso remoto (Routing and Remote Access Service).

SSID: Identificador de Conjunto de Servicios (Service Set Identifier)

TKIP: Protocolo de Integridad de Clave Temporal (Temporal Key Integrity Protocol).

TLS: Seguridad de la Capa de Transporte (Transport Layer Security).

TTLS: Seguridad de la Capa de Transporte Tunelizada (Tunneled Transport Layer Security).

USR: Usuario (User).

VPN: Red Virtual Privada (Virtual Private Network).

WAN: Red de Área Amplia (Wide Area Network).

WEP: Privacidad Equivalente a Cableado (Wired Equivalent Privacy).

Wi-Fi: Fidelidad inalámbrica (Wireless Fidelity).

WPA: Acceso Protegido Wi-Fi (Wi-Fi Protected Access).

WPS: Configuración Wi-Fi Protegida (Wi-Fi Protected Setup).

INTRODUCCIÓN

En los últimos años hemos visto un acelerado crecimiento en el uso de redes inalámbricas, esto se debe al incremento de equipos portátiles y las ventajas en la implementación de estas redes como el hecho de no tener que instalar cableado.

Actualmente, podemos observar que prácticamente en toda empresa, además del acceso por medios cableados, existen puntos de acceso inalámbricos. Esto incluso se ha propagado a los hogares, donde proveedores de servicio de internet ofrecen de manera gratuita la instalación de ruteadores inalámbricos.

A pesar de las múltiples ventajas que ofrece una red inalámbrica, la utilización del aire como medio de transmisión ha creado un nuevo riesgo en la seguridad que puede ser difícil de manejar.

La misma facilidad de instalación y configuración de estos equipos de acceso inalámbrico puede representar un problema, ya que usuarios con poca experiencia se limitan a usar la configuración predeterminada de fábrica que generalmente no es la óptima en cuanto a seguridad.

En el caso de las empresas, la falta de conocimiento por parte de los propietarios o el presupuesto para su implementación pueden influir en que la seguridad en estas redes no sea considerada de manera adecuada.

El presente proyecto pretende mostrar los riesgos de seguridad que se pueden encontrar en este tipo de redes y proponer algunas soluciones y recomendaciones para mejorar significativamente la seguridad en el acceso a redes inalámbricas.

CAPÍTULO 1

1. PRESENTACIÓN Y JUSTIFICACIÓN DEL PROYECTO

A continuación se presentará un resumen de los principales aspectos del proyecto como los antecedentes, la metodología a emplear, los objetivos principales y secundarios, así como los resultados que se espera obtener a lo largo del desarrollo del tema propuesto.

1.1. ANTECEDENTES

En la actualidad se ha incrementado el uso de dispositivos móviles por lo que en gran parte de empresas e instituciones se han implementado sistemas de acceso a la red por medio inalámbricos.

Uno de los problemas en un escenario de red inalámbrico es que se maneja un medio compartido, lo que facilita la captura de información ya que cualquier dispositivo que se encuentre dentro del rango del alcance de la señal puede acceder al medio. Otro problema es la falta de conocimiento del usuario final, que es aprovechado por los atacantes usando métodos como la creación de redes falsas que les permiten robar información confidencial o claves de acceso a la red.

Estos problemas hacen que la seguridad al momento de hacer una implementación de red inalámbrica sea de especial importancia. Sin embargo, muchas de las implementaciones de redes inalámbricas actuales no cuentan con el nivel de seguridad necesario de acuerdo a la información que manejan.

1.2. OBJETIVO GENERAL

Identificar las vulnerabilidades existentes en una infraestructura de red inalámbrica e implementar un modelo de seguridad que mitigue estas vulnerabilidades.

1.3. OBJETIVOS ESPECÍFICOS

- Describir la metodología para un test de penetración en redes inalámbricas.
- Implementar un escenario para pruebas y efectuar un test de penetración.
- Detectar e identificar las vulnerabilidades presentes en las redes inalámbricas.
- Mostrar diferentes modelos de seguridad, a nivel personal y empresarial.
- Implementar un modelo de seguridad a nivel empresarial.

1.4. JUSTIFICACIÓN

La información que se maneja actualmente de manera digital y que pasa a través de una red informática incluye información privada de los usuarios y documentos confidenciales de una organización. Sin las medidas de seguridad adecuadas esta información podría quedar expuesta poniendo en riesgo la privacidad de las personas u organizaciones.

En el caso de las redes inalámbricas, debido a los problemas de seguridad propios de esta tecnología, es necesario usar métodos de seguridad y control de acceso más robustos que en una red cableada. Una solución óptima para el acceso a una red inalámbrica

debería incluir autenticación y cifrado de datos para de esta manera mitigar posibles ataques y evitar accesos no autorizados. Además, se debe tomar en cuenta el nivel de acceso que se les otorga a los usuarios.

1.5. METODOLOGÍA

El proyecto constara de dos fases. La primera fase estará enfocada en la demostración de las vulnerabilidades existentes en la seguridad de las redes inalámbricas y la segunda en el estudio e implementación de métodos de seguridad que permitan evitar las vulnerabilidades demostradas en la fase anterior.

Para la primera fase se implementará un escenario con máquinas virtuales y equipos de red en donde se realizaran pruebas que permitan comprobar las vulnerabilidades a las que podría estar expuesta una red inalámbrica, para ello se usaran varias herramientas de auditoria de redes.

Luego de obtener los resultados de estas pruebas se procederá a la segunda fase, donde se determinarán los métodos de seguridad que permitan una solución confiable y adecuada de acuerdo al nivel de seguridad requerido por la infraestructura de red. Al igual que en la primera fase, se implementará la solución con la ayuda software de virtualización y equipos de red.

1.6. RESULTADOS ESPERADOS

Detectar el nivel de seguridad y las vulnerabilidades existentes en diferentes esquemas de seguridad de redes inalámbricas. Además se implementará un esquema de seguridad a nivel empresarial que permita mitigar estas vulnerabilidades.

CAPÍTULO 2

2. SEGURIDAD EN REDES INALÁMBRICAS

La naturaleza de las redes inalámbricas las hace más susceptibles a ser atacadas que las redes cableadas, debido a que estas usan como medio de transmisión el aire que es un medio compartido. Por esto es importante establecer mecanismos de seguridad al momento de implementarlas.

2.1. TIPOS DE AUTENTICACIÓN

Para que un cliente tenga acceso a una red o un punto de red, es necesario realizar el proceso de autenticación que consiste en verificar la identidad de un cliente previo a otorgarle dicho acceso.

Existen diferentes tipos de autenticación de acuerdo al nivel de seguridad que requiera la infraestructura de red:

- Autenticación Abierta
- WEP
- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise

2.1.1. Autenticación abierta

La autenticación abierta permite el acceso a la red a cualquier dispositivo, de esta manera cualquier dispositivo que conozca el SSID del punto de acceso puede obtener acceso a la red.

1.- Cualquier estación inalámbrica puede enviar una petición para la autenticación

2.- Una estación puede enviar una trama de administración de autenticación que contiene su identidad para autenticarse y conectarse

3.- El AP verifica el SSID del cliente y en respuesta envía una trama de verificación de autenticación

4.- Una vez que la verificación ha sido realizada se conecta a una red o a una estación inalámbrica.

2.1.2. WEP

Es un protocolo de seguridad en una red inalámbrica. Este tipo de seguridad está obsoleta ya que no ofrece una gran capa de seguridad en ninguna de las fases de autenticación, confidencialidad e integridad.

Al usar la misma contraseña para todos los usuarios y estaciones no se identifica al usuario que se conecta, además de dar acceso a cualquier usuario con la misma contraseña. Falla en brindar integridad, al enviar información en texto plano que puede ser analizada para obtener la clave de cifrado. En el caso de la integridad, WEP proporciona el mecanismo CRC-32, que se ha demostrado que es posible modificar parte del mensaje y a su vez el CRC lo que permitiría modificar la información que viaja en el mensaje sin que el destino se percate de ello.

Podemos encontrar varios problemas en el protocolo WEP que lo hacen vulnerable. Uno de ellos es el uso de una clave estática, esto permite que esta pueda ser determinada con la captura de una gran cantidad de paquetes. El vector de

inicialización (IV), que es el valor aleatorio usado para generar la llave de cifrado, es enviado en texto plano al cliente además de ser demasiado corto (24 bits) lo que disminuye el tiempo y la cantidad de paquetes necesarios para descifrar la clave a partir de este. [1]

2.1.3. WPA-Personal

WPA fue creado para corregir los problemas de seguridad que hacían vulnerable a WEP. Utiliza claves de codificación de 128 bits y claves de sesión dinámica para garantizar la privacidad y seguridad de la red inalámbrica. La versión Personal de WPA requiere la configuración manual de una clave pre-compartida (PSK) en el punto de acceso y los clientes. La misma contraseña utilizada en el punto de acceso debe utilizarse en todos los demás dispositivos inalámbricos que tienen acceso a la red. La seguridad depende de la complejidad y confidencialidad de la contraseña, cuanto más larga y compleja sea la contraseña, más robusta será la seguridad de la red inalámbrica. WPA fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado por lo que no implementa el estándar IEEE 802.11i en su totalidad. [2]

2.1.4. WPA2-Personal

WPA2 es una mejora de WPA que corrige algunas vulnerabilidades detectadas en WPA e implementa el estándar IEEE 802.11i completo. Al igual que WPA-Personal requiere una clave pre-compartida (PSK) en el punto de acceso y los clientes. [2]

La principal diferencia entre WPA y WPA2 son los tipos de cifrados que utilizan, WPA utiliza un tipo de cifrado conocido como TKIP mientras que WPA2 utiliza el cifrado AES, aunque por retro compatibilidad también soporta el uso de TKIP. [3]

Existe la posibilidad de capturar el handshake que se intercambia durante el proceso de autenticación en una red, y obtener las credenciales de los usuarios mediante ataques de diccionario o fuerza bruta. Se puede usar la GPU para acelerar el proceso de obtención de contraseña con seguridad WPA2-PSK.

2.1.5. WPA-Enterprise

La versión Empresarial de WPA, ofrece un control individualizado y centralizado sobre el acceso, cuando los usuarios tratan de conectarse a la red, necesitan presentar sus

credenciales de acceso al sistema. WPA-Enterprise verifica los usuarios de red mediante un servidor de autenticación como RADIUS. [2]

2.1.6. WPA2-Enterprise

WPA2-Enterprise es una mejora de WPA e implementa todo el estándar IEEE 802.11i completo. Al igual que el WPA-Enterprise, verifica los usuarios mediante un servidor de autenticación.

2.2. AUTENTICACIÓN 802.1X

El estándar 802.1x es una arquitectura de control de acceso para redes inalámbricas el cual hace uso de certificados digitales para proporcionar a los usuarios los servicios de autenticación y autorización. Aquí intervienen 3 entidades que son el cliente, el punto de acceso y el servidor de autenticación. Al usuario se le concede un certificado digital que permitirá realizar la autenticación y de esta manera hacer uso de la red. El proceso está basado en 3 fases:

- **Autenticación.-** Cuando el cliente entra en el área de cobertura, el punto de acceso pide la identidad y el cliente se la proporciona, luego se realiza el proceso de conexión donde los extremos se autentican mutuamente

- **Autorización.-** El cliente le indica al servidor de autenticación el tipo de conexión que desea, el ancho de banda y el tiempo que va a estar conectado, así como los certificados los cuales demuestran que el usuario está autorizado para el uso de la red y los privilegios que posee; en caso de haber algún problema se desautoriza al cliente.
- **Distribución de clave.-** El servidor de autenticación le pasa al punto de acceso la clave que debe utilizar con el cliente así como el tipo de servicio.

Esto se hace a través del uso de un servidor de autenticación como RADIUS. El 802.1x se basa en el protocolo EAP (Protocolo de autenticación extensible), definido por el IETF. Este protocolo se usa para transportar la información de identificación del usuario.

2.2.1. Funcionamiento de RADIUS

RADIUS (Remote Authentication Dial-In User Services) es un protocolo de autenticación ampliamente utilizado que permite tener la autenticación, la autorización y la auditoria centralizadas para el acceso de red. En la figura 2.1 se puede observar un ejemplo de infraestructura RADIUS con sus correspondientes elementos. Desarrollado inicialmente para acceso remoto dial-up, RADIUS es soportado actualmente por

servidores VPN, puntos de acceso inalámbrico, conmutador Ethernet, acceso DSL y otros tipos de redes de acceso. [4]

A pesar de que RADIUS originalmente soporte esquemas de autenticación como PAP, CHAP o EAP, en el caso de la autenticación 802.1x solo soporta EAP [5]. Adicionalmente, se pueden encontrar servidores proxy RADIUS; Un proxy RADIUS es un equipo que remite mensajes RADIUS entre clientes RADIUS, servidores RADIUS u otros proxies RADIUS. [6]

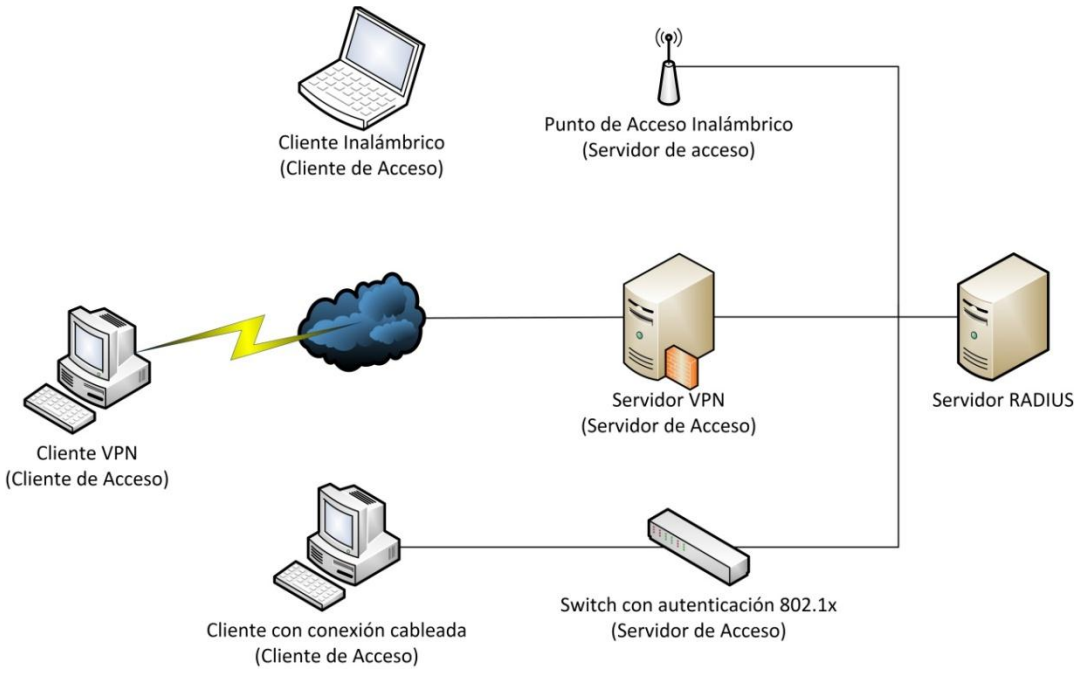


Figura 2.1 - Elementos de una infraestructura RADIUS

Una infraestructura RADIUS está formada por:

- Clientes de acceso.
- Servidores de acceso (clientes RADIUS)
- Servidores RADIUS.

Un ***servidor de acceso*** envía las credenciales de usuario, enviadas por un ***cliente de acceso***, y la información de los parámetros de conexión en forma de mensaje RADIUS al ***servidor RADIUS***.

El servidor RADIUS recibe y procesa las solicitudes de conexión enviadas por el servidor de acceso. De acuerdo con un conjunto de reglas y la información de la base de datos de cuentas de usuario, el servidor RADIUS autentica y autoriza la conexión, y devuelve un mensaje de aceptación o rechazo de acceso. El mensaje de aceptación de acceso puede contener restricciones de conexión que son implementadas por el servidor de acceso durante la conexión. De acuerdo a la respuesta recibida por el servidor RADIUS, el servidor de acceso concede o no el acceso al cliente de acceso.

2.2.2. Protocolo EAP

El protocolo Protocolo de Autenticación Extensible (EAP) es uno de los elementos básicos de 802.1x, en una extensión del protocolo punto a punto (PPP) utiliza métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información de longitudes arbitrarias y gestiona la contraseña con mecanismos de desafío-respuestas.

El protocolo EAP opera basado en 3 componentes:

- El autenticador (el punto de acceso)
- El solicitante (el software cliente)
- El servidor de autenticación

El ***autenticador*** es unos cortafuegos básicos que actúa como intermediario entre el usuario y el ***servidor de autenticación***. El usuario en este sistema se llama ***solicitante***. El autenticador es el que le otorga o deniega el acceso a la red basado en la respuesta obtenida del servidor de autenticación. Cuando se trata de una red inalámbrica, el punto de acceso actúa como autenticador. [7]

2.2.3. Métodos de autenticación EAP

EAP es una estructura de soporte, no un mecanismo específico de autenticación. EAP provee algunas funciones comunes y negociaciones para el o los mecanismos de autenticación escogidos. Estos mecanismos son llamados métodos de autenticación EAP, de los cuales se conocen actualmente unos 40. [8]

Los principales métodos de autenticación EAP usados en redes inalámbricas son:

- TLS (Seguridad de la Capa de Transporte)
- TTLS (Seguridad de la Capa de Transporte Tunelizada)
- PEAP (Protocolo de Autenticación Extensible Protegido)
- LEAP (Protocolo Ligero de Autenticación Extensible)

TLS: es un sistema de autenticación fuerte basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Infraestructura de Clave Pública) en ambos extremos.

TTLS: se basa en una identificación de usuario y contraseña que se transmiten cifrados mediante TLS. Es decir el cliente utiliza EAP-TLS para validar el servidor y crear un túnel TLS cifrado entre el cliente y el servidor para transmitir el nombre de usuario y la contraseña. El cliente puede utilizar otro protocolo de autenticación. A diferencia de EAP-TLS sólo requiere un certificado de servidor.

PEAP: es similar a EAP-TTLS, crea un túnel TLS para proteger otros métodos de autenticación. La principal diferencia con EAP-TTLS es que PEAP solo permite otros métodos de autenticación EAP, como MS-CHAPv2, a través del túnel TLS creado, mientras EAP-TTLS utiliza el túnel para ejecutar métodos de autentificación no implementados en EAP. [9]

LEAP: es un protocolo de autenticación ampliable desarrollado por Cisco que proporciona un mecanismo de autenticación desafío-respuesta y permite la asignación de claves dinámica. [10]

2.3. TIPOS DE CIFRADO DE DATOS

Los protocolos de cifrado son usados para producir las claves que cifrarán los datos durante la comunicación entre los dispositivos de

una red. El objetivo de estos es generar claves temporales de manera que no puedan ser descifradas por un atacante al capturar una gran cantidad de paquetes. Esto se consigue cambiando la clave usada cada cierta cantidad de paquetes impidiéndole a un atacante obtener la suficiente cantidad de paquetes para descifrar la clave.

2.3.1. TKIP

Es un protocolo de seguridad usado en WPA para mejorar el cifrado de datos en redes inalámbricas.. Debido a que las claves están en constante cambio, ofrecen un mejor nivel de seguridad para la red. [11]

2.3.2. CCMP

CCMP es un protocolo de cifrado de IEEE 802.11i creado para reemplazar a TKIP. CCMP emplea el algoritmo de seguridad AES (Advanced Encryption Standard). AES es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. AES es usado por WPA2 y ofrece un cifrado más seguro que TKIP, además de requerir menos procesamiento y ancho de banda. [12]. En la Tabla 1 se muestra un resumen comparativo de los tipos de cifrados.

	Algoritmo de cifrado	Longitud de llave de cifrado	Tamaño de IV	Longitud de llave de integridad	Mecanismo de comprobación de integridad
WEP	RC4	40 / 104-bit	24 - bits	Ninguna	CRC -32
TKIP	RC4	128 - bits	48 - bits	64 - bits	Algoritmo Michael
CCMP	AES	128 - bits	48- bits	128 - bits	CBC-MAC

Tabla 1 - Comparación de Tipos de Cifrado

CAPÍTULO 3

3. METODOLOGÍA DE UN TEST DE PENETRACIÓN A UNA RED INALÁMBRICA

Un test de penetración es un conjunto de metodologías y técnicas que permiten determinar las vulnerabilidades de un sistema. Aunque la parte principal de un test de penetración es la simulación de un ataque para determinar el nivel de seguridad de una red, es necesario que este procedimiento se lleve a cabo siguiendo varias etapas para que sea completado con éxito. Esto incluye las siguientes etapas:

- Planeación
- Descubrimiento
- Ataque
- Presentación de informe

3.1. PLANEACIÓN

Esta fase incluye el alcance de la evaluación, la estimación del esfuerzo y la legalidad. En primer lugar el cliente contrata al auditor de seguridad para definir los parámetros sobre los cuales se realizara el test de penetración. Esta fase es denominada **“Alcance de la evaluación”**. Aquí se definirá la ubicación donde se realizará el test de penetración y el área total de las instalaciones. Es importante además conocer el número de puntos de acceso y clientes inalámbricos. Adicionalmente se podría solicitar una lista estos dispositivos (tanto clientes como puntos de acceso) con sus respectivas direcciones MAC que permita identificarlos en busca de dispositivos desconocidos al momento de realizar la auditoria de la red. Finalmente se establecerá el procedimiento a realizar en caso de encontrarse con una vulnerabilidad en el sistema.

Una vez que el auditor tenga claro el alcance que tendrá su trabajo, éste debe estudiar los requerimientos del cliente para determinar la profundidad del test de penetración. Ya con conocimiento de los objetivos a cumplir como parte del test de penetración, el auditor procederá a realizar una estimación de las horas que se requieren para completar las pruebas y como estarán distribuidas a lo largo de los días de los que se dispone para el trabajo. Esta fase se denomina **“Estimación del esfuerzo”**.

Las pruebas de penetración son un asunto serio por lo tanto, es importante tener en cuenta los aspectos legales al momento de realizar una auditoría de seguridad. Dentro de la planeación esto es denominado **“Legalidad”**. De parte del auditor, es imprescindible obtener un acuerdo legal con el cliente que garantice que el auditor de seguridad o la empresa encargada de la auditoria no son responsables de los daños resultantes de esta prueba. Los clientes en su lugar pueden requerir que el auditor firme un acuerdo de confidencialidad para garantizar que los datos que se reúnan y los resultados de las pruebas de intrusión sean privados y no puedan ser revelados a terceros. Además, en el caso del auditor, se debe ser consciente de las leyes locales que pudieran aplicarse como los canales y niveles de potencia permitidos. Es importante asegurarse de no romper ninguna de las leyes locales durante el test de penetración [13]

3.2. DESCUBRIMIENTO

En esta fase, vamos a explorar las redes inalámbricas y encontrar diferentes puntos de acceso y clientes en los alrededores. Para esto realizaremos los siguientes pasos:

Paso 1.- Crear una interfaz en modo monitor usando una tarjeta inalámbrica que tenga dicha capacidad o característica. La figura 3.1 muestra un ejemplo de configuración de una interfaz en modo monitor.

Figura 3.1 - Creación de interfaz modo monitor

Paso 2.- Usar ***airodump-ng*** para iniciar la exploración del espacio aéreo.

Paso 3.- Hay que desplazarse por las instalaciones para obtener mayor número de clientes y puntos de acceso como sea posible.

Paso 4.- Solicitar al administrador del sistema de la empresa una lista de direcciones MAC para todos los puntos de acceso y clientes inalámbricos. Esto nos ayudará en la fase de ataque [13]

3.3. ATAQUE

Esta es la fase principal del test de penetración donde no solo se detectaran las vulnerabilidades de la red, sino también se tratara de determinar si existen intentos de comprometer la red que se estén llevando a cabo actualmente. Este procedimiento debe ser llevado a cabo complementando los siguientes puntos:

- **Buscar Puntos de Acceso Falsos:** usando la información que tenemos acerca de la red, se procederá a encontrar e identificar los puntos de acceso cercanos a la empresa en busca de puntos de acceso con nombres similares o iguales que no pertenecen a la empresa y son colocados por un posible atacante para engañar a los usuarios para que se conecten a ellos.

- **Buscar clientes no autorizados:** se buscará equipos desconocidos que estén conectados a la red empresarial. Encontrar alguno puede significar que un usuario está usando equipos externos a la empresa para conectarse o que un usuario no autorizado ha obtenido acceso a la red.
- **Romper el cifrado:** se procederá a capturar y analizar el tráfico de red inalámbrico para luego aplicar técnicas de fuerza bruta o ataques de diccionario en un intento de obtener la clave de acceso a la red. Esto permitirá determinar la fortaleza de la contraseña y la configuración seguridad de la red inalámbrica.
- **Penetrar en la infraestructura:** de haber obtenido acceso a la red en los procesos anteriores, se determinará qué tipo de información se puede obtener o que daño se puede causar al acceder a la red.
- **Comprometer a los clientes:** en esta etapa se buscará forzar a un cliente a conectarse a un punto de acceso falso creado por nosotros.

3.4. PRESENTACIÓN DE INFORME

Una vez que se han encontrado todas las vulnerabilidades de seguridad, se debe informar a la empresa. La estructura del reporte puede variar, sin embargo, debe contener mínimo los siguientes datos [13]:

- Descripción de la vulnerabilidad
- Gravedad
- Dispositivos afectados
- Tipo de vulnerabilidad (software/hardware/configuración)
- Soluciones provisionales
- Remediación

Los niveles de gravedad es un aspecto importante del informe, ya que son una guía que permite conocer rápidamente la importancia de una vulnerabilidad o incidente de seguridad y el tipo de medidas a tomar para solucionarlo. Podemos encontrar una tabla de los niveles de gravedad básicos en un informe en el **Anexo 3**.

CAPÍTULO 4

4. VULNERABILIDADES EN REDES INALÁMBRICAS

Cuando nos referimos a vulnerabilidad en redes inalámbricas no es otra cosa que una debilidad en la red que permite que usuarios malintencionados puedan violar la integridad, disponibilidad o confidencialidad de la misma.

4.1. ESCENARIO DE PRUEBAS

Para realizar las pruebas necesarias y determinar las vulnerabilidades en una red inalámbrica, se ha creado un ambiente de laboratorio, que consta de los siguientes elementos:

- 1 Equipo portátil con el sistema para las auditorias de seguridad.
- Equipos clientes (Smartphones, laptops)
- 1 Ruteador inalámbrico.

La figura 4.1 muestra el escenario empleado para realizar pruebas para demostrar las fallas de seguridad en las redes inalámbricas.

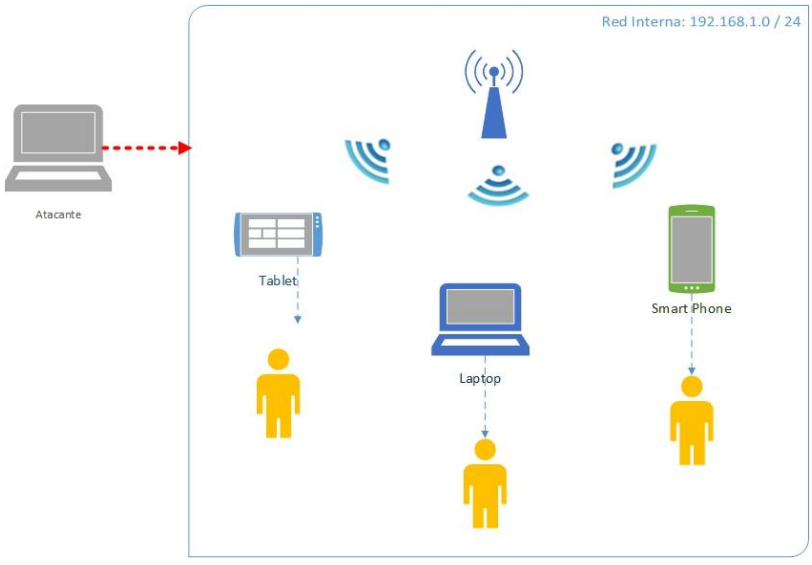


Figura 4.1 - Escenario de pruebas

4.2. EVALUACIÓN Y SELECCIÓN DE HERRAMIENTAS PARA ANÁLISIS DE VULNERABILIDADES EN UNA RED INALÁMBRICA.

Se han desarrollado un gran número de herramientas orientadas a facilitar la evaluación y auditoria de seguridad de redes y sistemas informáticos, incluso se pueden encontrar sistemas operativos completos que recopilan todas las herramientas necesarias para esta labor. A continuación revisaremos algunas de las distribuciones de Linux más reconocidas para la auditoria de redes inalámbricas.

- **Beini**

  Es una distribución de Linux para la auditoria de redes inalámbricas basada en Tiny Core Linux. Se destaca por su reducido tamaño y por incorporar herramientas con interfaz gráfica. Es considerado un sistema operativo para principiantes debido a su facilidad de uso. Carece de herramientas avanzadas, lo que limita su efectividad.

- **Wifiway**

  Es una distribución diseñada para la auditoria de seguridad en redes inalámbricas, bluetooth y RFID. A diferencia de otros sistemas, este no está basado en otras distribuciones sino que fue desarrollado desde cero.

- **Backtrack**

  Es un sistema operativo basado en Ubuntu derivado de dos distribuciones orientadas a la seguridad, el Auditor y el WHAX. El sistema incluye una amplia gama de herramientas que pueden ser usadas para realizar auditorías de seguridades a nivel empresarial.

- **Kali Linux**

  Es una distribución basada en Debian, es la evolución del sistema Backtrack. Kali Linux fue diseñado para la auditoria de seguridad informática en general. Admite la re-compilación del núcleo lo que permite agregar controladores, parches o nuevas funcionalidades que no estén incluidas en el kernel original.

En un comienzo se descartó el uso de Beini por no ser una herramienta de uso profesional. Si bien es efectiva en algunos procesos sencillos, esta no permite demostrar detalladamente el procedimiento realizado por las herramientas de auditoría.

Wifiway es un sistema totalmente enfocado en la auditoria de redes inalámbricas, cuenta con todas las herramientas necesarias y sería una elección válida para un proceso de análisis de vulnerabilidades

en una red inalámbrica; sin embargo, hemos optado por Backtrack 5 R3 principalmente por contar con un mayor soporte y documentación.

Aun cuando su desarrollo se haya detenido el año 2013, debido a la aparición de Kali Linux, la cantidad de información y documentación disponibles es mayor a la de otros sistemas. Además, aun cuenta con soporte por parte de los desarrolladores y la comunidad en sus foros oficiales.

En el proyecto realizado no se usó Kali Linux porque estaba aún en fase de pruebas y por no contar con la sufriente información en los foros sobre su implementación en auditorias de redes. La falta de información sobre el funcionamiento con ciertas tarjetas de redes también fue una limitante para el uso del sistema operativo.

4.3. EVASIÓN DE LA AUTENTICACIÓN INALÁMBRICA

Este tipo de ataques busca obtener acceso a la red inalámbrica de manera fraudulenta evadiendo los esquemas de seguridad más débiles encontrados en redes inalámbricas. El porcentaje de éxito de estos ataques es del 100%, además de tomar unos pocos minutos y ser sencillos de realizar.

4.3.1. Descubrir un SSID oculto

La configuración predeterminada de todos los puntos de acceso o ruteadores inalámbricos permiten la tra**n**smisión del identificador de red llamado SSID, que a su vez permite que clientes que se encuentren en un área cercana se conecten. Los administradores de red habilitan en el punto de acceso la opción “SSID no visible”, para que el equipo no emita su SSID y solo los usuarios que lo conozcan puedan conectarse.

Este método de seguridad implementado no ofrece una protección robusta ya que existen métodos para descubrir el SSID de una red. Un punto de acceso configurado para que su SSID no sea visible puede ser detectado fácilmente por medio de cualquier sistema o software de auditoría de redes. Sin embargo, un equipo no podrá realizar una conexión hacia el punto de acceso normalmente sin conocer el SSID y la contraseña respectiva.

En la figura 4.2 se puede observar como en sistemas operativos como Linux es fácilmente visible la información de la red, aun cuando el identificador se encuentra oculto. Además, es posible observar información tal como el tipo de seguridad, el canal y el porcentaje de señal. Otro método para

la identificación de redes inalámbricas es mediante el uso de software en conjunto con hardware que permita realizar un escaneo completo de todos los puntos de accesos inalámbricos disponibles para la conexión.

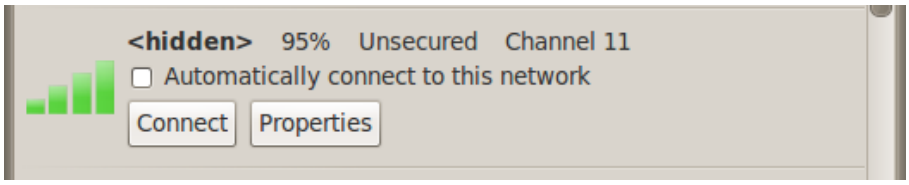


Figura 4.2 - Administrador de redes inalámbricas Linux

La figura 4.3 muestra el resultado de este comando, donde podemos visualizar la siguiente información que se será de utilidad para realizar el ataque a la red.

- Dirección MAC del Punto de Acceso
- Canal de trasmisión de información
- Frecuencia en la que trabaja el AP
- Calidad de la señal
- El tipo de cifrado configurado
- Identificador de la red: SSID
- Velocidad permitida de trasmisión

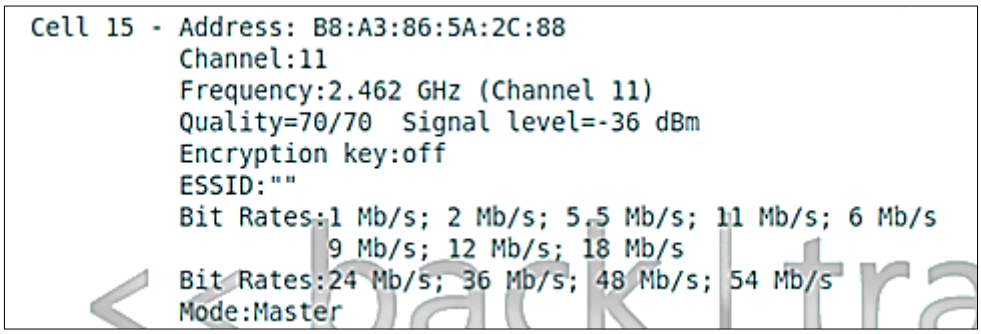


Figura 4.3 - Resultado de escaneo de redes disponibles

Con el comando ***<airmon-ng start wlan1>***, se activa el modo monitor de las tarjetas inalámbricas. También puede usarse para detener las interfaces y salir del modo monitor. Si escribimos el comando ***<airmon-ng>*** sin parámetros veremos el estado de nuestras tarjetas. [13] La salida de este comando se puede observar en la figura 4.4

Figura 4.4 - Interfaz de red inalámbrica: modo monitor

Wireshark es el programa que se utilizó en el análisis de los paquetes capturados por la interfaz configurada en modo

monitor. Entre los paquetes que captura el Wireshark está el nombre de la red que se encuentra oculta (SSID).

En la figura 4.5 se muestra una consola de Wireshark configurada para que desde la interfaz mon0 (monitor) capture todo el tráfico generado entre ambas partes – Cliente – Punto de Acceso. El proceso de descubrimiento del SSID puede tardar varios minutos ya se debe esperar que un cliente se conecte a la red.

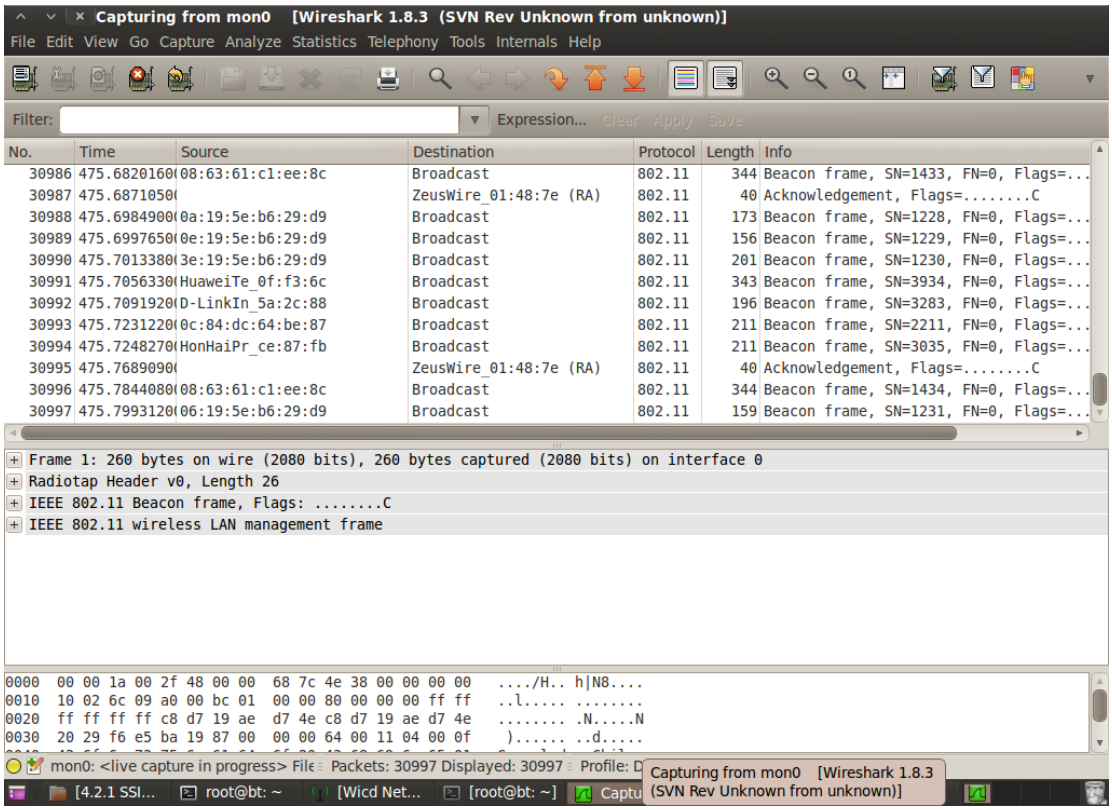


Figura 4.5 - Consola de Wireshark

Otro método es forzar que un cliente se des-autentique para así generar los paquetes necesarios para obtener la información requerida. Como se muestra en la Figura 4.6.

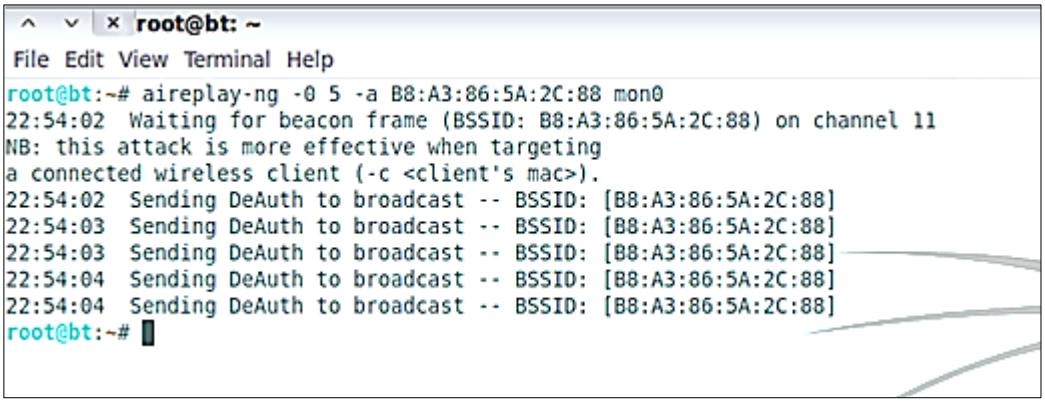


Figura 4.6 - Captura del proceso de autenticación

La función básica del ***airplay-ng*** es generar tráfico para ser usado en lo posterior por el ***aircrack-ng*** y así realizar el proceso de obtención de las claves WEP/WPA/WPA2. La figura 4.6 muestra la salida del comando ***airplay-ng.*** Los parámetros a usar son los siguientes [14]:

- Ataque 0: De-autenticación
- Ataque 5: Fragmentación
- BSSID: Dirección MAC del Punto de Acceso
- Mon0: interfaz en modo monitor

Cuando el Wireshark captura paquetes por medio de la interfaz inalámbrica en modo monitor, se visualizan todos los paquetes que viajan por el medio, si un cliente nuevo se intenta conectar se enviará el SSID para completar el proceso de conexión. Este proceso se muestra en la figura 4.7.

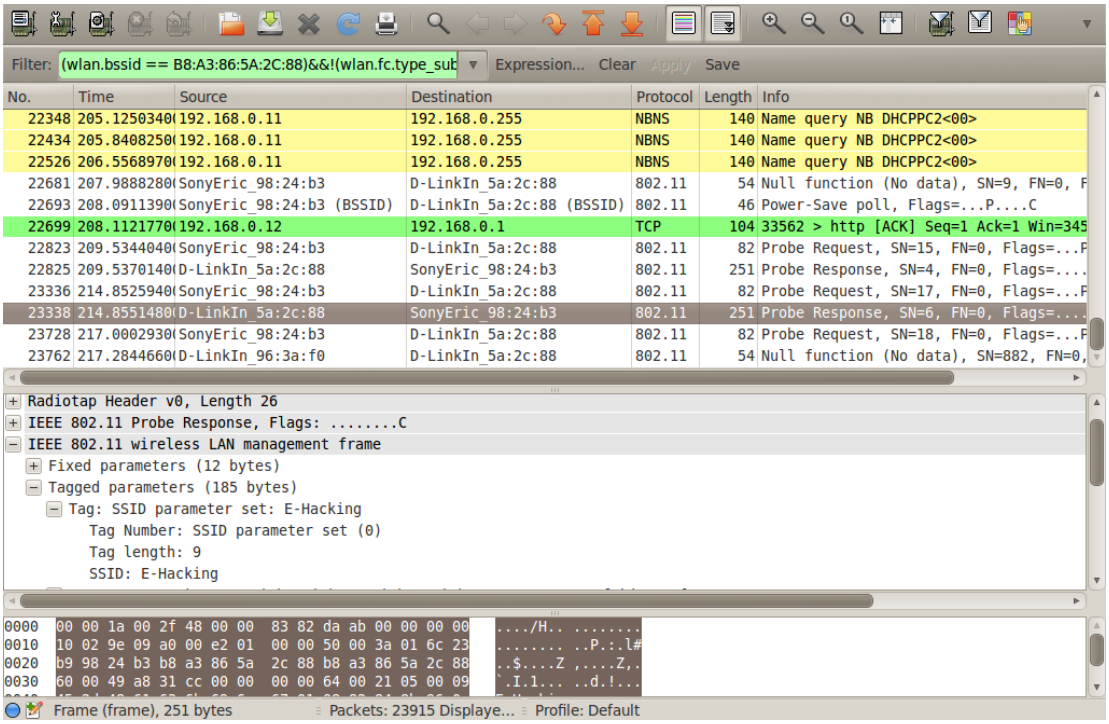


Figura 4.7 - Paquetes capturados por Wireshark

Una vez capturado una cierta cantidad de paquetes, estos serán visibles en el Wireshark, es posible utilizar un filtro para supervisar todos los paquetes no-beacon (no guiados), de extremo a extremo. (wlan.bssid == B8:A3:86:5A:2C:88) && (wlan.fc.type_subtype == 0x08) [13]

4.3.2. Eludir Filtrado MAC

El filtrado de direcciones MAC es una técnica de protección, autenticación y autorización que aún se piensa que es un método para asegurar la red, ya que solo los equipos registrados en la tabla MAC del Ruteador o Punto de acceso pueden conectarse. La figura 4.8 muestra un escenario de red protegido por filtrado de direcciones MAC.

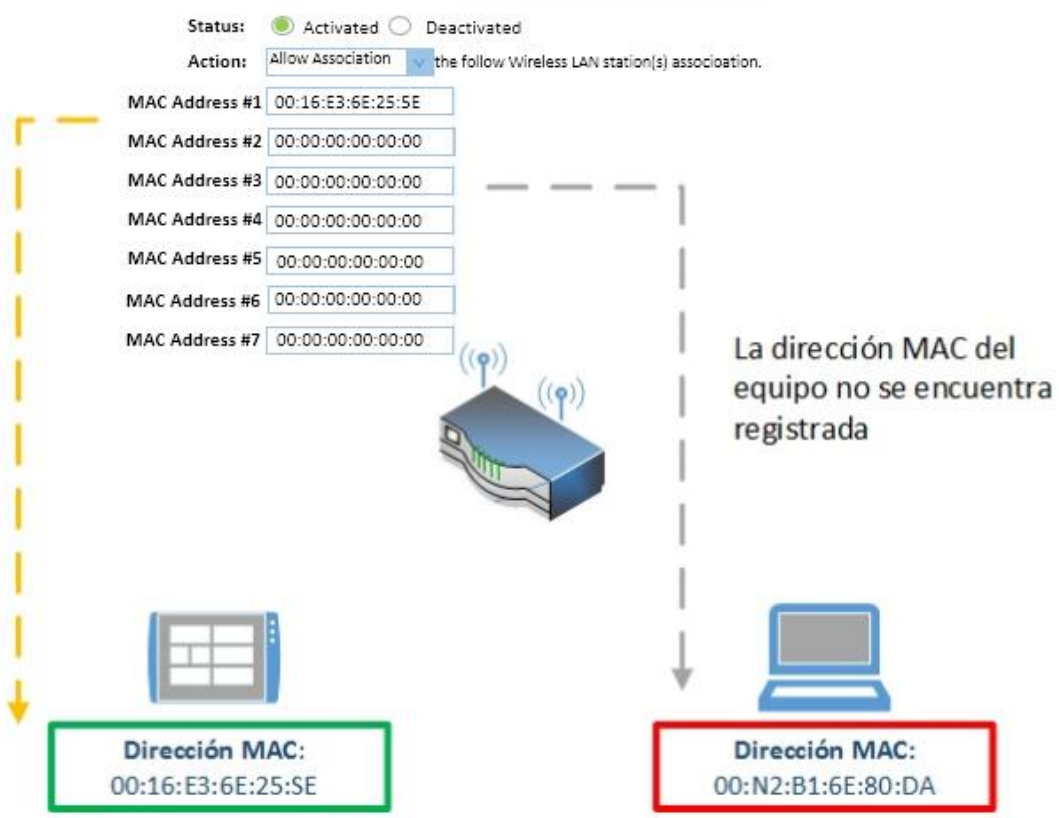


Figura 4.8 - Escenario de red: clientes registrados en la tabla MAC

Este método de seguridad solo se basa en las direcciones físicas de los equipos (MAC), que se encuentra guardada en una tabla que poseen los equipos de conexión, en este caso un Ruteador inalámbrico. Como se muestra en la figura 4.9, si un cliente intenta conectarse la operación no tendrá éxito debido a que la dirección MAC no se encuentra registrada, sin importar que la red se encuentre asegurada con una clave o sin clave.

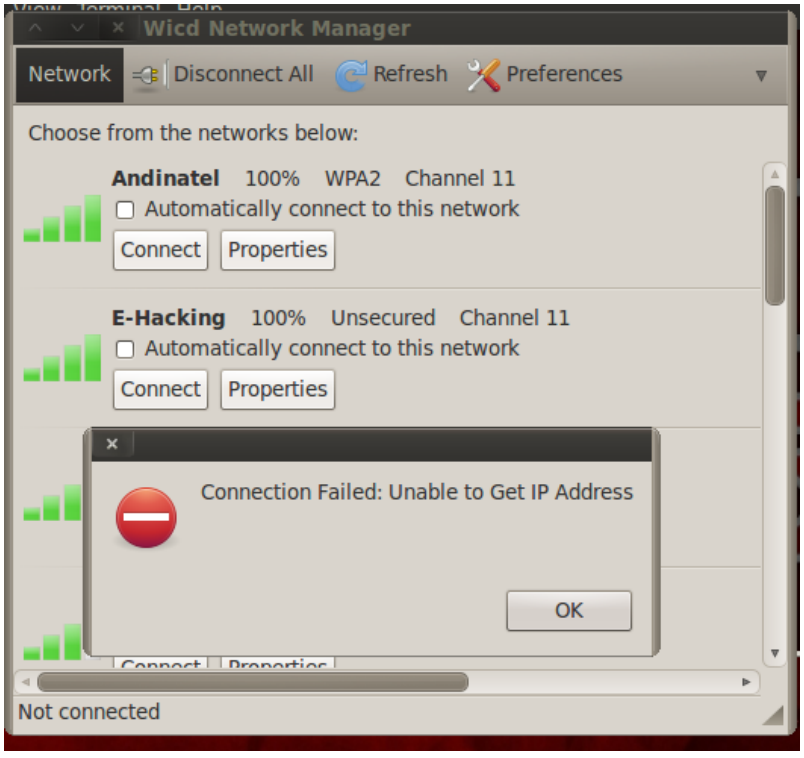


Figura 4.9 - Conexión a red protegida con filtrado MAC

Para proceder a conectarse a un punto inalámbrico sin tener que estar registrado en la tabla MAC, es necesario monitorear el entorno y esperar a que un cliente se conecte, en este caso para tomar su dirección MAC y copiarla. El proceso se realiza mediante el siguiente comando:

Airodump-ng –c <Canal> –a --bssid <Dirección Mac> <interfaz monitor>

El parámetro –C indica el canal en el que se encuentra trabajando la red inalámbrica, el parámetro –a asegura que solo se muestre información del cliente que se ha conectado al Punto de Acceso, el BSSID , es la dirección MAC del punto de acceso al cual se desea conectar. La salida de este comando se muestra en la figura 4.10.

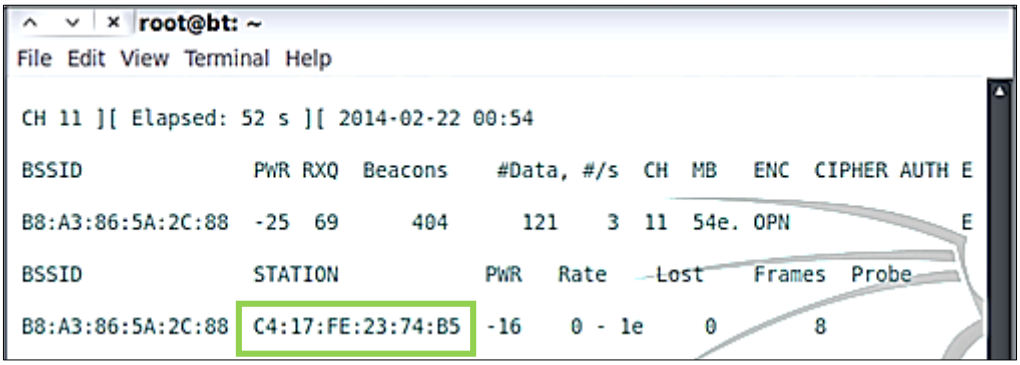


Figura 4.10 - Dirección MAC del cliente que será copiada

Una vez obtenida la información requerida se procede a la utilización del comando ***<macchange>*,** el cual permite cambiar dirección MAC propia de la interfaz inalámbrica que se esté usando. La figura 4.11 muestra el funcionamiento de este comando.

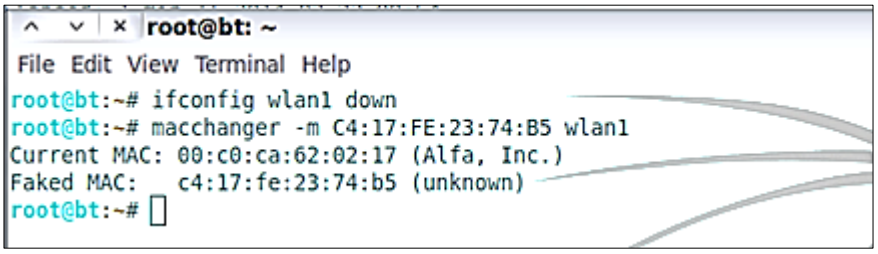


Figura 4.11 - Cambio de dirección MAC a una interfaz de red

Una vez que el equipo que no pertenece a la red copia la dirección MAC de un cliente, este realiza un proceso de des-autenticación para desconectar al host cliente y poder conectar el equipo intruso a la red mediante la MAC duplicada. La figura 4.12 muestra como luego de copiar la dirección MAC de un cliente legítimo le es posible al atacante conectarse a la red. El atacante tendrá acceso a la red mientras que el cliente original no podrá conectarse debido a que ya existe un equipo con una MAC registrada (MAC duplicada).

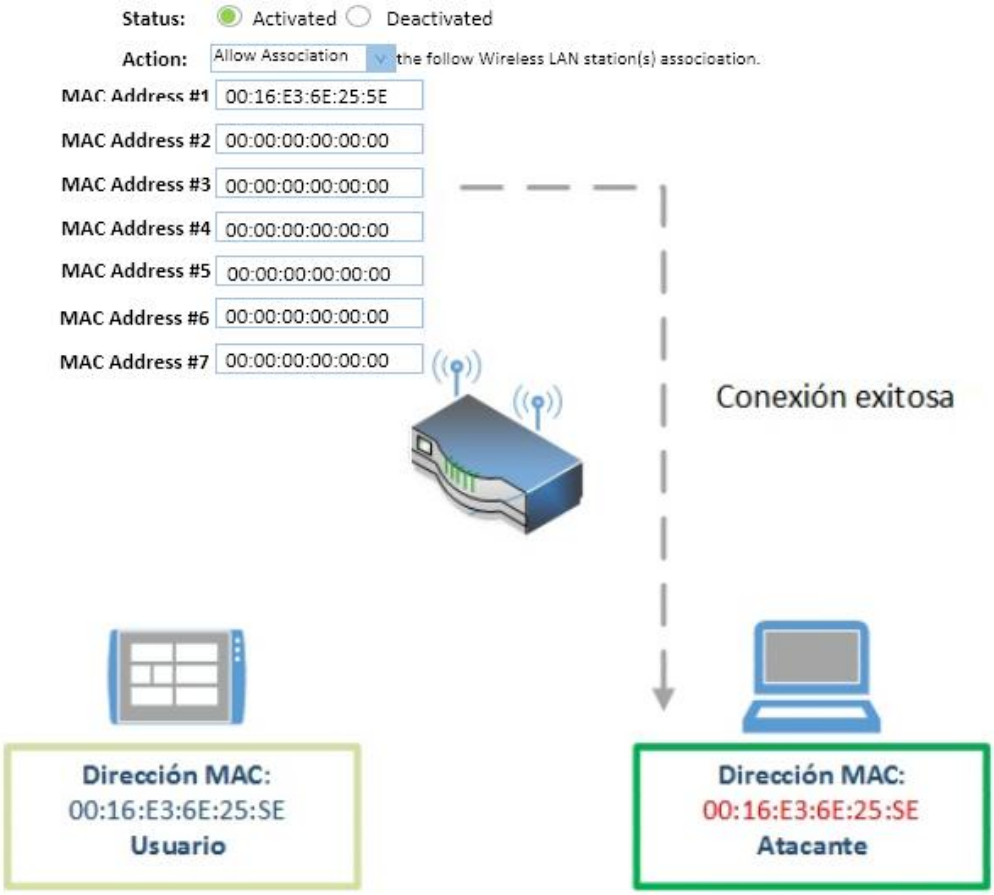


Figura 4.12 - Diagrama de red: Intervención de intruso mediante dirección MAC

Al realizar una comprobación de la conexión mediante el comando ***<iwconfig>,*** se puede observar que el equipo intruso se encuentra asociado al punto de acceso antes visto. La figura 4.13 muestra la salida de este comando.

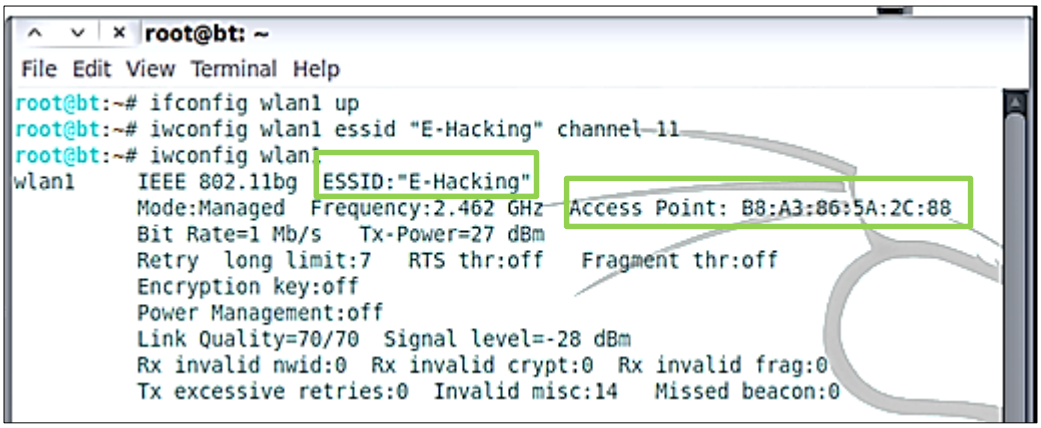


Figura 4.13 - Resultado de conexión mediante una dirección MAC copiada

4.3.3. Eludir autenticación de clave compartida WEP

Para realizar una prueba de intrusión en una red inalámbrica, es necesario detectar un punto de acceso vulnerable. La figura 4.14 muestra el proceso de autenticación de clave compartida.

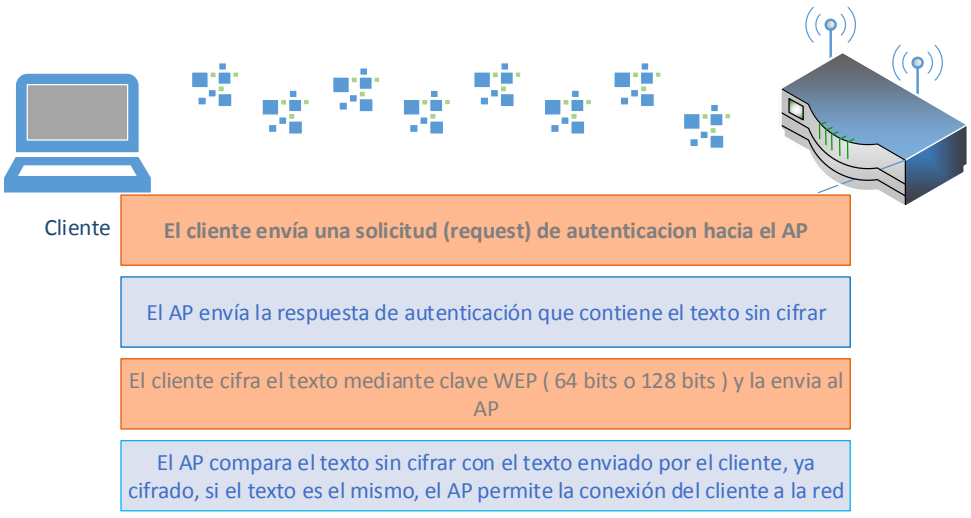


Figura 4.14 - Proceso de autenticación con clave compartida

Con un escaneo general de las redes disponibles se obtendrá el SSID de la red, señal, direccion MAC del Punto de Acceso, y lo mas importante, el tipo de seguirdad. Toda la informacion recolectada es indispensable para poder realizar una conexión exitosa hacia la red. Entre mas óptima sea la señal que emite el Punto de Aceso mayor sera la posibilidad de conexión. La figura 4.15 muestra la interfaz del software inSSIDer, una de las herramientas que permiten hacer un escaneo general de las redes inalambricas.

En el gráfico se puede observar una red con una señal óptima, y con seguirdad de clave compartida – WEP, la cual será de utilidad para realizar la prueba descrita.

Una vez obtenida la información se procede a realizar un monitoreo de la red en espera que un cliente se conecte para interceptar los paquetes de asociación que se envian entre el Punto de Acceso y el clente mediante el comando ***<airodump-ng>***

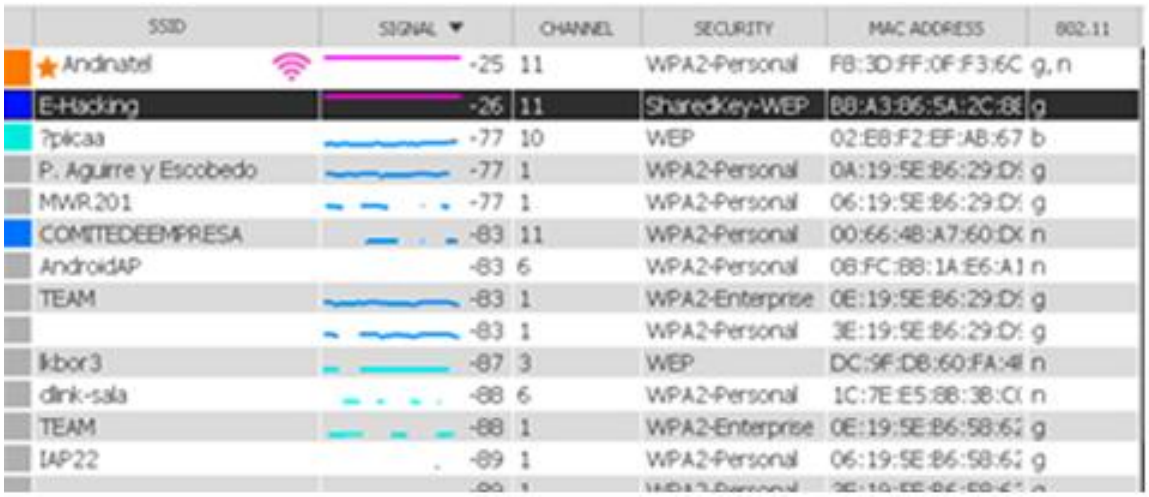


Figura 4.15 - Interfaz del software inSSIDer

Una vez que un host se conecte al Punto de Acceso será detectado, indicando cuál es su dirección MAC y el tipo de autenticación que usa, en este caso SKA. Un indicador de que se ha capturado la información necesaria para descifrar la clave compartida es que en la columna AUTH se muestre el tipo de autenticación. Esto se muestra en la salida del comando ***<airodump-ng>*** en la figura 4.16.

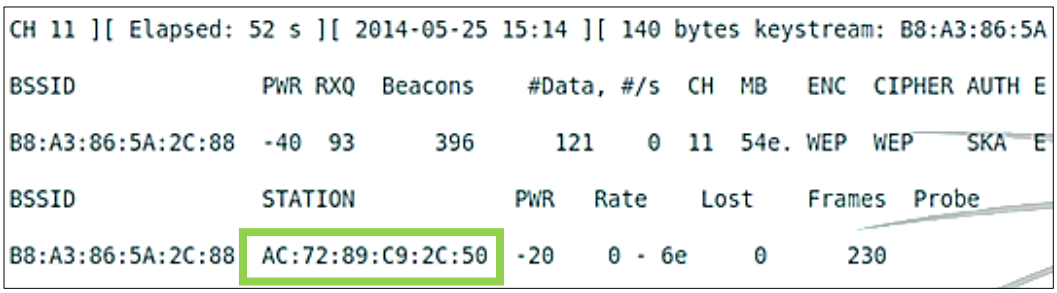


Figura 4.16 - Información del cliente conectado a la red

La captura realizada se guardara en un directorio con el nombre por defecto, esto será keystream ***- dirección mac -*** .xor el cual contiene la clave compartida. En la figura 4.17 vemos un ejemplo de un archivo keystream generado automáticamente.

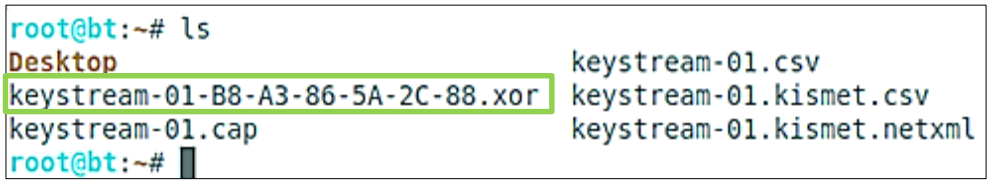


Figura 4.17 - Archivos creados automáticamente al monitorear la red

Para falsificar una autenticación de clave compartida, es necesario usar la herramienta <***aireplay-ng>,*** la cual sus parámetros son descritos en la Tabla 2:

aireplay-ng -1 0 –e E-Hacking –y keystream-01-B8:A3:B6:5A:2C:88.XOR –a B8:A3:B6:5A:2C:88 –h aa:aa:aa:aa:aa:aa mon0

Parámetro	**Descripción**
-1	Falsa autenticación
0	tiempo de re asociación en segundos

-e E-Hacking	Nombre de la red Wireless
-y keystream…xor	Nombre del archivo capturado
-a B8:A3:86:5ª:2C:88	Dirección MAC del Punto de acceso
-h aa:aa:aa:aa:aa:aa	Dirección MAC falsa
mon0	Nombre de la interfaz usada

Tabla 2 - Parámetros del airplay-ng

Si todos los parámetros se encuentran correctos al ejecutar el comando <**aireplay-ng>** se mostrarán varios mensajes indicando una autenticación exitosa hacia el punto de acceso seleccionado, como se puede observar en la figura 4.18

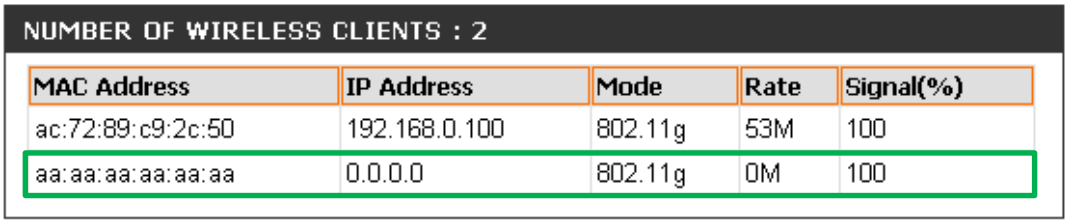
```
The interface MAC (00:C0:CA:62:02:17) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether AA:AA:AA:AA:AA:AA
15:37:34  Waiting for beacon frame (BSSID: B8:A3:86:5A:2C:88) on channel 11

15:37:34  Sending Authentication Request (Shared Key) [ACK]
15:37:34  Authentication 1/2 successful
15:37:34  Sending encrypted challenge. [ACK]
15:37:34  Authentication 2/2 successful
15:37:34  Sending Association Request [ACK]
15:37:34  Association successful :-) (AID: 1)
```

Figura 4.18 - Proceso de autenticación con la dirección MAC falsa

Para verificar el éxito de la prueba, en la tabla de clientes inalámbricos que posee el ruteador se puede observar un cliente asociado con una MAC distinta a las direcciones habituales. Esto se puede observar en la figura 4.19

La dirección MAC ***aa:aa:aa:aa:aa:aa*** falsa es la que se ha ingresado para realizar la autenticación, el ruteador no puede determinar la veracidad de la MAC, tan solo evalúa la clave compartida. Cabe recalcar que en este proceso no se sabe en ningún momento cual es la clave, tan solo se realiza el proceso de autenticación hacia un punto de acceso.


NUMBER OF WIRELESS CLIENTS : 2

MAC Address	IP Address	Mode	Rate	Signal(%)
ac:72:89:c9:2c:50	192.168.0.100	802.11g	53M	100
aa:aa:aa:aa:aa:aa	0.0.0.0	802.11g	0M	100

Figura 4.19 - Dirección MAC falsa agregada a la tabla MAC del Ruteador.

4.4. ATAQUES EN LA INFRAESTRUCTURA

Estos ataques están enfocados a los principales protocolos de seguridad en redes inalámbricas, desde los primeros en aparecer como WEP hasta sistemas de seguridad más complejos que incluyen el uso de servidores de autenticación como WPA2-Enterprise con servidores RADIUS. La figura 4.20 muestra un ejemplo de un posible escenario de ataque.

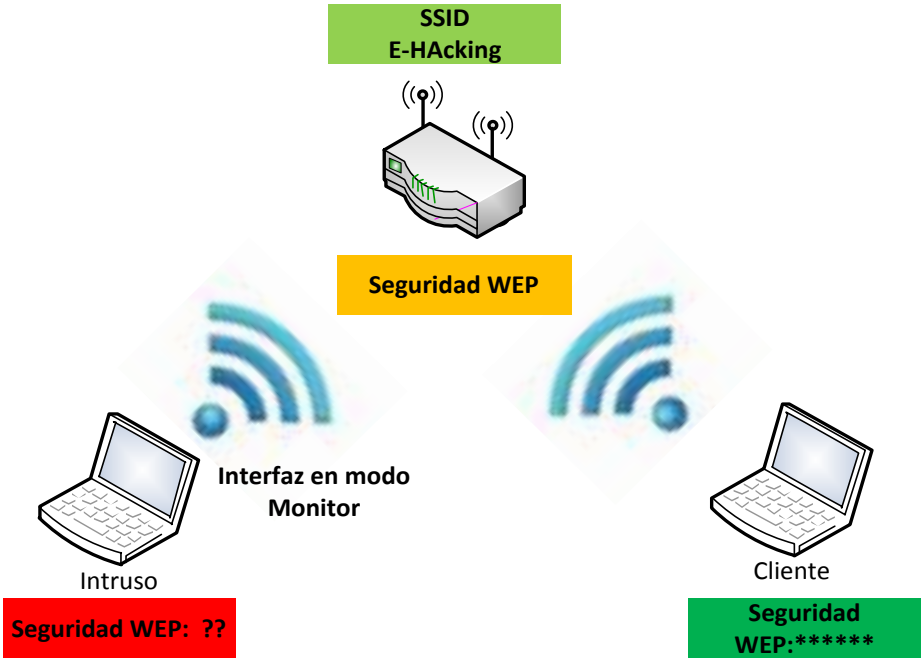


Figura 4.20 - Escenario de red: Mecanismo de seguridad WEP

4.4.1. Descifrar claves WEP

El primer paso para realizar el procedimiento de conexión hacia una red con seguridad WEP, es realizar un escaneo de las redes disponibles en el medio que se encuentre configurado con dicha seguridad. La figura 4.21 muestra una red con seguridad WEP detectada por medio del administrador de redes inalámbricas de Linux. Una vez localizado el objetivo se debe iniciar la interfaz inalámbrica en modo monitor como se muestra en la figura 4.22.

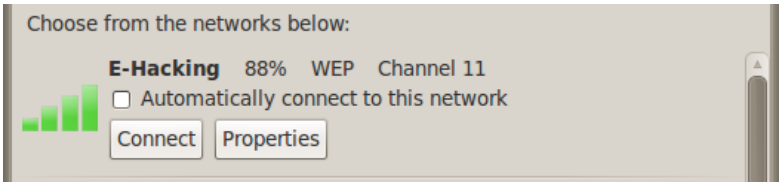


Figura 4.21 - Red con seguridad WEP

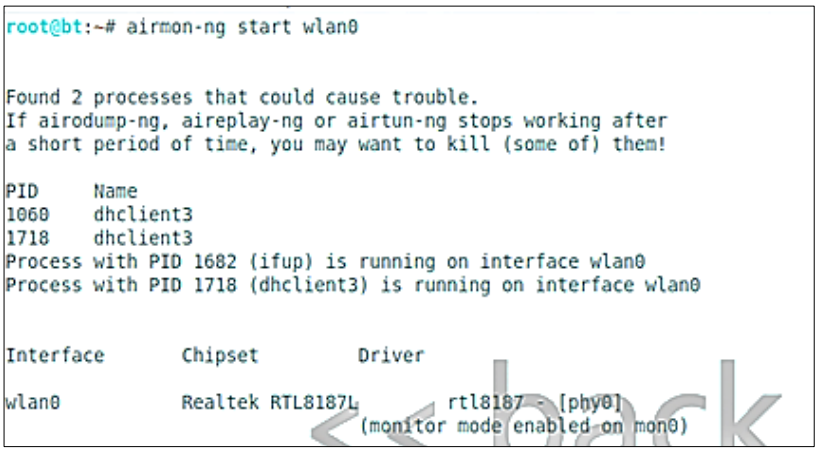
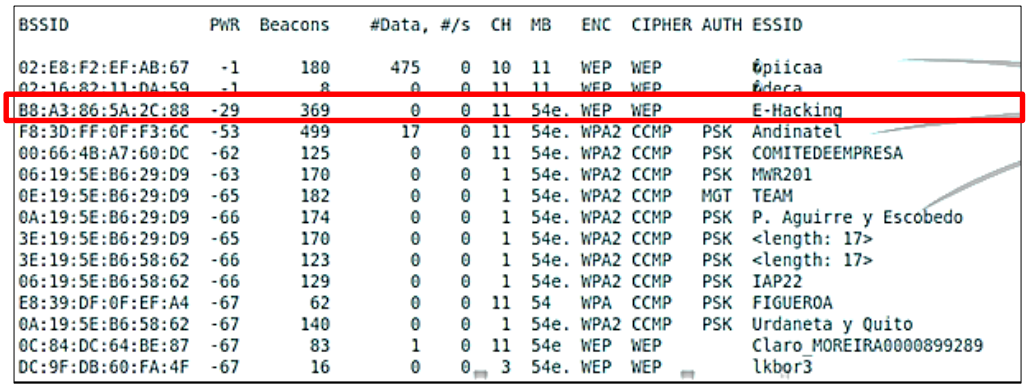


Figura 4.22 - Interfaz modo monitor: Monitoreando conexiones WEP

Con el comando ***<Airodump-ng>*** obtendremos más información de la red inalámbrica como la dirección MAC del AP, el tipo de seguridad usada, el canal de transmisión, y la potencia de la señal; toda esta información es valiosa para realizar la respectiva conexión. La figura 4.23 muestra la salida del comando ***<Airodump-ng>.***



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
02:E8:F2:EF:AB:67	-1	180	475	0	10	11	WEP	WEP		ópiicaa
02:16:82:11:DA:59	-1	8	0	0	11	11	WEP	WEP		ódeca
B8:A3:86:5A:2C:88	-29	369	0	0	11	54e.	WEP	WEP		E-Hacking
F8:3D:FF:0F:F3:6C	-53	499	17	0	11	54e.	WPA2	CCMP	PSK	Andinatel
00:66:4B:A7:60:DC	-62	125	0	0	11	54e.	WPA2	CCMP	PSK	COMITEDEEMPRESA
06:19:5E:B6:29:D9	-63	170	0	0	1	54e.	WPA2	CCMP	PSK	MWR201
0E:19:5E:B6:29:D9	-65	182	0	0	1	54e.	WPA2	CCMP	MGT	TEAM
0A:19:5E:B6:29:D9	-66	174	0	0	1	54e.	WPA2	CCMP	PSK	P. Aguirre y Escobedo
3E:19:5E:B6:29:D9	-65	170	0	0	1	54e.	WPA2	CCMP	PSK	<length: 17>
3E:19:5E:B6:58:62	-66	123	0	0	1	54e.	WPA2	CCMP	PSK	<length: 17>
06:19:5E:B6:58:62	-66	129	0	0	1	54e.	WPA2	CCMP	PSK	IAP22
E8:39:DF:0F:EF:A4	-67	62	0	0	11	54	WPA	CCMP	PSK	FIGUEROA
0A:19:5E:B6:58:62	-67	140	0	0	1	54e.	WPA2	CCMP	PSK	Urdaneta y Quito
0C:84:DC:64:BE:87	-67	83	1	0	11	54e	WEP	WEP		Claro_MOREIRA0000899289
DC:9F:DB:60:FA:4F	-67	16	0	0	3	54e.	WEP	WEP		lkbor3

Figura 4.23 - Escaneo de redes disponibles

Para la prueba se tomó la dirección MAC del AP --88:A3:86:5A:2C:88, y se procedió a monitorear solo dicho punto de acceso, en espera de que un cliente se conecte. Una vez que el cliente se conectó toda la información que viajaba por el medio se guardó en un archivo.

El comando ***<airodump-ng>*** es el encargado de capturar paquetes del medio inalámbrico además de acumular los vectores de inicialización que serán usado con el ***<aircrack-ng>*** con el fin de obtener la clave WEP. La figura 4.24 muestra la salida del comando ***<airodump-ng>*** donde podemos observar

el proceso de conexión entre el cliente y el AP.

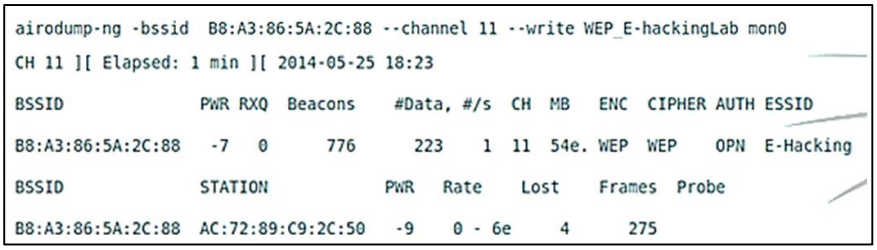


Figura 4.24 - Proceso de conexión: Cliente-AP

A continuación se detalla el significado de cada uno de los campos mostrados por el comando ***<airodump-ng>*** [15]:

- **BSSID:** Dirección MAC del punto de acceso.
- **PWR:** Nivel de señal. Su significado depende del controlador que usemos, pero cuanto mayor sea el PWR más cerca estaremos del AP o del cliente. Si el PWR es -1, significa que el controlador no soporta la detección del nivel de señal. Si el PWR es -1 para algunos clientes (estaciones) es porque los paquetes proceden del AP hacia el cliente pero las transmisiones del cliente se encuentran fuera del rango de cobertura de la tarjeta. Lo que significa que solo escuchas la mitad de la comunicación. Si todos los clientes tienen PWR -1 significa que el controlador no tiene la capacidad de detectar el nivel de señal.

- **RXQ:** Calidad de recepción calculada a través del porcentaje de paquetes recibidos correctamente en los últimos 10 segundos.
- **Beacons:** Número de “paquetes anuncio” o Beacons enviadas por el AP. Cada punto de acceso envía alrededor de diez Beacons por segundo cuando la velocidad (rate) es de 1M, (la más baja) de tal forma que se pueden recibir desde muy lejos.
- **# Data:** Número de paquetes de datos capturados (si tiene clave WEP, equivale también al número de IVs), incluyendo paquetes de datos broadcast (dirigidos a todos los clientes).
- **#/s:** Numero de paquetes de datos capturados por segundo calculando la media de los últimos 10 segundos.
- **CH:** Canal en la que se encuentra el AP.
- **MB:** Velocidad soportada por el AP.
- **ENC:** Algoritmo de encriptación que se usa. OPN = no existe encriptación (abierta),”WEP?” = WEP u otra (no se han capturado suficientes paquetes de datos para saber si es WEP o WPA/WPA2), WEP (sin el

interrogante) indica WEP estática o dinámica, y WPA o WPA2 en el caso de que se use TKIP o CCMP.

- **CIPHER:** Tipo de cifrado de datos, Puede ser CCMP, WRAP, TKIP, WEP, WEP40, o WEP104.
- **AUTH:** El protocolo de autenticación usado. Puede ser MGT, PSK (clave pre compartido), o OPN (abierta).
- **ESSID:** También llamado “SSID”, que puede estar en blanco si la ocultación del SSID está activada en el AP. En este caso, airodump-ng intentará averiguar el SSID analizando paquetes “Probe responses” y “association request” (son paquetes enviados desde un cliente al AP).
- **STATION:** Dirección MAC del Cliente conectado al AP.
- **Lost:** El número de paquetes perdidos en los últimos 10 segundos.
- **Frames:** El número de paquetes de datos enviados por el cliente.
- **Probes:** Los ESSIDs a los cuales ha intentado conectarse el cliente.

La figura 4.25 muestra la salida del comando ***<ls>,*** donde se podrá observar varios archivos creados, los cuales contienen la información de negociación entre el Punto de Acceso y el cliente. Posteriormente se ejecutó el comando ***<aireplay-ng>*** de la siguiente manera:

```
root@bt:~# aireplay-ng -3 -b B8:A3:86:5A:2C:88 -h AC:72:89:C9:2C:50 mon0
```

```
root@bt:~# ls
Desktop                                keystream-01.kismet.netxml
keystream-01-B8-A3-86-5A-2C-88.xor     WEP_E-hackingLab-01.cap
keystream-01.cap                       WEP_E-hackingLab-01.csv
keystream-01.csv                       WEP_E-hackingLab-01.kismet.csv
keystream-01.kismet.csv                WEP_E-hackingLab-01.kismet.netxml
root@bt:~#
```

Figura 4.25 - Archivos que contienen información de conexión Cliente-AP

Al momento de ejecutar el aireplay-ng, el airodump-ng también empezará a trabajar y a registrar todos los paquetes generados (frames). La información obtenida por los comandos descritos se muestra en las figuras 4.26, 4.27.

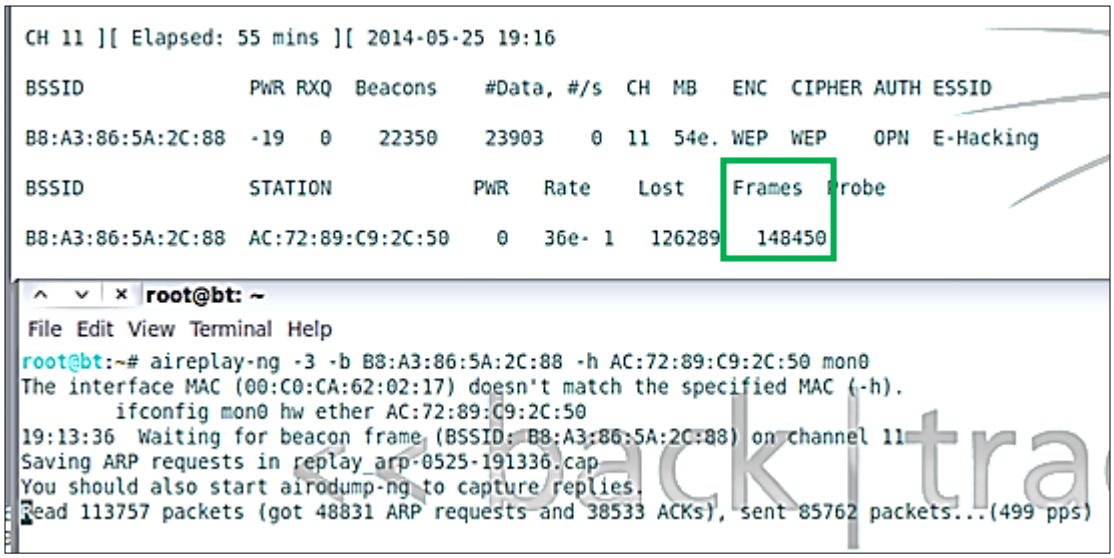


Figura 4.26 - Proceso de generación de tramas

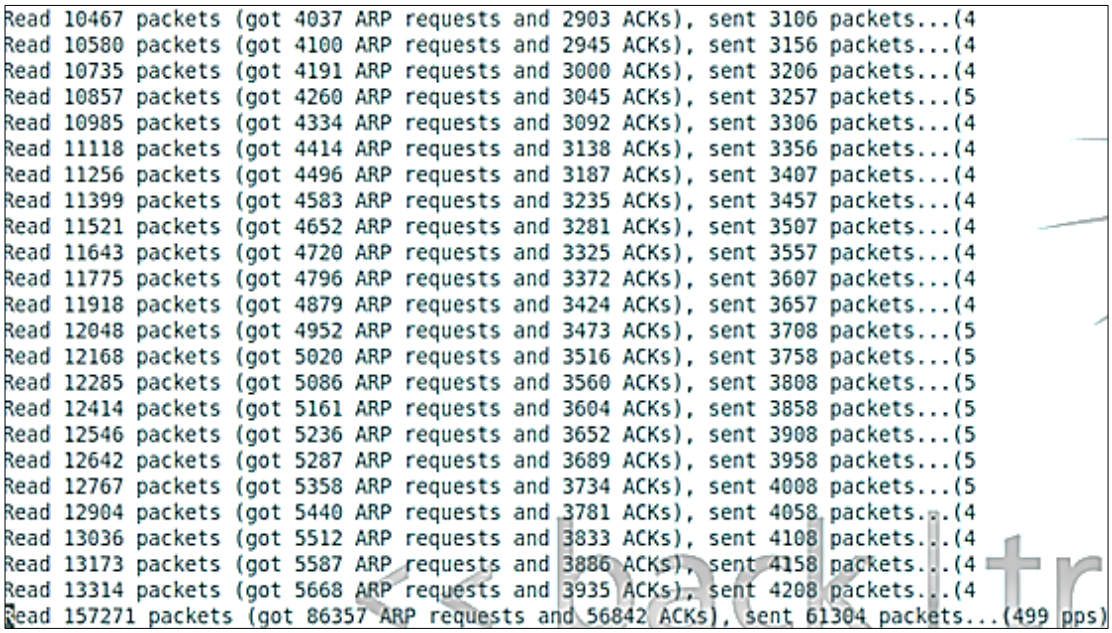


Figura 4.27 - Requerimientos ARP

Todos estos paquetes son almacenados en los archivos antes creados (WEP_E-hacking.cap). Entre mayor sea la cantidad de tramas enviadas habrá mayor posibilidad de obtener la clave de la red inalámbrica. Cuando la herramienta sea capaz de capturar la suficiente cantidad de IVs, la contraseña podrá ser descifrada. La figura 4.28 muestra el análisis de los IVs capturados y el proceso de descifrado de la contraseña.

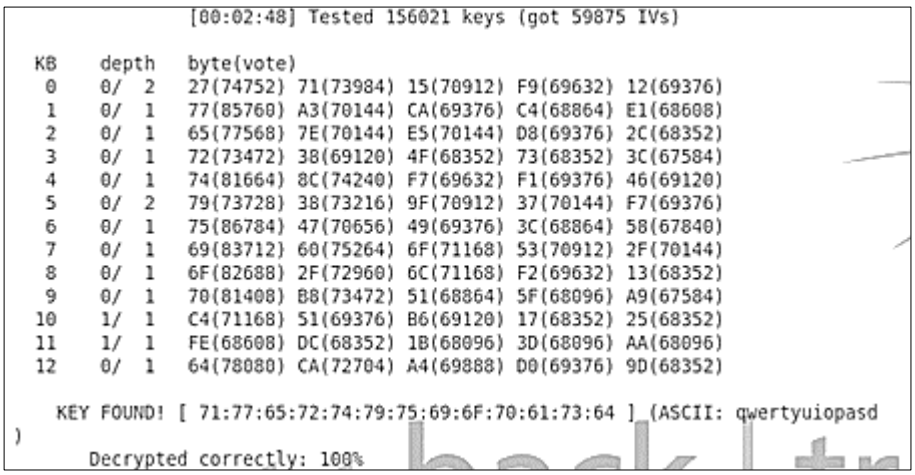


Figura 4.28 - Comprobación de IVs y proceso de descifrado

4.4.2. Descifrar claves WPA/WPA2

Para poder descifrar claves WPA/WPA2 se debe tener en cuenta la complejidad que esto representa, ya que el proceso de cifrado es más complejo que WEP.

Se mostraran 2 formas, de obtener una clave WPA/WPA2

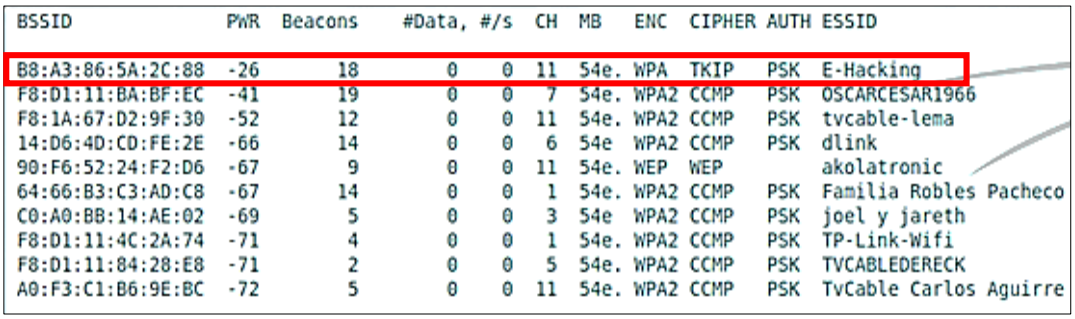
- Ataque de Diccionario
- John the Ripper

El ataque de diccionario

Se lleva a cabo mediante un archivo con múltiples palabras contenidas normalmente en un diccionario real que puede estar en diversos idiomas. De manera predeterminada el sistema operativo usado para realizar las pruebas viene con un diccionario cargado el cual servirá para realizar un ataque de bajo nivel para demostrar el procedimiento y funcionamiento del ataque de diccionario

Para empezar con el procedimiento de obtención de una clave WPA/WPA2 es necesario realizar un escaneo de las redes disponibles, por lo general mayoría de redes de microempresas, negocios o de casa poseen claves WPA/WPA2.

En la figura 4.29 como resultado del escaneo de las redes podemos visualizar una red (E-Hacking) que posee una clave WPA la cual se puede atacar. El algoritmo de cifrado (ENC) es WPA, el tipo de cifrado es TKIP y la autenticación es PSK.



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B8:A3:86:5A:2C:88	-26	18	0	0	11	54e.	WPA	TKIP	PSK	E-Hacking
F8:D1:11:BA:BF:EC	-41	19	0	0	7	54e.	WPA2	CCMP	PSK	OSCARCESAR1966
F8:1A:67:D2:9F:30	-52	12	0	0	11	54e.	WPA2	CCMP	PSK	tvcable-lema
14:D6:4D:CD:FE:2E	-66	14	0	0	6	54e	WPA2	CCMP	PSK	dlink
90:F6:52:24:F2:D6	-67	9	0	0	11	54e.	WEP	WEP		akolatronic
64:66:B3:C3:AD:C8	-67	14	0	0	1	54e.	WPA2	CCMP	PSK	Familia Robles Pacheco
C0:A0:BB:14:AE:02	-69	5	0	0	3	54e	WPA2	CCMP	PSK	joel y jareth
F8:D1:11:4C:2A:74	-71	4	0	0	1	54e.	WPA2	CCMP	PSK	TP-Link-Wifi
F8:D1:11:84:28:E8	-71	2	0	0	5	54e.	WPA2	CCMP	PSK	TVCABLEDERECK
A0:F3:C1:B6:9E:BC	-72	5	0	0	11	54e.	WPA2	CCMP	PSK	TvCable Carlos Aguirre

Figura 4.29 - Detección de redes disponibles

Una vez obtenido los datos de la red, se usó el comando ***<airodump-ng>*** con el cual se realizó la captura de paquetes, con el fin de obtener la información deseada, en este caso el proceso de autenticación:

airodump-ng --bssid B8:A3:86:5A:2C:88 --channel 11 --write WPA_E-HackingLab mon0

Se creó un archivo en donde se guardó toda la información necesaria para poder obtener la clave WPA/WPA2, con el parámetro – Write <*Nombre del archivo* >.

Una vez ejecutado el comando ***<airodump-ng>*** se debe esperar a que un cliente se conecte a la red, lo cual para saber si se ha realizado el proceso de conexión se debe visualizar como en la figura 4.30, la estación asociada al punto de

acceso, esto se puede comprobar ya que en la columna ***Probe*** debe aparecer el SSID correspondiente a la red.

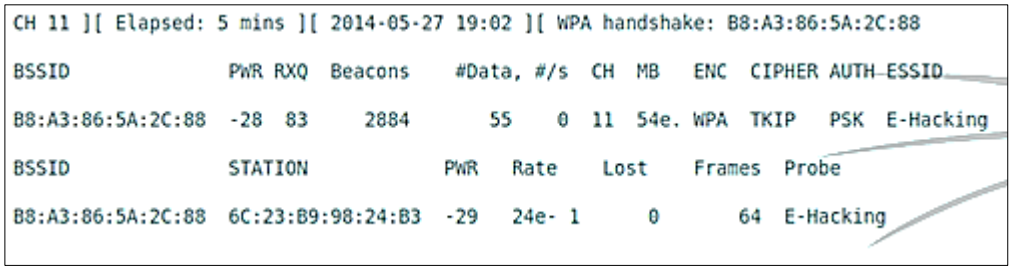


Figura 4.30 - Asociación del cliente y el punto de acceso

En forma predeterminada el sistema operativo Backtrack contiene pre-cargado un diccionario llamado darkcode.lst, en la figura 4.31 podemos observar la ruta predeterminada de este diccionario. Cabe recalcar que se pueden utilizar un sin número de diccionarios que pueden llegar a pesar más de 20 GB en texto.

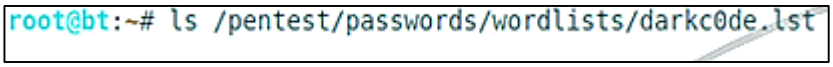


Figura 4.31 - Dirección del diccionario

Finalizado el proceso de autenticación, cliente – Punto de Acceso se crean varios archivos los cuales se usaron para

descifrar la clave WPA/WPA2 mediante el uso de diccionario. Estos archivos se pueden observar en la figura 4.32.

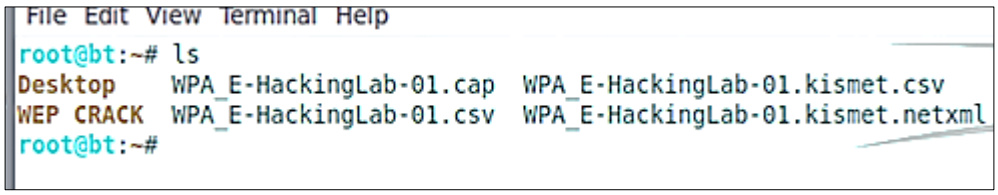


Figura 4.32 - Archivos creados

En conjunto con el comando ***<aircrack-ng>,*** se añade la ruta del diccionario de la siguiente manera:

```
root@bt:~# aircrack-ng WPA_E-HackingLab-01.cap -w /pentest/passwords/wordlists/darkc0de.lst
```

En la figura 4.33 se pude observar el proceso de comprobación de clave El tiempo que tome este proceso depende de los siguientes factores:

- Complejidad de contraseña: combinación de números, letras, minúsculas, mayúsculas y cualquier otro caracter que haga más compleja la contraseña.
- El diccionario es leído línea por línea en orden, buscando coincidencia de la palabra, en su contenido y la clave. Entre mayor sea el tamaño del diccionario

mayor será el tiempo de búsqueda, pero también será se tendrá más posibilidades de éxito.

- Si se trabaja en un equipo con poca capacidad de memoria y/o procesador el tiempo de procesamiento tardará más.

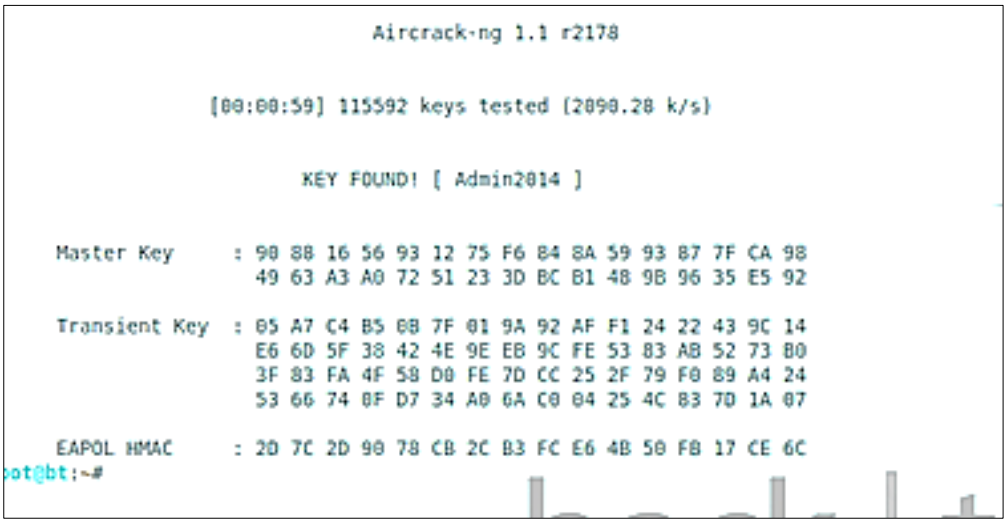


Figura 4.33 - Proceso de comprobación de clave

Ataque Jhon The Ripper

John the Ripper es un software para descifrar claves de manera muy rápida, identificando la debilidad de una clave. Es capaz de analizar o entender diversos algoritmos tales como:

- DES, MD5, blowfish
- Kerberos, AFS

- Hash LM (Lan Manager), sistema usado en Windows NT/2000/XP/2003

Es posible mediante módulos adicionales el software pueda trabajar con MD4, LDAP, MySQL.

Como en las pruebas anteriores, la interfaz inalámbrica debe ser iniciada en modo monitor para que sea capaz de capturar e inyectar tráfico en la red como se muestra en la figura 4.34.

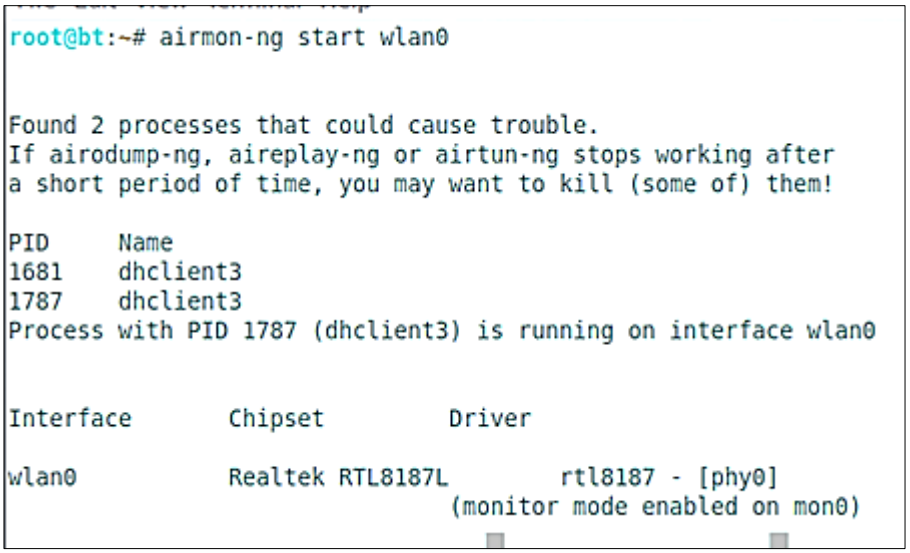


Figura 4.34 - Interfaz modo monitor

En la figura 4.35 se muestra la salida del comando ***<airodum-ng mon0>*** donde se visualizan todas las redes inalámbricas y los clientes asociados.

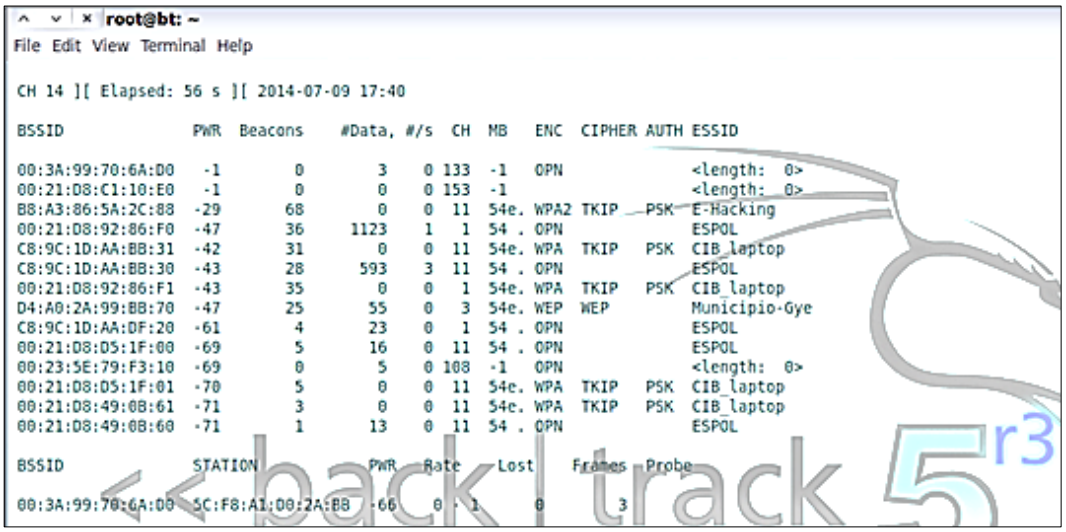


Figura 4.35 - Información de redes disponibles

Se toma la dirección MAC del punto de acceso del cual se empezó a monitorear como se muestra en la figura 4.36. La información visualizada consta del nombre de la red, el tipo de cifrado y la potencia de señal, datos que son fundamentales para proceder o realizar el ataque.

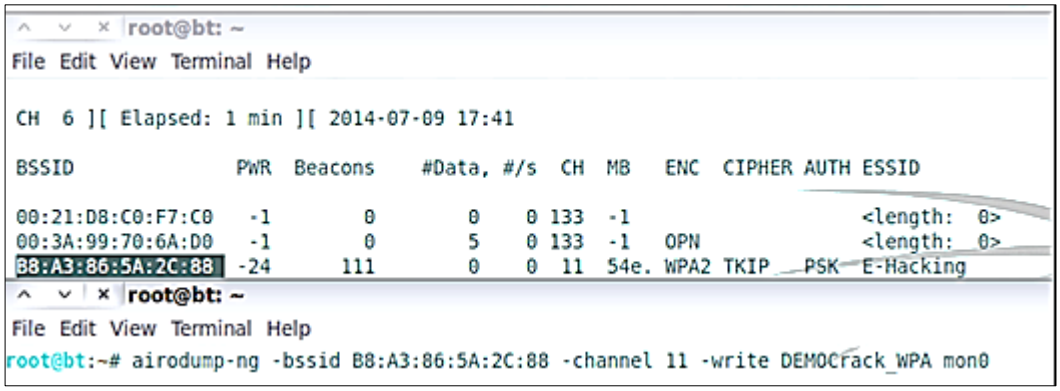


Figura 4.36 - Proceso de obtención de información de la red inalámbrica

La asociación del punto de acceso y el cliente se puede comprobar verificando el campo “Probe”. Si aparece el SSID, la asociación ha tenido éxito. Podemos observar que esto es lo que sucede en la figura 4.37.

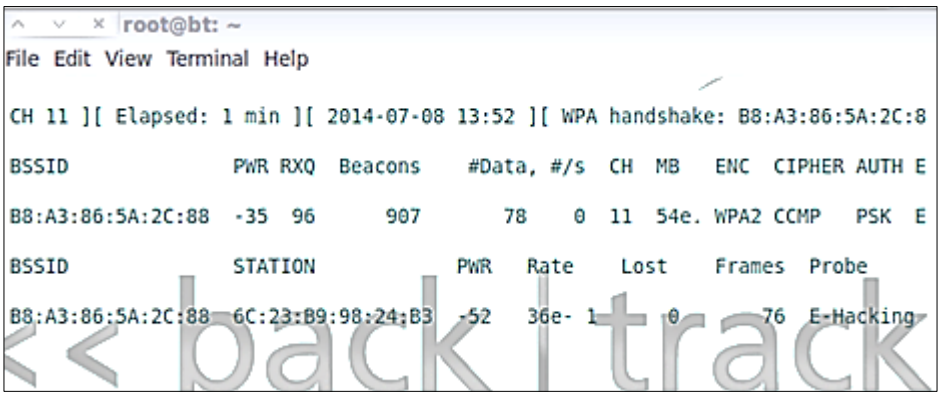


Figura 4.37 - Asociación del cliente con el punto de acceso

Para determinar si se ha capturado la información necesaria se ejecuta el comando ***<aircrack-ng>*** <Nombre del archivo creado> como se muestra en la figura 4.38, en donde podemos observar información como:

- BSSID: dirección MAC del punto de acceso
- ESSID: nombre de la red,
- Encryption o cifrado: muestra el tipo de cifrado
- Adicionalmente muestra que se ha realzado la negociación con éxito (handshake).

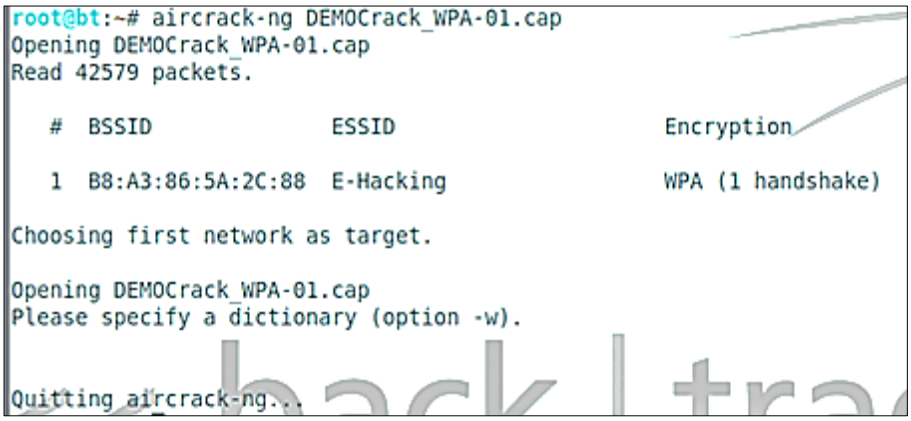


Figura 4.38 - Visualización del archivo capturado con el Handshake

En la figura 4.39 se detalla la ruta predeterminada de John the Ripper que viene ya cargado en el sistema operativo Backtrack. Para descifrar claves se puede usar los archivos predeterminados de John the Ripper:

- All.char: todos los caracteres serán usados
- Alpha.chr: caracteres alfanuméricos
- Alnum: combinación de números
- Password.lst: contraseñas más comunes

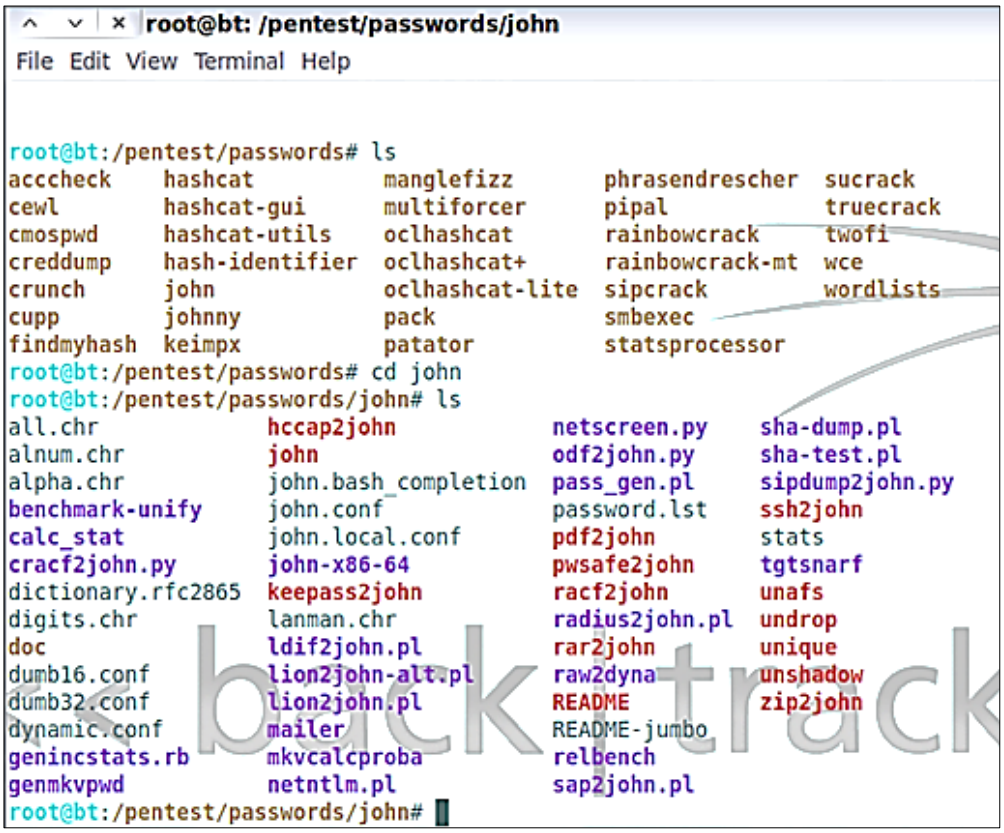


Figura 4.39 - Localización de John the Ripper

En la figura 4.40 se muestra el proceso que ejecuta John the Ripper para la verificación de claves. Ejecutando el siguiente comando se procesó el archivo con todos los caracteres y posibles combinaciones, este proceso se ejecutará hasta que se muestre un mensaje indicando que se ha encontrado la contraseña:

. /John –incremental=all.chr –stdout | aircrack-ng –w /root/DEMOCrack_WPA-01.cap –e E-Hacking

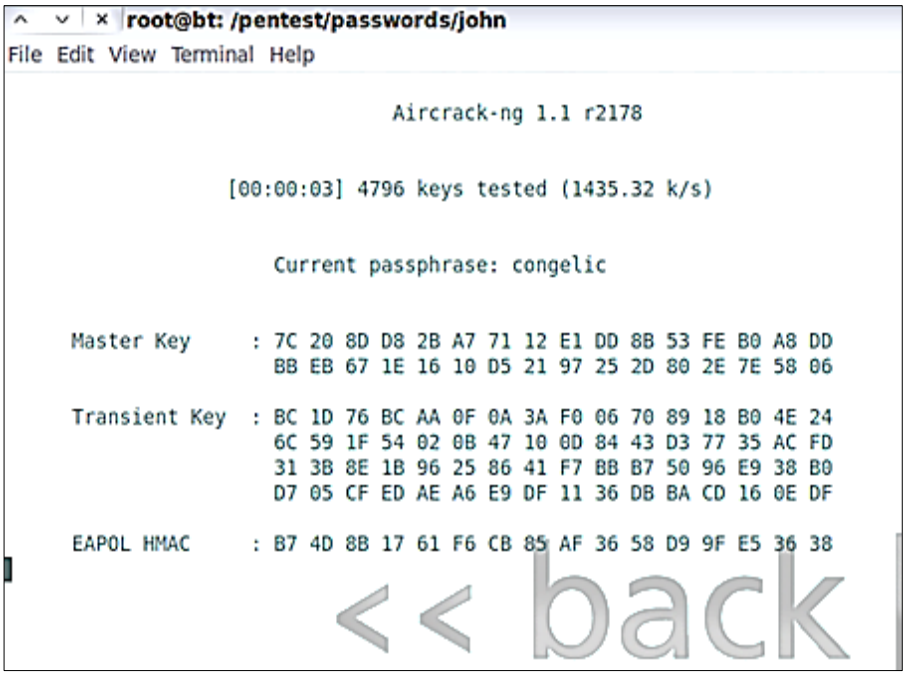


Figura 4.40 - Proceso de verificación de claves con John the Ripper

La capacidad de procesamiento debe ser lo suficientemente alta para que el proceso de descifrado sea lo más rápido posible. En la figura 4.41 se puede observar que el consumo del procesador llega a un 100% de su capacidad, sin embargo la memoria no sufre una sobrecarga como el procesador.

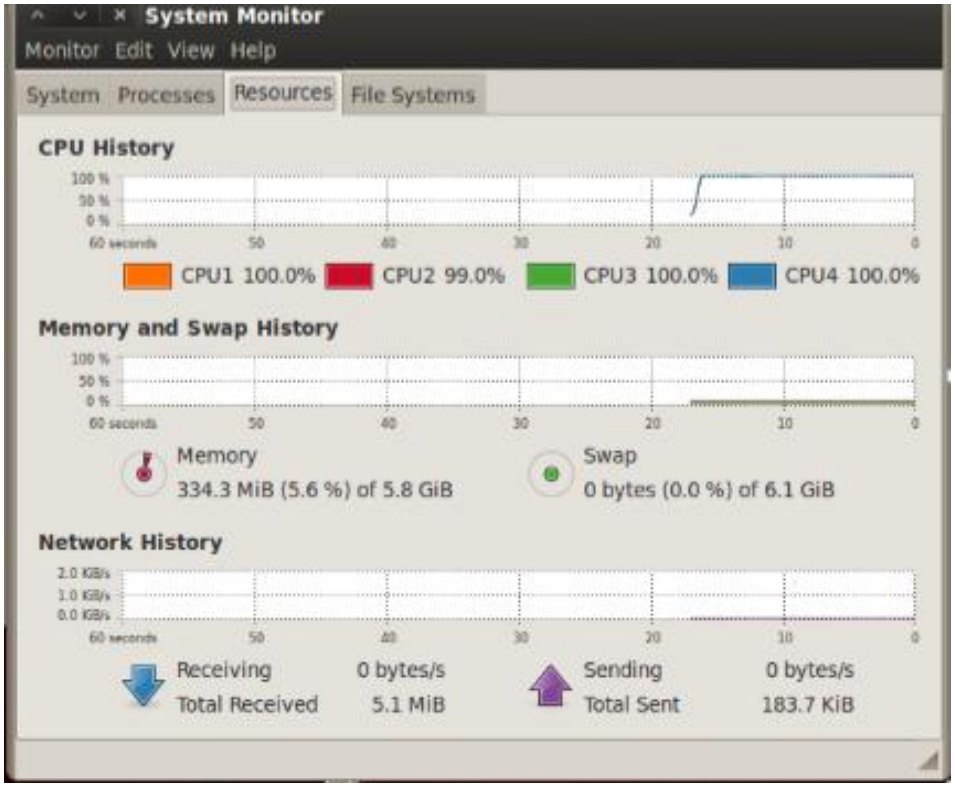


Figura 4.41 - Monitoreo del uso del procesador

Finalizado el proceso, se mostró una ventana similar a la que se generó con ***<aircrack-ng>***. El resultado de la comprobación se puede observar en la figura 4.42.

La información mostrada será: la clave descifrada, la cantidad de claves comprobadas y el tiempo que tomo todo el proceso lo cual dependerá de los factores antes mencionados.

Con las pruebas realizadas tanto, con aircrack como John the Ripper se demuestra que es posible obtener claves

WPA/WPA2, pero todo dependerá si el escenario y las herramientas son las adecuadas para realizar esta tarea.

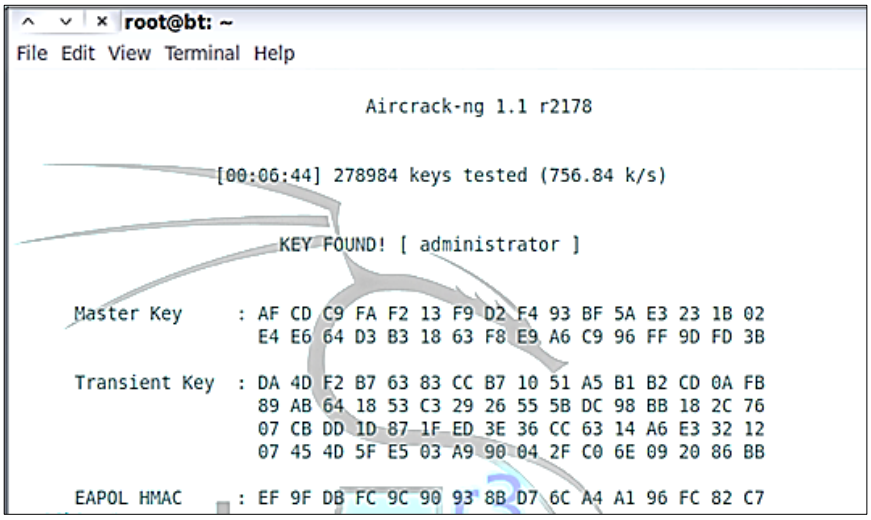


Figura 4.42 - Finalización de comprobación de claves

4.4.3. RADIUS: PAP

Los administradores de sistemas para asegurar la red inalámbrica en ambientes empresariales usan servidores de autenticación como RADIUS, en conjunto con Active Directory, pero si se deja mal configurado el servidor RADIUS este podría representar un gran riesgo para toda la infraestructura empresarial. La figura 4.43 muestra un ejemplo de una red empresarial.

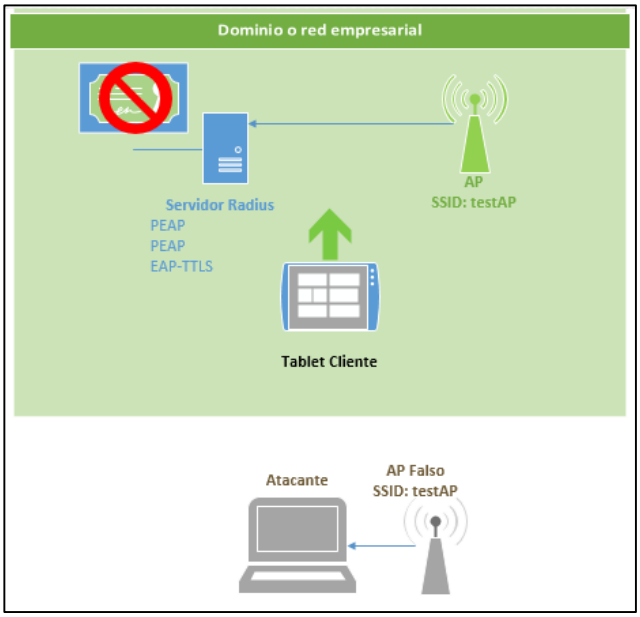
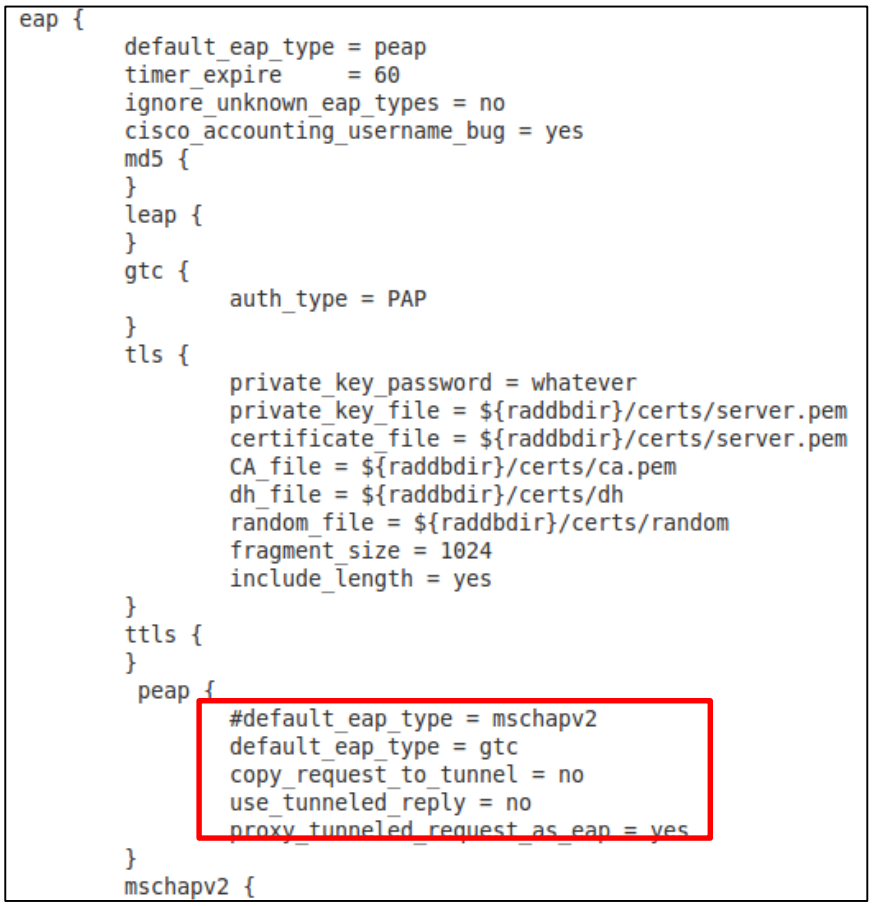


Figura 4.43 - Diagrama de red: autenticación RADIUS PAP

En esta sección se demuestra cómo es posible obtener las credenciales de acceso en el proceso de autenticación con un servidor RADIUS con una configuración poco segura, es decir sin verificar el certificado digital o que no posea conexión a una entidad certificadora. Para estas pruebas se utiliza el FreeRadius que en forma predeterminada se encuentra en la distribución Linux Backtrack.

Existe un archivo en el cual se puede cambiar el método de autenticación para que obligue al cliente utilizar EAP-GTC, un método de autenticación que no cifra la información y la envía

por el medio en texto plano. En la figura 4.44 se puede observar este archivo de configuración.



```
eap {
        default_eap_type = peap
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = yes
        md5 {
        }
        leap {
        }
        gtc {
                auth_type = PAP
        }
        tls {
                private_key_password = whatever
                private_key_file = ${raddbdir}/certs/server.pem
                certificate_file = ${raddbdir}/certs/server.pem
                CA_file = ${raddbdir}/certs/ca.pem
                dh_file = ${raddbdir}/certs/dh
                random_file = ${raddbdir}/certs/random
                fragment_size = 1024
                include_length = yes
        }
        ttls {
        }
         peap {
                #default_eap_type = mschapv2
                default_eap_type = gtc
                copy_request_to_tunnel = no
                use_tunneled_reply = no
                proxy_tunneled_request_as_eap = yes
        }
        mschapv2 {
```

Figura 4.44 - Configuración de archivo: autenticaciones RADIUS

Al ejecutar los procesos del RADIUS para la captura de las credenciales del cliente, estas se envían hacia el punto de acceso en texto plano. En la figura 4.45 se muestra el proceso mencionado.

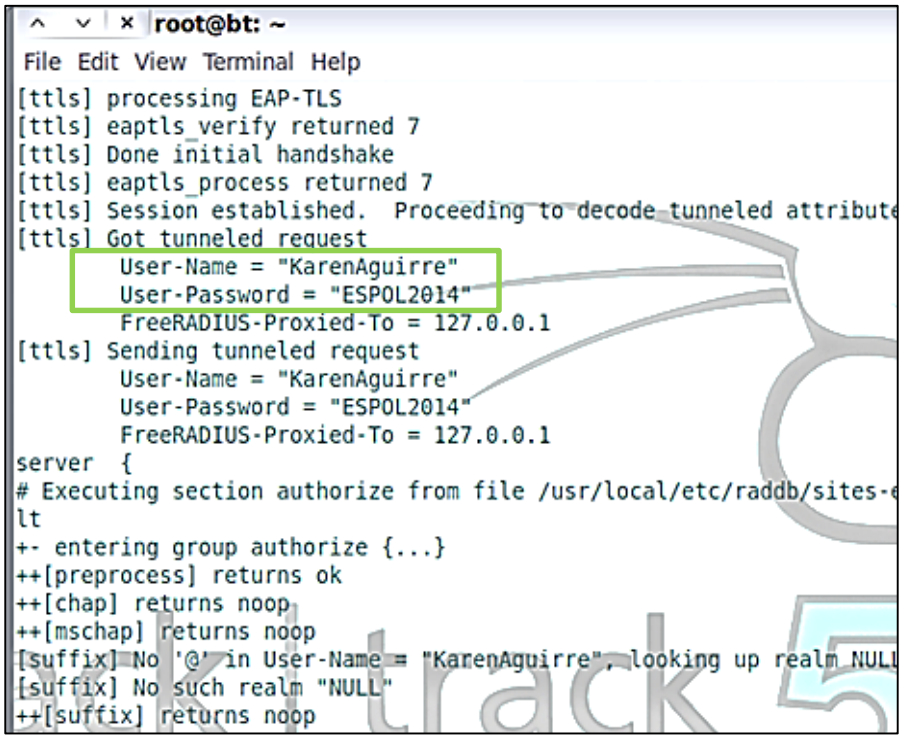


Figura 4.45 - Obtención de credenciales en texto plano

4.4.4. RADIUS: PEAP

PEAP utiliza certificados del lado del servidor para la validación del servidor RADIUS. Casi todos los ataques contra PEAP aprovechan errores de configuración en la validación de certificados [13].

Para configurar un servidor RADIUS falso es necesario conectar un ruteador inalámbrico y asignar una dirección IP dinámica por medio del comando ***<dhclient>*** a la interfaz

conectada, la cual será usada por el servidor. En la figura 4.46 se puede observar el proceso de obtención de una dirección IP.

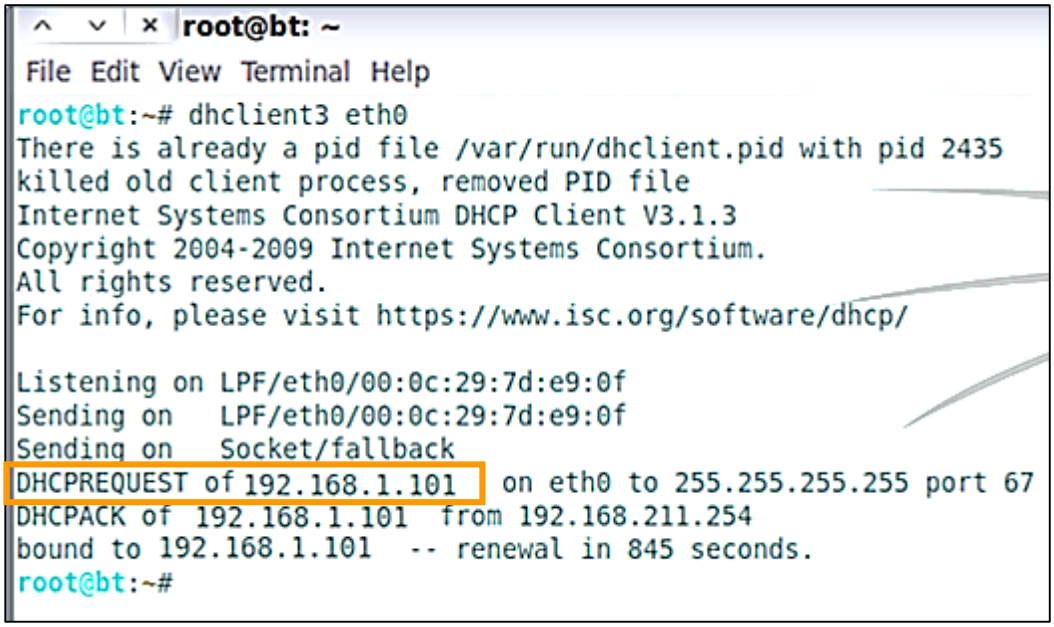


Figura 4.46 - Proceso de obtención de dirección IP mediante DHCP

Una vez obtenida la dirección IP por dhcp se configura el punto de acceso con la misma dirección IP. La figura 4.47 muestra la configuración del ruteador para que apunte a esta IP como servidor RADIUS.

Figura 4.47 - Configuración de un ruteador como servidor RADIUS

Para comprobar que la dirección IP este asignada a una interfaz de red se utiliza el comando ***<ifconfig>*** el cual permite visualizar información de la interfaz configurada. La salida de este comando se visualiza en la figura 4.48.

```
root@bt:~# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0c:29:46:2d:b3
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe46:2db3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:542 errors:0 dropped:0 overruns:0 frame:0
          TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:49819 (49.8 KB)  TX bytes:7034 (7.0 KB)
          Interrupt:19 Base address:0x2000
```

Figura 4.48 - Verificación de la interfaz de red

En la ruta mostrada en la figura 4.49 se encuentran todos los archivos necesarios para la configuración del servidor FreeRadius

```
root@bt:/usr/local/etc/raddb# ls
acct_users                clients.conf       ldap.attrmap    sites-available
attrs                     dictionary         modules         sites-enabled
attrs.access_challenge    eap.conf           policy.conf     sql
attrs.access_reject       example.pl         policy.txt      sql.conf
attrs.accounting_response experimental.conf preproxy_users  sqlippool.conf
attrs.pre-proxy           hints              proxy.conf      templates.conf
certs                     huntgroups         radiusd.conf    users
root@bt:/usr/local/etc/raddb#
```

Figura 4.49 - Archivos de configuración

Unos de los archivos a configurar es el ***eap.conf*** que contiene los métodos de autenticación de Radius para el cliente. En este caso se verifica que se esté usando el método PEAP que viene configurado de manera predeterminada en el FreeRadius como podemos observar en la figura 4.50.

```
    eap {
            default_eap_type = peap
            timer_expire     60
            ignore_unknown_eap_types = no
            cisco_accounting_username_bug = yes
            md5 {
            }
            leap {
            }
            gtc {
                    auth_type = PAP
            }
            tls {
                    private_key_password = whatever
                    private_key_file = ${raddbdir}/certs/server.pem
                    certificate_file = ${raddbdir}/certs/server.pem
                    CA_file = ${raddbdir}/certs/ca.pem
                    dh_file = ${raddbdir}/certs/dh
                    random_file = ${raddbdir}/certs/random
                    fragment_size = 1024
                    include_length = yes
```

Figura 4.50 - Configuración del archivo EAP.conf: autenticación RADIUS

El archivo ***client.conf*** muestra la lista de clientes (segmentos de red) que pueden conectarse al servidor RADIUS. La configuración de este archivo la podemos observar en la figura 4.51.

```
#per_socket_clients {
#       client 192.168.3.4 {
#               secret = testing123
#        }
#}

client 192.168.0.0/16 {
       secret          = hack
       shortname       = testAP
}
client 172.16.0.0/12 {
       secret          = test
       shortname       = testAP
}
client 10.0.0.0/8 {
       secret          = test
       shortname       = testAP
}
#client 127.0.0.1 {
#       secret          = test
#       shortname       = testAP
#}
```

Figura 4.51 - Configuración del archivo client.conf: segmentos de red

Antes de ejecutar el servicio de autenticación de RADIUS se debe crear el archivo de registro para poder almacenar la información o negociación entre el cliente y el punto de acceso, o esperar a que se realice una conexión para que el

archivo de registro se cree automáticamente. El comando para la creación de este archivo se muestra en la figura 4.52.

Figura 4.52 - Creación del archivo de registro

En la figura 4.53 podemos observar cómo se inicia el servidor RADIUS una vez configurados los archivos. Si todo se encuentra bien configurado mostrara el estado "Listo para procesar requerimientos".

Figura 4.53 - Inicio del Servidor RADIUS

Cuando se esté ejecutando el servidor RADIUS, se realiza un seguimiento del archivo de registro, el cual contiene información de la conexión entre ambos puntos, (cliente y servidor). En la figura 4.54 se observa que entre esa información podemos encontrar el usuario, el desafío y la respuesta.

Figura 4.54 - Captura de credenciales mediante archivo de registro

Al ejecutar el comando ***asleep*** con los datos adquiridos, se usó el diccionario por defecto pre-cargado en el sistema. El proceso demora según la complejidad de la clave y si esta encuentra coincidencia en el diccionario. Es posible usar diversos diccionarios en diferentes idiomas o diccionarios que contengan las claves más usadas. En la figura 4.55 se muestra un ejemplo del uso del asleep y el resultado que se obtiene.

Figura 4.55 - Proceso de obtención de clave

4.4.5. RADIUS: EAP-TTLS

En EAP-TTLS (EAP-Túnel Transport Layer Security), el servidor se autentica con un certificado. El cliente que desee puede usar el certificado también. Desafortunadamente, esto no tiene soporte nativo en versiones anteriores a Windows 8 por lo cual es necesario el uso utilidades de terceros.

Existen múltiples opciones de protocolo de autenticación que se pueden utilizar con EAP-TTLS. El más común es nuevo MSCHAP-v2. [13].

En el archivo eap.conf solo se realiza el cambio del tipo protocolo de autenticación. La figura 4.56 muestra el archivo eap.conf modificado para usar EAP-GTC.

```
eap {
        default_eap_type = peap
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = yes
        md5 {
        }
        leap {
        }
        gtc {
                auth_type = pap
        }
        tls {
                private_key_password = whatever
                private_key_file = ${raddbdir}/certs/server.pem
                certificate_file = ${raddbdir}/certs/server.pem
                CA_file = ${raddbdir}/certs/ca.pem
                dh_file = ${raddbdir}/certs/dh
                random_file = ${raddbdir}/certs/random
                fragment_size = 1024
                include_length = yes
        }
        ttls {
        }
         peap {
                default_eap_type = mschapv2
                #default_eap_type = gtc
                copy_request_to_tunnel = no
                use_tunneled_reply = no
                proxy_tunneled_request_as_eap = yes
        }
        mschapv2 {
        }
}
```

Figura 4.56 - Modificación del archivo eap.conf

Como en versiones anteriores a Windows 8 no tiene la posibilidad de usar TTLS con MSCHAPv2 se puede comprobar la configuración en dispositivos Apple o con un software suplicante para la autenticación. En la figura 4.57 se muestra la configuración de Windows para usar un software suplicante.

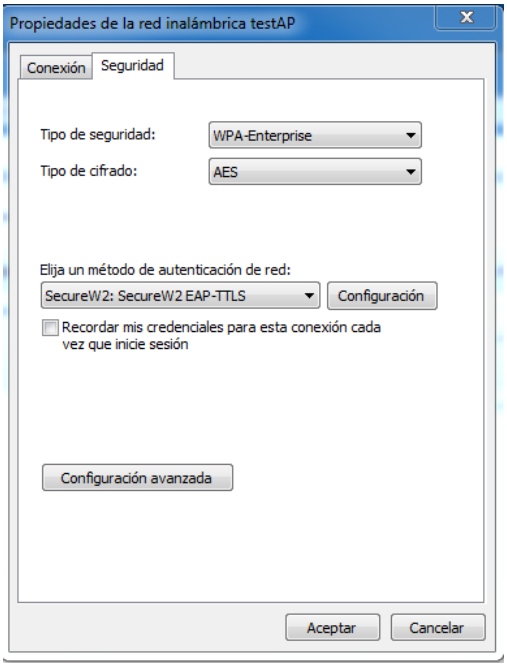


Figura 4.57 - Propiedades de red: configuración en cliente

En este caso se usara para la demostración el software llamado Secure W2, el cual permite usar varios protocolos de autenticación en este caso el MSCHAPv2. Una vez configurado el cliente está habilitado para poder conectarse al punto de acceso e ingresar sus credenciales. En la figura 4.58 se muestra el SecureW2 configurado para MSCHAPv2.

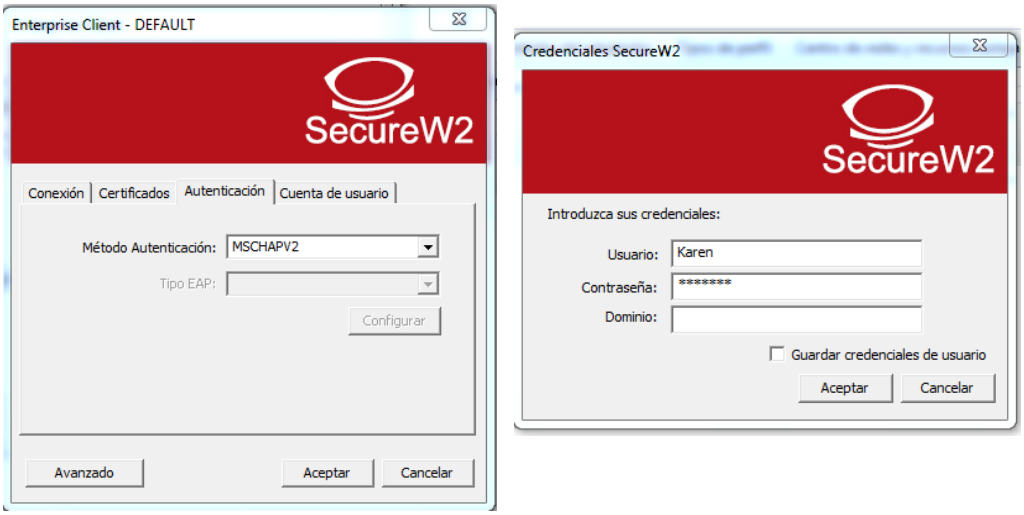


Figura 4.58 - Software suplicante de autenticación: configurado para MSCHAPv2

El atacante puede duplicar el nombre del punto de acceso, haciendo que el cliente no note la diferencia entre los nombres de las redes. Muchos usuarios suelen conectarse a la primera red disponible haciendo que sus credenciales sean fácilmente robadas. Estas credenciales pueden ser también para la autenticación en Active Directory lo cual hace más peligroso que el usuario y la contraseña sean tomados por algún atacante en la red. La figura 4.59 muestra un escenario de red atacado mediante un AP falso.

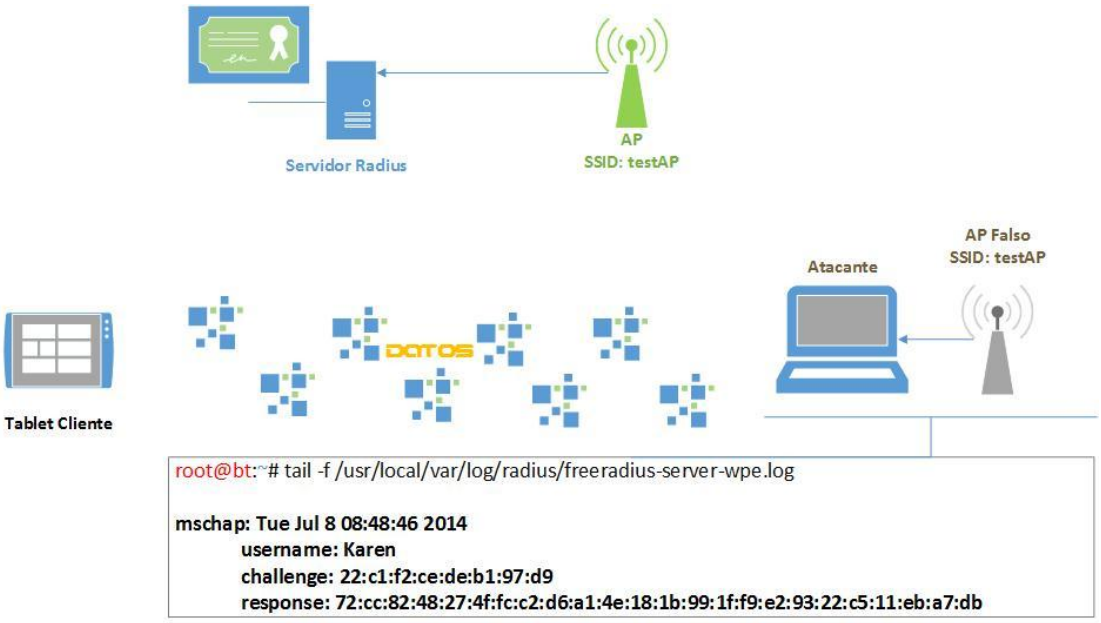


Figura 4.59 - Diagrama de red: obtención de credenciales

Al igual que en el proceso de obtención de clave en PEAP, el procedimiento se repite, se hace el uso del comando asleep seguido de las credenciales obtenidas que se encuentran cifradas. Al finalizar el proceso se muestra la contraseña del usuario correspondiente como se muestra en la figura 4.60.

Figura 4.60 - Proceso de obtención de clave MSCHAPv2

4.5. RESULTADOS DEL TEST DE PENETRACIÓN

Se comenzó probando los sistemas que actualmente se consideran menos seguros como el SSID oculto y el filtrado MAC. En ambos casos el proceso consiste en observar los paquetes que se transmiten entre un cliente legítimo y el punto de acceso. En este procedimiento se pudo observar que la información requerida (SSID y dirección MAC) se mostraba en texto plano por lo que no se requiere ningún procesamiento adicional, esto le da un 100% de probabilidades de éxito al ataque. Sin embargo, uno de los inconvenientes que se pudo detectar es que para capturar ésta información es necesario que al menos un cliente legítimo esté conectado a la red.

Para comprobar la seguridad de WEP se realizaron varias pruebas en donde se usaron algunas contraseñas de diferentes longitudes y complejidad como “diego”, “qwertyuiopasd”, “municipio2011” y “k5l4d7hal44gw”. En todos los casos se obtuvo con éxito la contraseña en diferentes tiempos que van desde los 2 hasta los 5 minutos. La complejidad de la contraseña no afecto la velocidad de obtención de la contraseña, sin embargo se pudo observar que cuando la calidad de la señal no era optima se producía perdida de paquetes lo que si generó un aumento en el tiempo que tardó la herramienta obtener la contraseña.

Las pruebas con WPA/WPA2 fueron realizadas mediante ataques de diccionario, que es el único tipo de ataque posible contra WPA/WPA2 en la actualidad. Se probaron contraseñas sencillas como “qwerty”, “12345678”, “administrator” y contraseñas que se sabía que estaban dentro del diccionario como “Admin2014”. En estas pruebas se pudo obtener las contraseñas en tiempos diferentes desde 1 hasta 15 minutos. Al comprobar otras contraseñas no comunes o más complejas como “k5l4d7ha” no fue posible obtener la contraseña luego de recorrer todo el diccionario, proceso que tardó 4 horas con 18 minutos. Un dato importante que se pudo observar es la velocidad de comprobación de claves que llevo a ser de 1920 clave por segundo.

En el caso de las autenticaciones basadas en RADIUS el ataque va dirigido a los clientes por medio de puntos de acceso falso. Se hizo pruebas con varias configuraciones de seguridad diferentes en la conexión inalámbrica de los clientes. Cuando la opción de verificar el certificado del servidor estuvo deshabilitada, el cliente se conectó al punto de acceso falso sin problemas permitiendo capturar el hash enviado por el cliente que luego pudo ser usado para realizar ataques de diccionario sobre él. Cuando la opción de verificar el certificado de servidor estuvo habilitada, pero no se especificó la entidad de certificación de confianza, el usuario al intentar conectarse

era advertido con un mensaje, sin embargo al aceptar pudo conectarse permitiendo capturar el hash. Un usuario sin conocimientos podría conectarse a esta red sin percatarse del problema se seguridad. Cuando la opción de verificar el certificado de servidor estuvo habilitada y se especificó la entidad de certificación de confianza, el cliente rechazo la conexión y no le permitió al usuario conectarse por lo que el hash no pudo ser capturado.

4.6. ANÁLISIS DEL TEST DE PENETRACIÓN

En un test de penetración podemos identificar las vulnerabilidades existentes en una infraestructura de red implementada o que será implementada, como se ha podido apreciar en las pruebas realizadas a la infraestructura de red inalámbrica, con diferentes métodos de seguridades convencionales no ha sido posible proteger el acceso a la red, todos los métodos vistos han sido vulnerados con ataques de diccionario y algunas variantes.

Backtrack con múltiples herramientas y en conjunto de hardware especializado ha permitido no solo romper la seguridad de una red inalámbrica sino también ha permitido obtener las credenciales de los usuarios, en un tiempo relativamente corto.

El tiempo que toma en tener acceso a la red dependerá de factores tales como:

- Tipo de seguridad implementada; Filtrado MAC, ocultar el SSID.
- Tipo de cifrado utilizado; WEP/WPA/WPA2, en el caso de WPA/WPA2 dependerá de que tan compleja sea la contraseña y como este formada, sea numérica, alfanumérica o con caracteres especiales.

Si una clave WPA/WPA2 es un poco compleja el tiempo de obtención de clave es largo, y es necesario tener las herramientas necesarias para realizar el proceso es necesario utilizar diccionarios no convencionales, en varios idiomas, con varias combinaciones y hasta diccionarios especializados para estos trabajos los cuales pueden llegar a pesar más de 30 GB en texto.

Para procesar este tipo de archivos es necesario tener equipos de mayores capacidades, ya que el nivel de requerimiento es alto, se necesita un CPU que sea capaz de soportar la carga de procesamiento, pero actualmente hay métodos que ayudan a agilizar el trabajo tal como el uso de la GPU de un equipo, es decir la tarjeta gráfica.

Con respecto a las autenticaciones mediante RADIUS PAP/PEAP/EAP-TTLS, también han sido vulnerados debido a su mala configuración. Existen administradores de redes que implementan RADIUS pero este no es bien configurado, lo cual es peligroso y aprovechado por los hackers.

Si no existe una entidad certificadora que autentique la identidad del cliente con el Punto de acceso, este método es fácilmente intersectado ya que no se usa ningún certificado, y cualquier cliente se conecta a la red.

El sistema usado en las pruebas realizadas ha sido el Linux Backtrack 5 r3, que siendo software libre posee variedad de herramientas para realizar un test de penetración a nivel de infraestructura de red, pero no es el único sistema el cual tiene estas características, por mencionar algunos de los sistemas o herramientas tenemos el reciente sistema Kali Linux, whoppix, Matriux, Blackbuntu entre otros.

En ambientes domésticos, la complejidad de contraseña juega un papel muy importante al momento de implementar una red inalámbrica, y en una red empresarial es importante la implementación de seguridad más robusta que mitigue todos estos

ataques anteriormente vistos, por lo que se emplearan certificados digitales para la solución.

CAPÍTULO 5

5. SOLUCIONES PROPUESTAS

El nivel de seguridad a implementarse dependerá del ambiente en el que se encuentre la red y las necesidades propias del individuo o empresa. Podemos dividir el estudio en dos ambientes básicos, seguridad a nivel personal y seguridad a nivel empresarial.

5.1. SEGURIDAD A NIVEL PERSONAL

Dentro de un ambiente personal, de un hogar o una pequeña oficina, donde generalmente se cuenta con equipos de acceso a la red inalámbrica de bajas prestaciones, es recomendable optimizar la

seguridad al menos en lo posible dentro de las limitaciones de hardware y software que se poseen.

La configuración de seguridad óptima para estos casos es la autenticación WPA2 con el tipo de cifrado AES. En la actualidad muchos ruteadores y puntos de acceso inalámbricos ofrecen la opción WPA/WPA2 con TKIP/AES, este modelo permite la autenticación tanto WPA como WPA2 y puede ser usado por motivos de compatibilidad si se tienen equipos que no soporten WPA2. La seguridad WEP debe ser evitada ya que es la más vulnerable y se la puede atacar y obtener acceso a la red en muy poco tiempo.

Otro punto que determina el nivel de seguridad en una red inalámbrica de estas características es la complejidad de la contraseña, como medidas básicas de seguridad se debe considerar una longitud de al menos 8 caracteres, en donde no se debe emplear palabras del diccionario, ni ningún tipo de información personal como números de identificación, teléfonos o fechas de cumpleaños. En su lugar es recomendable usar una combinación de letras mayúsculas y minúsculas, números y símbolos. Esto aumenta la seguridad de la red contra ataques de diccionario o fuerza bruta.

5.2. SEGURIDAD A NIVEL EMPRESARIAL

Las empresas manejan mucha información confidencial y suelen ser el blanco de ataque con mayor frecuencia y por hackers más capacitados (incluso organizaciones de hackers) que un usuario en una red propia en su hogar. Por esto se han desarrollados métodos de seguridad más complejos que involucran servidores de seguridad y acceso, lo que hace que sean también más costosos de implementar.

5.2.1. Protocolo EAP-TLS

Este protocolo puede funcionar en conjunto con WPA/WPA2 Enterprise otorgando un nivel de seguridad que hasta la actualidad no ha podido ser vulnerado [13].

EAP-TLS está basado en el uso de certificados digitales para la autenticación tanto del cliente como el servidor de autenticación. Este es probablemente el mejor método de seguridad existente en la actualidad para el acceso a redes inalámbricas. [16] En la figura 5.1, se puede observar un ejemplo de una implementación de EAP-TLS.

Esta implementación requiere del despliegue de una arquitectura PKI, en donde al menos debe existir un servidor

de certificación para la emisión y manejo de los certificados, y un servidor de autenticación como un servidor RADIUS. Se deben distribuir certificados tanto a los servidores de autenticación como a los clientes inalámbricos.

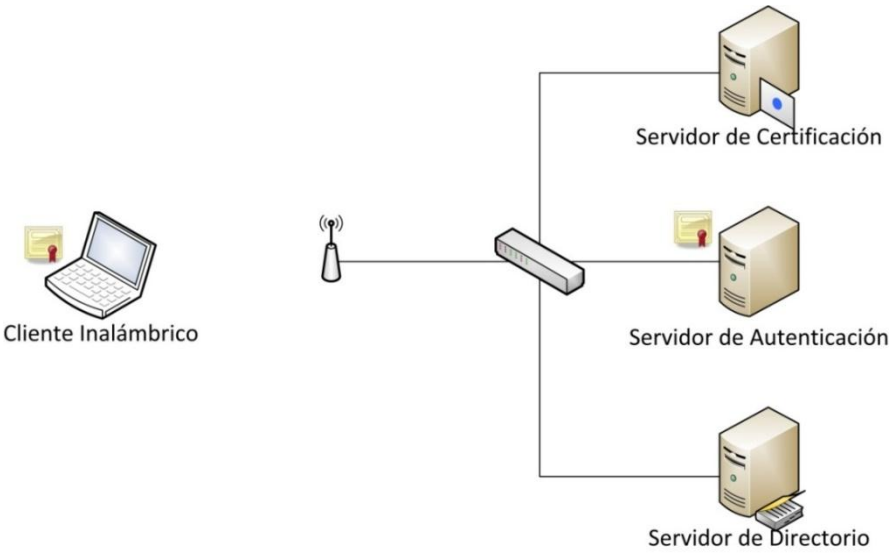


Figura 5.1 - Protocolo EAP-TLS

La mayor ventaja de este modelo de seguridad es el uso de certificados digitales en lugar de contraseñas, lo que elimina el problema de una contraseña de usuario débil o comprometido. Las desventajas de este modelo de seguridad son la dificultad de su implementación y la carga administrativa que genera la distribución de certificados a todos los clientes para su autenticación.

5.2.2. Control de Acceso a la Red (NAC)

NAC combina en una solución la autenticación de usuarios, evaluación de seguridad de punto final y control de acceso. La solución NAC asegura que cada terminal cumpla con las políticas de seguridad de la red antes de otorgarle el acceso a la misma. El propósito de NAC se divide en dos partes: permitir el acceso a la red únicamente a usuarios y sistemas autorizados, y asegurar el cumplimiento de las políticas de seguridad de la red. [17]

Los componentes fundamentales de NAC son: puntos finales (EP), puntos de cumplimientos de políticas (PEP) y punto de decisión de políticas (PDP) [18]. En la figura 5.2 se pueden observar estos elementos dentro de una solución NAC.

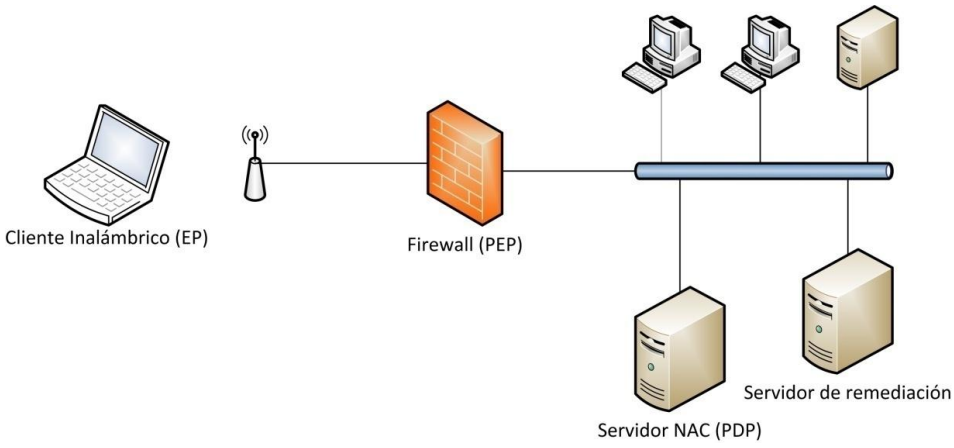


Figura 5.2 - Control de Acceso a la Red

Los ***puntos finales*** son los equipos que requieren el acceso a la red, dependiendo de la solución estos pueden o no tener un agente. Un agente es un software que se instala en los equipos que permite hacer una evaluación automática del estado del equipo (antivirus, actualizaciones del sistema, etc.) y enviar la información obtenida al servidor NAC.

El ***punto de decisión de políticas*** es el servidor principal de la solución NAC, es aquí donde se evalúa al equipo que solicita el acceso a la red basándose en la información del estado del equipo recibida del ***punto de cumplimiento de políticas***.

Otro elemento que incluyen algunas soluciones NAC son los servidores de remediación, estos ofrecen una resolución automática a los problemas de los equipos que no cumplen las políticas de acceso a la red. Cuando un equipo no cumple con las políticas es puesto en cuarentena, en este estado se les da acceso a los servidores de remediación de donde podrán obtener las correcciones necesarias para calificar como equipo saludable y poder obtener acceso a la red.

En un ambiente como una red inalámbrica, en donde existen equipos que entran y salen constantemente de la red, una solución como NAC puede proveer seguridad ante amenazas como software malicioso adquirido por los equipos cuando se encuentran fuera de la empresa. Esto es posible gracia a su capacidad de aislar equipos que no cumplen con las normas de seguridad y ofrecerles una remediación de problemas. Actualmente existen varias soluciones NAC como NAP (Network Access Protection) de Microsoft, NAC (Network Admision Control) de Cisco, y otras de código abierto como PacketFence.

5.2.3. Acceso a través de VPN

Las VPN fueron creadas para el acceso seguro a una red privada a través de una red pública o poco segura. Basados en este mismo principio se empezó a optar por usarlas en redes locales inalámbricas, cuya seguridad es un inconveniente, para conectarse a través de un canal cifrado con la red interna de la empresa. La figura 5.3 muestra un modelo de red inalámbrica con acceso a través de VPN a la red interna de la empresa.

En este modelo de seguridad la red inalámbrica está separada de la red interna de la empresa por un equipo que cumple el

rol de servidor VPN. De esta manera los usuario inalámbricos, luego de obtener acceso a la red inalámbrica, aun no pueden obtener acceso a los recursos que se encuentra dentro de la red interna de la empresa, sino hasta que establezcan una conexión VPN con la misma. Así, aun cuando la seguridad de la red inalámbrica pueda ser vulnerada el atacante no tendrá acceso a los recursos de la empresa.

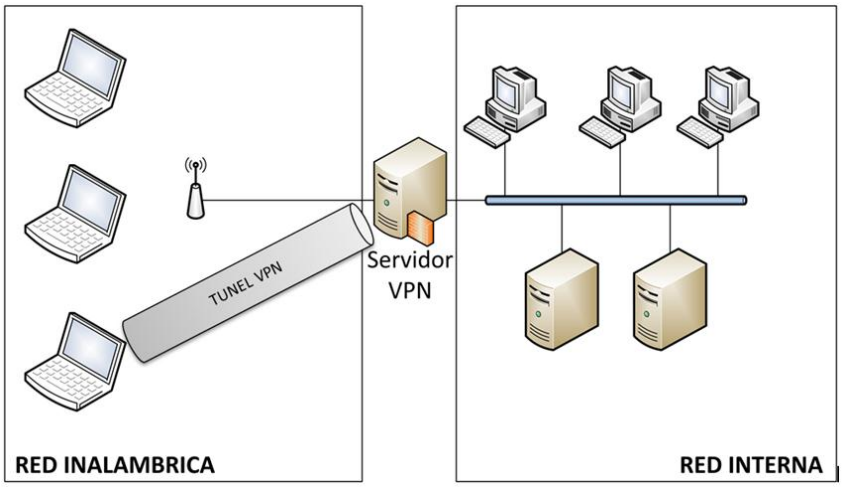


Figura 5.3 - Acceso a través de VPN

Otra ventaja al tener las redes separadas por el servidor VPN, es que se podría del mismo modo colocar un cortafuegos detrás de él, lo que permitiría el control de los recursos a los que el usuario puede acceder desde la red inalámbrica.

5.2.4. Comparación de las soluciones empresariales

Cada una de las soluciones descritas tiene diferentes características y capacidades que debemos analizar para determinar cuál es la que mejor se adapta a nuestra red y necesidades de seguridad. A continuación se analizarán los beneficios que ofrece cada una.

En el caso de EAP-TLS se ofrece un esquema de seguridad en donde su principal fortaleza es el uso de certificados digitales, que brindan un nivel de seguridad muy superior a las contraseñas. Otra ventaja es la autenticación tanto del cliente como el servidor que permite también a los clientes identificar al servidor al que se están conectando, evitando así ataques orientados a clientes en donde se crean puntos de acceso falsos.

NAC está enfocado no solo a la autenticación de los usuarios, sino a resolver un problema especialmente importante en los equipos portátiles, el ingreso de software malicioso de fuentes externas a la empresa. Al no tener el control administrativo de estos equipos, la evaluación de cumplimiento de políticas previo a otorgar el acceso a la red ayuda en gran medida a mitigar la propagación de infecciones a través de la red.

El acceso a través de VPN permite dar cierto nivel de acceso, como conexión a internet, a usuarios dentro de la red inalámbrica que son considerados como invitados, mientras que para obtener acceso a recursos dentro de la red interna se requerirá una conexión a través de VPN. La inclusión de un cortafuegos en este modelo de seguridad, permite un control de los recursos a los que pueden acceder los usuarios luego de conectarse a la red. De esta manera, se puede limitar el acceso de los usuarios a ciertos segmentos o servicios dentro de la red.

La selección de uno de estos modelos de seguridad dependerá de varios factores específicos del ambiente donde se implementará como el tipo de usuarios y sistemas que accederán a la red, las políticas de seguridad de la empresa, la infraestructura de red actual y el impacto que podría causar en la red su implementación, por lo que antes de optar por una de estas soluciones se deberá hacer un estudio y analizar cuidadosamente estos factores.

CAPÍTULO 6

6. IMPLEMENTACIÓN DE SEGURIDAD INALÁMBRICA A TRAVÉS DE UNA VPN

Se implementó un modelo de seguridad en donde se combinaron los beneficios del acceso a través de VPN y los certificados digitales para maximizar la seguridad en el acceso a la red inalámbrica. El uso de un servidor VPN que además funcione como cortafuegos para el acceso de los clientes inalámbricos a la red de la empresa permite, no solo el control de los usuarios que puedan acceder a la red sino, los recursos específicos a los que pueden acceder dentro de la red interna de la empresa. Por otra parte, el uso certificados digitales como método de

autenticación de los usuarios, proporciona un método más seguro al no depender de la complejidad de la contraseña elegida por los usuarios, ni la confidencialidad con que mantengan esa contraseña.

6.1. DISEÑO GENERAL

Se contó con un servidor VPN/Cortafuegos que fue implementado por medio del Forefront Threat Management Gateway 2010, este permitió crear un túnel seguro para el acceso a la red interna. Para la autenticación de los usuarios este servidor se contactó con un servidor RADIUS, implementado usando el servicio de Network Policy and Access Services de Windows Server 2008 R2. El servidor RADIUS usó como método de autenticación el EAP-TLS y se contactó con un servicio de directorio Active Directory de donde obtuvo el grupo de usuarios que tiene permitido el acceso. Para la emisión y manejo de certificados digitales se implementó un servidor de certificación. Adicionalmente, se instaló un servidor interno que cumplió el rol de servidor web, este representó los recursos internos de la empresa. La figura 6.1 muestra el diseño general donde se puede observar los servidores y su ubicación dentro de los segmentos de red interna y red inalámbrica.

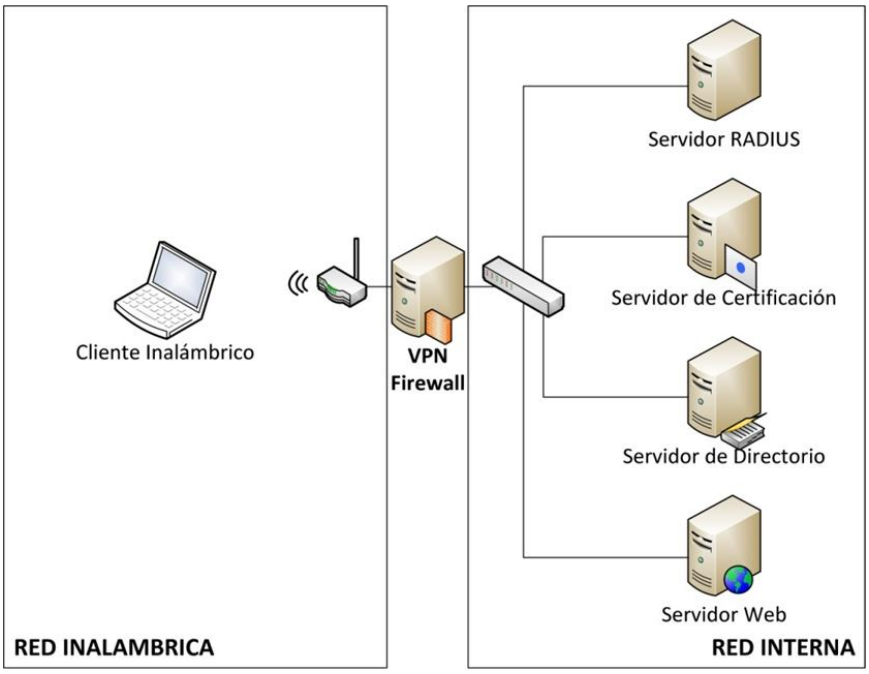


Figura 6.1 - Diseño General

6.2. DESCRIPCIÓN DEL ESCENARIO DE SIMULACIÓN

Empezaremos describiendo los elementos de hardware y software que se usaron para la simulación por medio de máquinas virtuales. A continuación se detalla el hardware con sus características:

- **TP-Link WR543G:** Es ruteador inalámbrico que soporta los estándares inalámbricos IEEE 802.11g y IEEE 802.11b, además cuenta con 4 puertos LAN de 10/100Mbps. Cuenta con una antena desmontable omnidireccional de 5dBi y trabaja en un rango de frecuencias de 2.4 a 2.4835GHz. Soporta los protocolos de seguridad inalámbrica WEP, WPA, WPA2, WPA-PSK y WPA2-PSK.

- **Acer Aspire One D-150:** Es una computadora portátil de bajo rendimiento. Cuenta con un procesador Intel ATOM N280, el cual trabaja a 1.66 GHz, y 2GB de memoria RAM DDR2. Tiene 2 interfaces de red: una interfaz inalámbrica que soporta los estándares inalámbricos IEEE 802.11b y IEEE 802.11 g, y otra cableada que trabaja a 10/100Mbps. Tiene instalado el sistema operativo Windows 8 PRO.
- **Toshiba Satelite M-645:** Es una computadora portátil de gama media. Cuenta con un procesador Intel Core i3, el cual trabaja a 2.8 GHz, y 3GB de memoria RAM DDR3. Tiene 2 interfaces de red: una interfaz inalámbrica que soporta los estándares inalámbricos IEEE 802.11b y IEEE 802.11 g, y otra cableada que trabaja a 10/100Mbps. Tiene instalado el sistema operativo Windows 7 Professional.

El software seleccionado para la implementación de la solución está formado por un conjunto de servidores Microsoft. Para la creación y administración de las máquinas virtuales se usó el software de virtualización de código abierto VirtualBox. A continuación se detallan las versiones de software que se usaron:

- Windows Server 2008 R2, dentro del cual se instalaron los servicios: Active Directory Domain Services, Active

Directory Cetificate Services, Network Policy and Access Services y Internet Information Services.

- Forefront Threat Management Gateway 2010
- Oracle VirtualBox 4.3.6

En resumen, el hardware constó de dos portátiles y un ruteador inalámbrico. Estos equipos con la ayuda del software de virtualización permitieron recrear los elementos principales de un escenario de red empresarial.

La figura 6.2 muestra los equipos usados para la simulación y su funcionalidad dentro del escenario. Los equipos físicos cumplirán los roles detallados a continuación:

- El ruteador inalámbrico fue usado como equipo de acceso a la red inalámbrica.
- La portátil de menor capacidad (Acer Aspire One D-150) fue usada como cliente inalámbrico.
- La otra portátil (Toshiba Satelite M-645) ejecutó varias máquinas virtuales que incluyeron los servidores de la red.

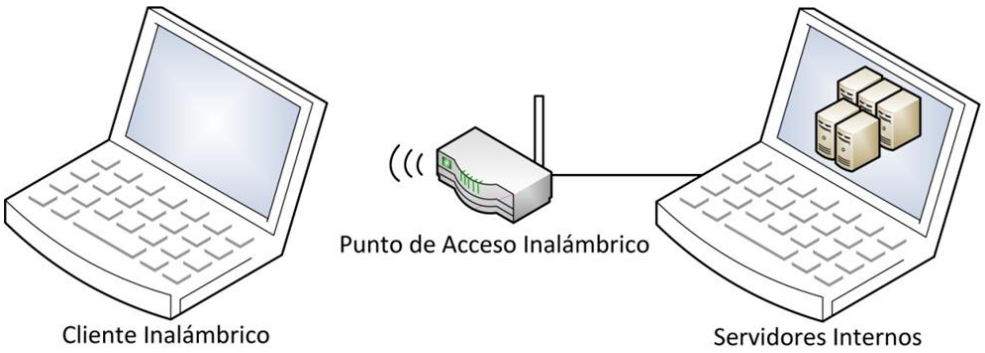


Figura 6.2 - Escenario de Simulación (Equipos)

La figura 6.3 muestra los servidores que se implementaron dentro de cada máquina virtual. Los servidores quedaron distribuidos de la siguiente manera:

- Una máquina virtual con un servidor web interno que sirvió para probar el acceso a los recursos de la red interna por parte del cliente inalámbrico (SERVER).
- Una máquina virtual con dos interfaces de red que fue usada como VPN/Cortafuegos para el acceso de los usuarios inalámbricos (VPN).
- Una máquina virtual donde se implementaron un servidor de dominio, un servidor de certificación y un servidor RADIUS (DC-CA-NPS).

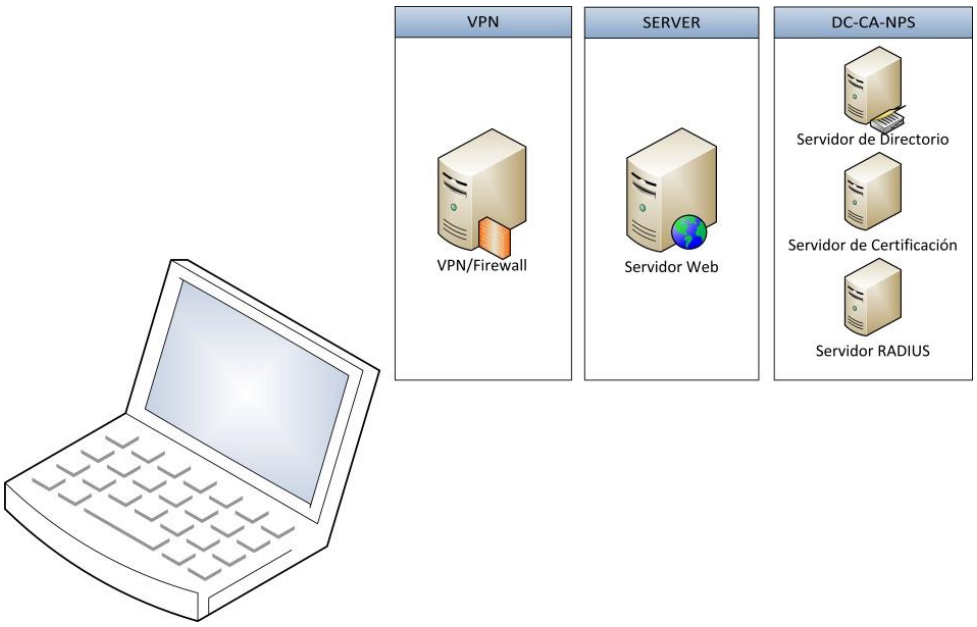


Figura 6.3 - Escenario de Simulación (Máquinas Virtuales)

Para completar el escenario fue necesaria la creación de una red virtual por medio del VirtualBox. La máquina virtual VPN contó con 2 interfaces de red, una de ellas fue conectada a la red física a través de la interfaz de red de la portátil, mientras la otra fue conectada a la red virtual creada. Esta red virtual representó la red interna de la empresa, por lo que los demás servidores solo tuvieron una interfaz que estuvo conectada a esta red. La figura 6.4 muestra la ubicación de los equipos dentro de las redes en el escenario de simulación.

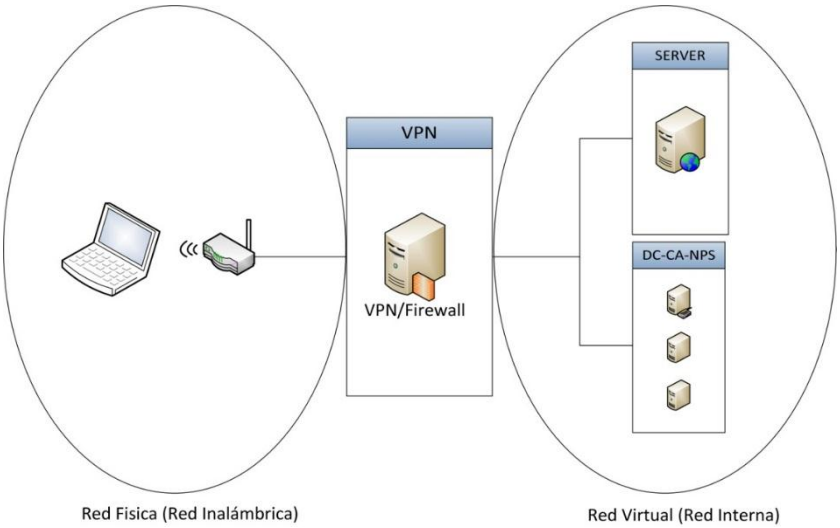


Figura 6.4 - Escenario de Simulación (Redes)

6.3. IMPLEMENTACIÓN

Para el proceso que se describirá a continuación se crearon las máquinas virtuales VPN, SERVER y DC-CA-NPS usando el software de virtualización VirtualBox y se instaló en ellas el sistema operativo Windows Server 2008 R2. Adicionalmente se asignó el direccionamiento IP como se muestra en las tablas 3 y 4.

Red	Rango de IPs
Red Interna	10.10.10.0/24
Red Externa (Inalámbrica)	192.168.1.0/24
Conexiones VPN	10.10.20.0/24

Tabla 3 - Direccionamiento (Redes)

Equipo	Dirección IP / Máscara de Subred	Puerta de Enlace Predeterminada	DNS
DC-CA-NPS	10.10.10.100/24	10.10.10.101	127.0.0.1
VPN (Interfaz 1)	10.10.10.101/24	No Configurado	10.10.10.100
VPN (Interfaz 2)	192.168.1.250/24	192.168.1.1	No Configurado
SERVER	10.10.10.102/24	10.10.10.101	10.10.10.100
AP	192.168.1.1/24	No configurado	No configurado

Tabla 4 - Direccionamiento (Configuración IP)

6.3.1. Instalación y Configuración de Active Directory

Esta implementación está basada en la integración de varios servicios en donde las cuentas de usuario son administradas por un servicio de directorio. En un ambiente empresarial generalmente podemos encontrar un servicio de directorio implementado, por lo que solo tendremos que configurarlo para integrarlo a nuestra solución de seguridad.

Para nuestra implementación al no contar con una red previamente configurada, hicimos una instalación sencilla de un Controlador de Dominio usando Windows Server 2008 R2, en donde creamos el dominio “tesis.com”.

Empezamos instalando el Active Directory en la maquina DC-CA-NPS **(Anexo 5.1)**. Luego procedimos a crear cuentas de usuarios y grupos a los que más adelante asignamos permisos para el acceso a la red interna a través de la red inalámbrica. Con la ayuda del Active Directory Users and Computers creamos la estructura mostrada en la figura 6.5, en donde asignamos al usuario Diego Chóez (dchoez) como miembro del grupo de seguridad WirelessUsersGroup.

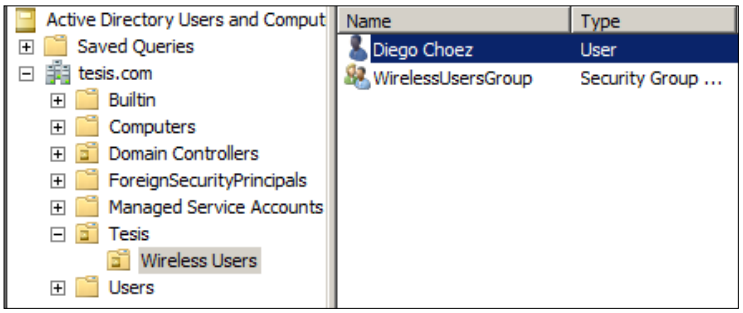


Figura 6.5 - Usuarios y grupos en el Active Directory

6.3.2. Instalación y Configuración de “Certification Authority”

Para el manejo y emisión de los certificados digitales usamos la maquina DC-CA-NPS, en donde agregamos el rol de “Certification Authority”. Debemos tomar en cuenta que para que pueda integrarse con el Active Directory es necesario instalarlo como tipo “Enterprise”.

Adicionalmente para facilitar la distribución de los certificados digitales a los clientes instalamos el “Certification Authority Web Enrollment”, este servicio instala un portal web desde el cual podemos solicitar y descargar los certificados digitales desde los clientes. **(Anexo 5.2)**

6.3.3. Instalación y Configuración de Network Policy Server

La máquina DC-CA-NPS también cumplió el rol de servidor RADIUS, para que el equipo pueda cumplir con esta función instalamos el Network Policy Server. Mediante el asistente de configuración de conexiones del Network Policy Server pudimos configurar al servidor NPS como servidor RADIUS. Aquí se establecieron los parámetros de configuración para cada uno de los clientes RADIUS, como dirección IP o nombre y la clave compartida. En nuestra infraestructura solo contamos con uno, que es el servidor VPN.

Para un mayor control se agregó a las políticas de petición de conexiones a un grupo específico de usuarios asignándoles así permisos para acceder a través de esta conexión. Usamos el grupo de usuarios que creamos previamente en el Active Directory, “WirelessUsersGroup”. **(Anexo 5.3)**

6.3.4. Instalación y Configuración de Forefront TMG

En la máquina virtual VPN instalamos el Forefront TMG que nos permitió habilitarla como servidor VPN y Cortafuegos. Para su configuración, este equipo debió ser previamente agregado al dominio “tesis.com”.

De acuerdo al diseño propuesto, éste equipo funcionó como cortafuegos de borde entre la red cableada y la red inalámbrica por lo que debió contar con dos adaptadores de red, uno para cada red. Esto se debe considerar desde su instalación, ya que desde el asistente de instalación se establece la red que el servidor conocerá como “red interna” y esto repercutirá en las políticas de seguridad que serán implementadas. Más adelante en el proceso de configuración se estableció al otro adaptador como “red externa”, este adaptador es el que estaba conectado a la red inalámbrica.

Una vez instalado el Forefront TGM, habilitamos el acceso a clientes VPN a través de este servidor. En este punto se configuró el tipo de autenticación (EAP con certificados digitales), el servidor RADIUS que se usó para autenticar a los clientes (en nuestra implementación es el servidor DC-CA-

NPS), y el protocolo de túnel admitido para las conexiones de los clientes (PPTP).

Opcionalmente, para mejorar la seguridad y aprovechar las funcionalidades del Forefront TGM podemos agregar reglas de cortafuegos, en donde solo daremos acceso a ciertos servicios o protocolos a los usuarios conectados a través de la VPN. **(Anexo 5.4)**

6.3.5. Configuración de Punto de Acceso Inalámbrico

En nuestro ruteador inalámbrico realizamos las configuraciones básicas para habilitar el acceso inalámbrico, usamos como tipo de seguridad WPA2-Personal con cifrado AES. Esto permitió brindar un primer nivel de seguridad para el acceso a la red inalámbrica de la empresa. **(Anexo 5.5)**

6.3.6. Configuración de VPN en el cliente

Antes de configurar el cliente para el acceso a la VPN necesitamos obtener un certificado digital para autenticarnos. Para ello debimos conectar temporalmente el equipo cliente a la red interna para poder acceder al CA y solicitar el certificado. Otra opción habría sido solicitar el certificado desde

un equipo de la red interna, para luego exportarlo e instalarlo en el equipo cliente.

Una vez instalado el certificado en el cliente, y ya estando conectados a la red inalámbrica, agregamos una nueva conexión VPN y configuramos esta conexión para que use el certificado ya instalado en el equipo para autenticarse. **(Anexo 5.6)**

6.4. RESULTADOS DE LA IMPLEMENTACION

Al completar de manera exitosa la implementación se pudo constatar lo siguiente. Los clientes estaban configurados para autenticarse ante el servidor usando un certificado digital y no una contraseña. Esto eliminó cualquier desventaja producida al usar contraseñas de usuario, como la posibilidad que el usuario use una contraseña sencilla, que la tenga anotada en un lugar visible o que sea robada. Al mismo tiempo el equipo cliente comprobaba la identidad del servidor. La configuración no permitía que el cliente se conecte con ningún servidor a menos que este servidor se identifique usando un certificado digital emitido por la entidad de certificación propia de la empresa, eliminado así la posibilidad de que se conecte con un punto de acceso falso. La inclusión de un cortafuegos permitió tener un control sobre los recursos a los que podía acceder un cliente

inalámbrico. De esta manera, aun cuando llegase a comprometerse la seguridad de la red inalámbrica los recursos que quedarían expuestos ante el atacante serian limitados.

CONCLUSIONES

1. Deshabilitar la difusión del SSID y el filtrado de direcciones MAC son métodos realmente sencillos de eludir. En las pruebas se demostró que con el uso de un analizador de paquetes es posible ver en texto plano tanto el SSID de un punto de acceso como las direcciones MAC de los clientes conectados. Luego es posible cambiar la dirección MAC de nuestra tarjeta para que coincida con una de las direcciones permitidas. Este proceso solo depende de la captura de paquetes y no requiere procesamiento adicional por lo que puede ser realizado en menos de 5 minutos.

2. La seguridad WEP está obsoleta. En las pruebas realizadas se pudo comprobar que, sin importar la longitud o la complejidad de la contraseña, ésta se pudo obtener con un 100% de éxito. El proceso de obtención de esta contraseña en ninguna de las pruebas tardo más de 4 minutos.
3. Una contraseña lo suficientemente compleja con WPA/WPA2 logra que un ataque de diccionario pierda sus posibilidades de éxito llegando a 0%, ya que si la contraseña no se encuentra en el diccionario será imposible de obtener. Por otro lado, un ataque de fuerza bruta a esta tecnología seria impráctico debido al tiempo que requiere. En un ejemplo, si tuviéramos una contraseña con 8 caracteres entre mayúsculas, minúsculas y números, tendríamos 82^8 posibles contraseñas. En las pruebas realizadas se alcanzó una velocidad de 1950 claves comprobadas por segundo. A la velocidad mencionada anteriormente comprobar todas las posibles contraseñas del ejemplo tardaría 33240 años.
4. La autenticación del servidor por parte del cliente también es importante ya que ayuda a prevenir ataques de puntos de acceso falsos. En las pruebas se demostró que si un cliente no está configurado para comprobar la identidad del servidor, es posible que el cliente sin darse cuenta se conecte a un punto de acceso falso que use el mismo SSID que uno verdadero.

5. Los certificados digitales como alternativa al uso de contraseñas nos ofrecen un método de autenticación mucho más seguro, pero su adopción se ha limitado debido a la complejidad de su implementación.
6. El nivel más alto de seguridad en una red inalámbrica se lo puede obtener con una implementación de seguridad basada en certificados digitales, configurada de manera que tanto el cliente como el servidor requieran un certificado para autenticarse mutuamente, además que los únicos certificados admitidos sean los emitidos específicamente por la entidad de certificación propia de la empresa.

RECOMENDACIONES

1. En instalación de puntos de acceso inalámbricos personales se debe evitar dejar ciertos valores predeterminados, como el nombre y contraseña de administrador y el SSID. Existen sitios web que recopilan estos valores predeterminados de los diferentes modelos y fabricantes que pueden ser consultados fácilmente por usuarios maliciosos.
2. Deshabilitar la opción WPS en los puntos de acceso siempre que sea posible, una vulnerabilidad en esta tecnología permite realizar ataques de fuerza bruta en tiempos relativamente cortos (4-10 horas) en comparación con ataques a WPA.

3. En un ambiente empresarial, mantener la red inalámbrica en una subred independiente y limitar los recursos a los que se puede acceder a través de ella.
4. Antes de seleccionar un modelo de seguridad empresarial debemos tomar en cuenta que este sea compatible con los diferentes sistemas operativos de los clientes inalámbricos.
5. Como responsables de la administración de la red de una organización debemos asegurarnos de informar adecuadamente acerca de los riesgos de seguridad en redes inalámbricas a los propietarios de la organización.

GLOSARIO

Ataque de diccionario: tipo de ataque informático en donde se trata de obtener una contraseña probando todas las palabras o cadenas de caracteres de una base de datos comúnmente llamada diccionario.

Ataque de fuerza bruta: tipo de ataque informático en donde se trata de obtener una contraseña probando todas las combinaciones de caracteres posibles.

Auditoría: registro de las acciones realizadas por un usuario o entidad.

Autenticación desafío-respuesta: método que permite probar la identidad de un usuario sin enviar directamente la contraseña a través de la red. En su lugar se envía un valor al cliente, este realiza un cálculo sobre ese valor que implica el uso de la contraseña, y el resultado es devuelto al servidor.

Autenticación: proceso por el que un usuario o entidad prueba su identidad ante un sistema u otra entidad.

Autoridad de Certificación: entidad encargada de emitir y administrar certificados digitales.

Autorización: proceso que permite determinar los recursos y privilegios a los que tiene acceso un usuario o entidad.

Certificado digital: documento digital emitido por una autoridad de certificación que garantiza la vinculación entre usuario o entidad con una clave pública.

Cifrado: procedimiento que permite transcribir un mensaje usando una clave y un algoritmo con el objetivo de volverlo incomprensible ante quienes no posean la clave de descifrado.

Clave pre-compartida: clave secreta que compartida entre las partes en un sistema de comunicaciones a través de un canal seguro antes de ser usada.

Cliente: equipo o aplicación informática que solicita y hace uso de los servicios de otro, conocido como servidor.

Credenciales: combinación de nombre de usuario, contraseña y otros elementos que permiten a un usuario probar su identidad.

Cortafuegos: software o hardware que controla el paso del tráfico en una red basado en un conjunto de reglas de acceso.

Diagrama: representación gráfica de uno o varios elementos de un entorno.

Dial-up: forma de acceso a internet que usa la infraestructura de la red telefónica publica conmutada (PSTN).

Distribución Linux: Software basado en el núcleo Linux que incluye diversos paquetes de software, dando origen a diversas ediciones de sistema.

Dominio: conjunto de ordenadores conectados en una red que confían a uno o varios de los equipos de dicha red la administración de los usuarios y privilegios.

Frecuencia: Numero de ciclos que una señal u onda realiza en cada segundo.

Infraestructura de clave pública: plataforma que incluye el hardware, software, políticas y procedimientos necesarios para la gestión de certificados digitales.

Interfaz: conexión física entre dos sistemas o dispositivos que permiten la comunicación entre distintos niveles.

Kerberos: protocolo de autenticación, permite la autenticación entre dos equipos en una red.

Registro: información de eventos en un determinado rango de tiempo, de una aplicación o servicio.

Máquina virtual: computador simulado a través de un software de virtualización que permite la ejecución de software como si fuese un equipo real.

Punto de Acceso: hardware que permite a un dispositivo móvil conectarse a una red existente.

Servicio: proceso informático no interactivo que se ejecuta en segundo plano que puede ser controlado por el usuario.

Servidor: equipo o aplicación informática que proporciona servicios a otros denominados clientes.

Software malicioso: software que tiene como objetivo ingresar sin autorización a un sistema para obtener información, dañarlo o tomar el control de él.

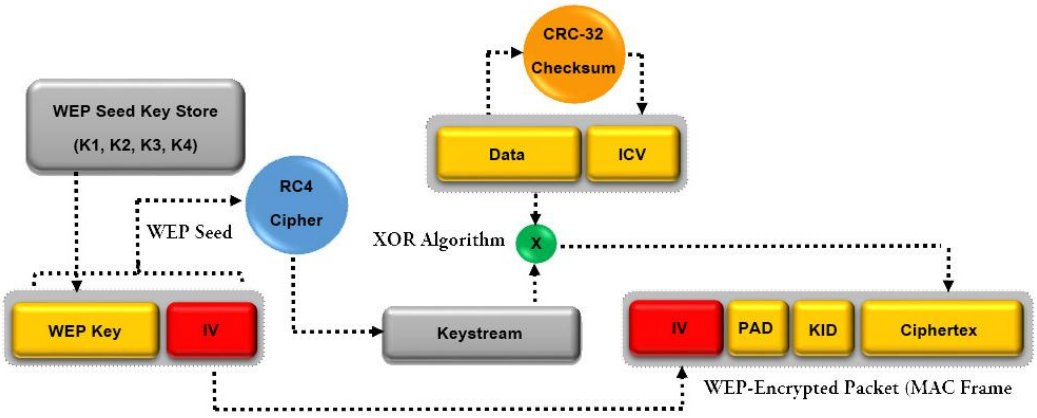
Texto plano: texto que no tiene ningún formato o cifrado, es decir, que no requieren ser interpretados para leerse.

Túnel: técnica que permite encapsular un protocolo de red dentro de otro. Esto permite transportar un protocolo a través de una red incompatible o proveer una ruta segura a través de una red poco confiable.

Vulnerabilidad: error o debilidad en un sistema informático que permite comprometer su integridad, disponibilidad o seguridad.

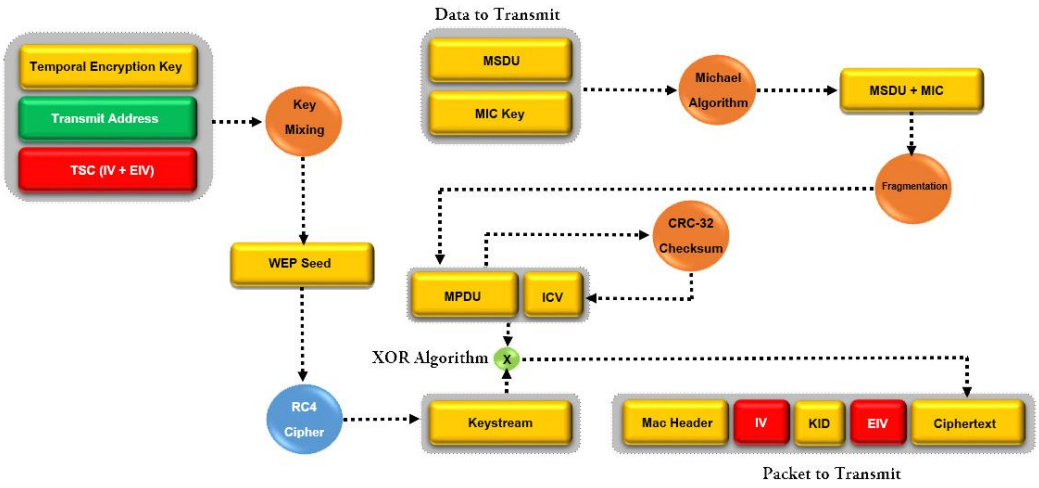
ANEXO 1

1.1 ESQUEMA DEL CIFRADO WEP



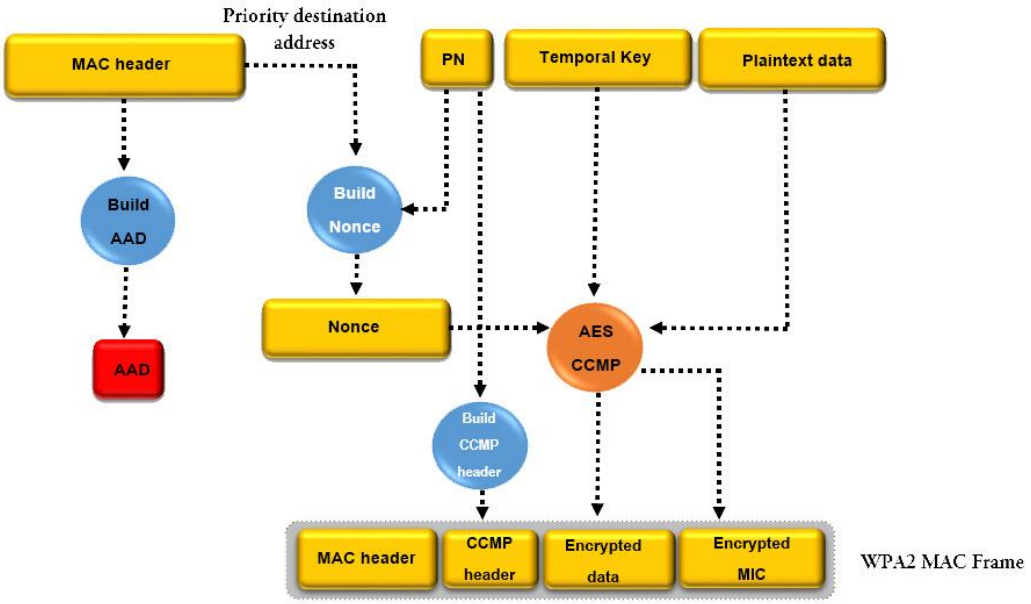
Esquema de funcionamiento de cifrado WEP [19]

1.2 ESQUEMA DEL CIFRADO WPA



Esquema de funcionamiento de WPA [19]

1.3 ESQUEMA DEL CIFRADO WPA2



Esquema de funcionamiento de WPA2 [19]

ANEXO 2

COMPARACIÓN DE TIPOS DE AUTENTICACIÓN

	Autenticación	Tipos de cifrado	Uso	Características
Abierta	Ninguna	Ninguno	No recomendado	- Permite el acceso a cualquier dispositivo - Se puede proveer seguridad usando portales cautivos
WEP	PSK	RC4 - simétrico	Solo si se requiere por compatibilidad	- Primer método de autenticación implementado en redes inalámbricas - Actualmente obsoleta
WPA-Personal	PSK	TKIP, CCMP	Hogar	- Creada para corregir los problemas de seguridad de WEP - Originalmente usa TKIP para el cifrado, actualmente también soporta CCMP - La seguridad depende de la complejidad y confidencialidad de la contraseña
WPA2-Personal	PSK	CCMP, TKIP	Hogar - Empresa Pequeña	- Implementa por completo el estándar IEEE 802.11i - Usa CCMP de manera predeterminada, soporta TKIP por retrocompatibilidad - WPA2/CCMP permite aprovechar la máxima velocidad del estándar 802.1n
WPA-Enterprise	802.1x	TKIP, CCMP	Empresa	- Requiere una infraestructura RADIUS - Provee autenticación de usuarios - Alto costo de implementación
WPA2-Enterprise	802.1x	CCMP, TKIP	Empresa	- Junto a una implementación de certificados digitales constituye uno de los sistemas más seguros en la actualidad. - Alto costo de implementación

ANEXO 3

NIVELES DE GRAVEDAD EN UN INFORME DE UN TEST DE PENETRACION

Nivel de Gravedad	Problemas Encontrados	Medidas a tomar
Alto	Se ha detectado que un ataque ha sido llevo a cabo o está siendo llevado a cabo	Determinar los daños causados o la información confidencial que fue comprometida
Medio	Se ha encontrado una vulnerabilidad en el sistema que puede ser explotada por un atacante	Determinar las causas de la vulnerabilidad y proponer soluciones que mejoren la seguridad del sistema
Bajo	Se ha encontrado una vulnerabilidad en los procedimientos que podría ser explotada.	Recomendar procedimientos administrativos y políticas que permitan evitar los inconvenientes encontrados

ANEXO 4

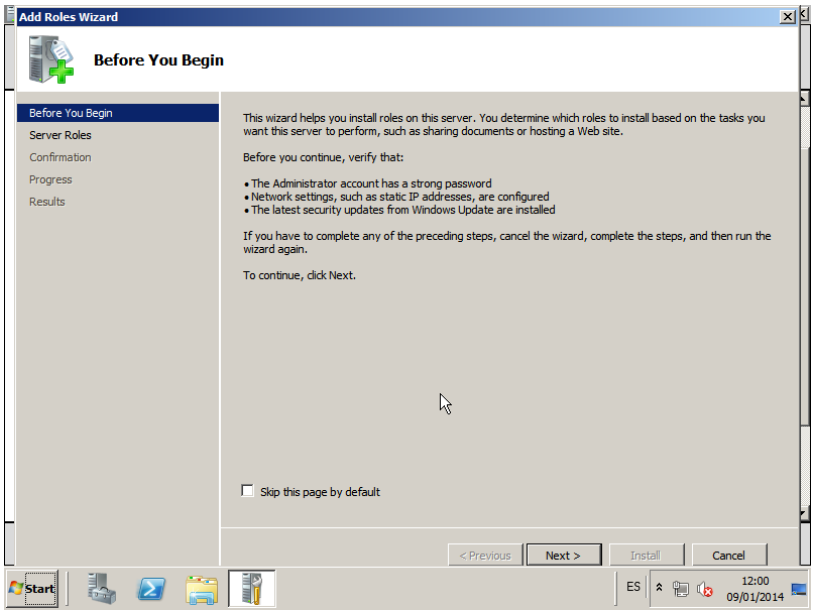
COMPARACIÓN DE SISTEMAS OPERATIVOS PARA AUDITORIA DE REDES INALÁMBRICAS

	Uso	Sistema Base	Entornos Gráficos	Ventajas	Desventajas
Beini	Orientado a la auditoria de redes WiFi	Tiny Core Linux	Tiny Core Linux	- Herramientas en entorno gráfico. (Facilidad de uso) - Tamaño Reducido (50Mb)	- Pocas herramientas y opciones avanzadas. - No recibe actualizaciones constantes.
Wifiway	Orientado a la auditoria de redes WiFi, Bluetooth y RFID	Distribución Original	KDE	- Disponible en español - Gran cantidad de herramientas para evaluación y auditoria de redes inalámbricas	- Desarrollo detenido, última versión liberada en 2012.
Backtrack	Orientado a la auditoria de seguridad en general	Ubuntu	KDE, Gnome	- Mayor documentación y soporte. - Mayor cantidad de herramientas para auditoria en general	- Se requiere de un mayor nivel de conocimientos para su uso. - En el año 2013 fue reemplazado por Kali Linux.
Kali Linux	Orientado a la auditoria de seguridad en general	Debian	KDE, Gnome , Xfce, LXDE	- Soporte para una gran cantidad de dispositivos inalámbricos - Soporte para sistemas basados en ARM - Admite la recompilación del kernel	- Se requiere de un alto nivel de conocimientos en hacking ético y desarrollo para aprovechar al máximo sus funciones.

ANEXO 5

5.1 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN DE ACTIVE DIRECTORY

Abrimos el Server Manager, damos clic derecho en roles y en el menú desplegable seleccionamos “Add roles”. Se abrirá el asistente para agregar roles.

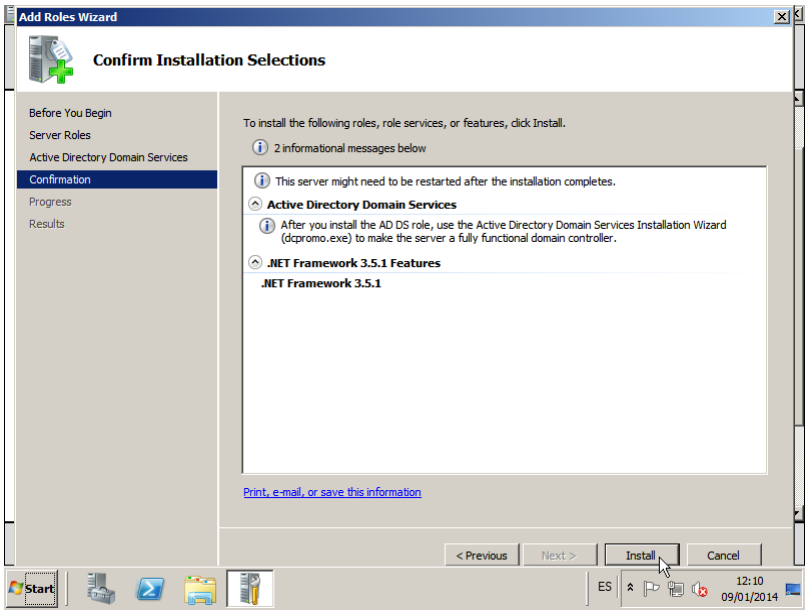


Instalación de Active Directory 1

Damos clic en siguiente y en la lista de roles habilitamos la casilla de verificación “Active Directory Domain Services”. Si aún no tenemos instalado el .NET Framework, se mostrará un mensaje advirtiéndonos que es requerido para la instalación del Active

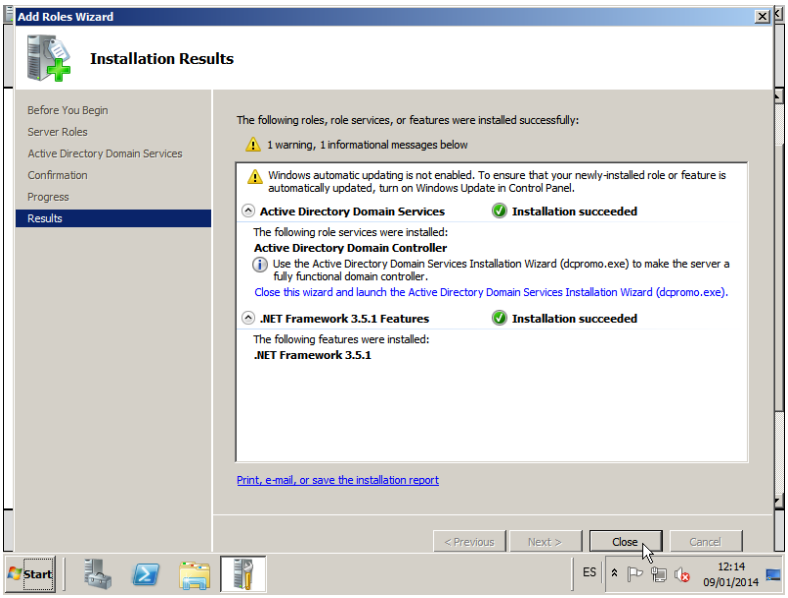
Directory, elegimos “Add required features” para continuar. Luego clic en siguiente.

En la siguiente ventana se nos muestra una pequeña descripción y recomendaciones del rol que vamos a instalar, solo damos clic en siguiente. A continuación se nos pide confirmar lo que se va a instalar mostrándonos un resumen de lo seleccionado durante todo el proceso de instalación, damos clic en instalar.



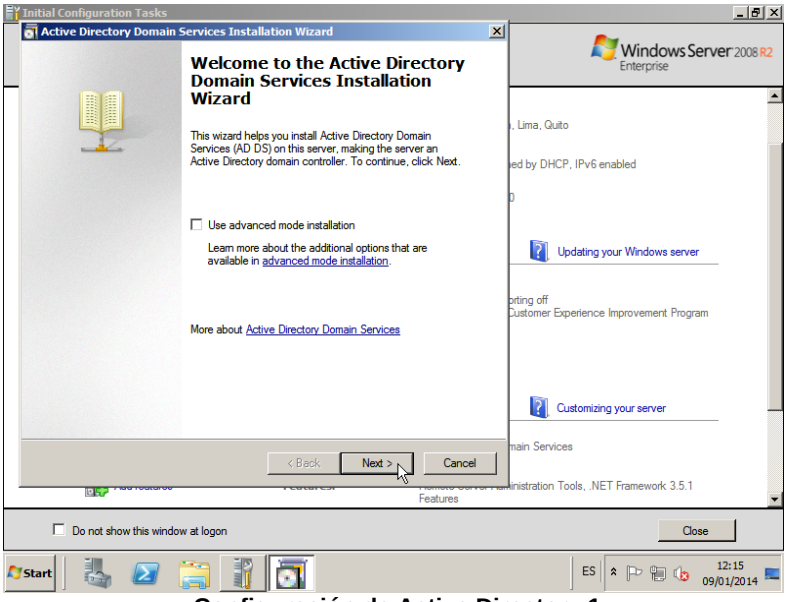
Instalación de Active Directory 2

Al finalizar la instalación veremos un informe en donde podremos verificar que el proceso se llevó a cabo de manera correcta.



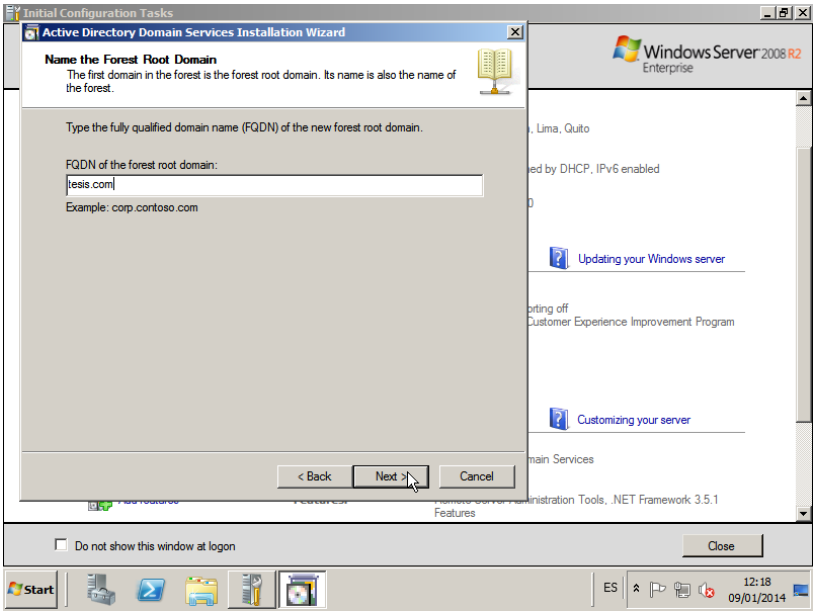
Instalación de Active Directory 3

Con esto hemos completado la instalación del servicio de directorio, ahora crearemos un dominio llamado “tesis.com”.



Configuración de Active Directory 1

Abrimos una ventana de ejecución de Windows escribiendo “Run” en la barra de búsqueda del menú de inicio y seleccionando la opción entre los resultados de la búsqueda o usando la combinación de teclas Windows+R. En la ventana de ejecución escribimos “dcpromo.exe”, con lo que se ejecutará el asistente de instalación y configuración del Active Directory.



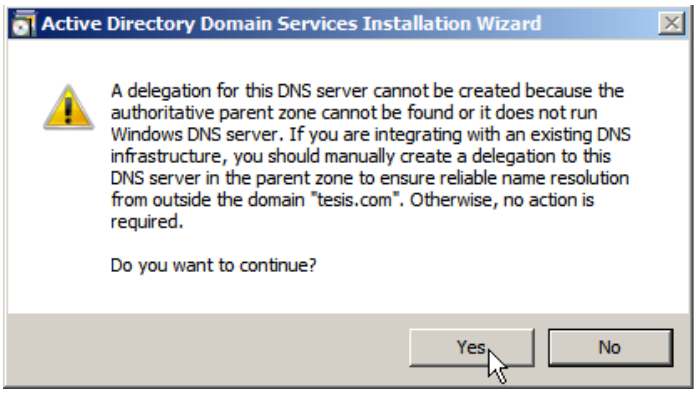
Configuración de Active Directory 2

Damos clic en siguiente, se nos mostrara una advertencia con respecto a las nuevas configuraciones de seguridad de Windows Server 2008, damos clic en siguiente. Seleccionamos “Create new Domain in a new forest” ya que es el primer y único dominio que

tendremos en nuestra implementación. En el siguiente paso se nos solicitará ingresar el nombre que le queremos dar al dominio, ingresamos “tesis.com”.

A continuación en las siguientes 2 ventanas se nos pedirá establecer el Forest Functional Level y el Domain Functional Level, en ambos casos seleccionamos Windows Server 2008, ya que en nuestro dominio solo trabajaremos con Windows Server 2008.

Siguiendo con el proceso de instalación, seleccionamos instalar el servicio de servidor DNS, necesario para el funcionamiento del Active Directory. Se mostrará una advertencia relacionada con la infraestructura de DNS, sin embargo, al ser el primer servidor DNS instalado en nuestra infraestructura no representará un problema para la instalación, damos clic en “Yes” para poder continuar con la instalación

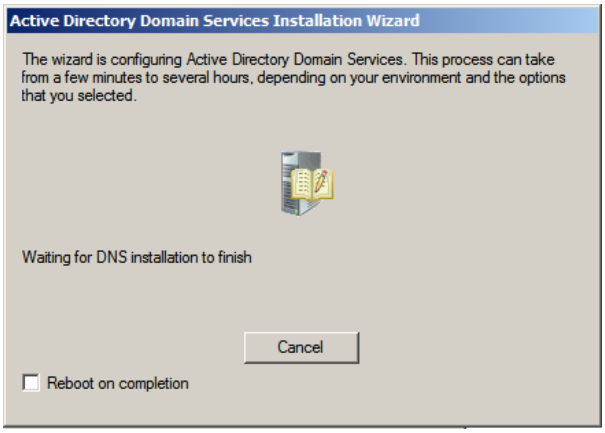


Configuración de Active Directory 3

Luego de dar clic en siguiente se nos solicitará el ingreso de algunas rutas usadas para almacenar archivos y bases de datos del Active Directory, dejamos las opciones predeterminadas y damos clic en siguiente.

En el siguiente paso ingresamos y confirmamos la contraseña para el modo de restauración del Active Directory, damos clic en siguiente. Se mostrará un resumen de las opciones elegidas durante el proceso de instalación, luego de verificar que todo esté de acuerdo a nuestros requerimientos, damos clic en siguiente para que comience el proceso de configuración.

Mientras se ejecuta este proceso podemos seleccionar la casilla de verificación “Reboot on completion” para que al finalizar el proceso el equipo se reinicie automáticamente completando el proceso de instalación y configuración.

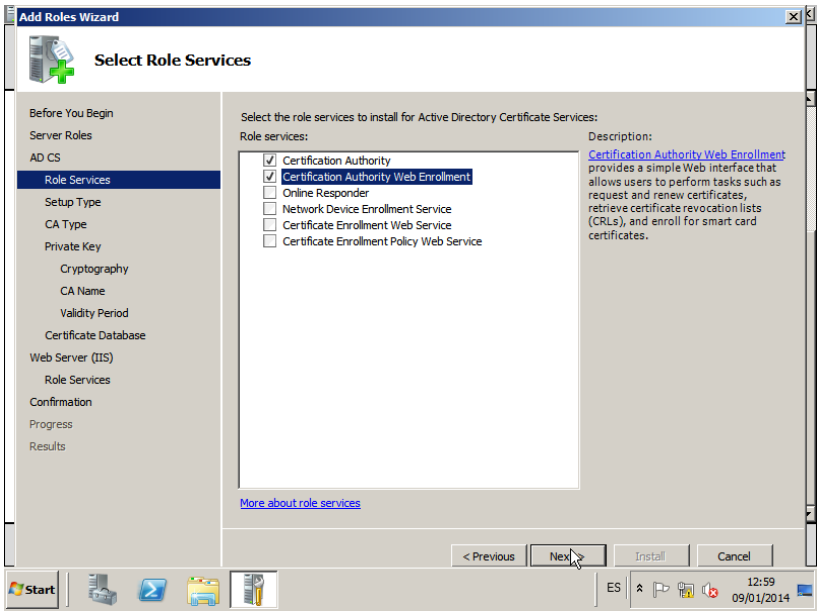


Configuración de Active Directory 4

5.2 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN DE CERTIFICATION AUTHORITY

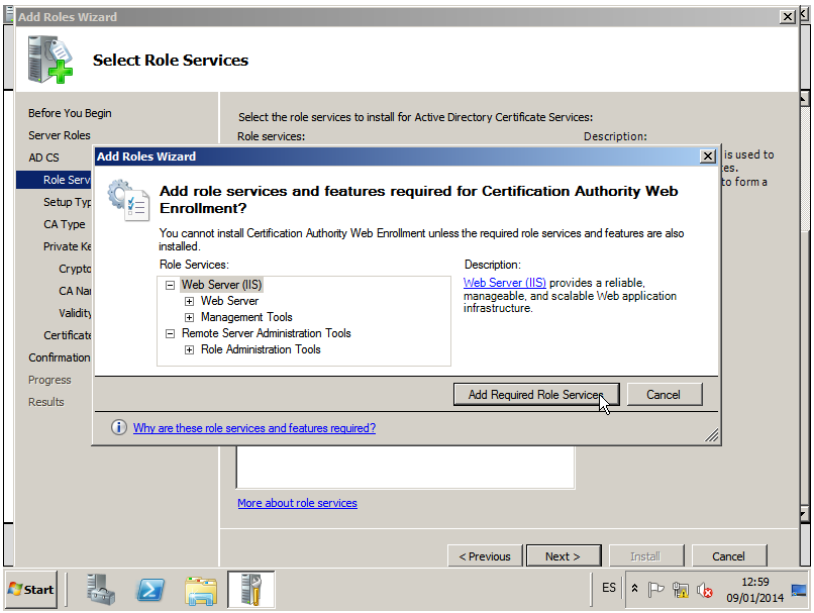
Ingresamos al asistente para agregar roles, para esto vamos al Server Manager, clic derecho en Roles, “Add Roles”.

En la lista de roles seleccionamos “Active Directory Certificate Services” y damos clic en siguiente, entonces seleccionamos “Certification Authority” y “Certification Authority Web Enrollment”.



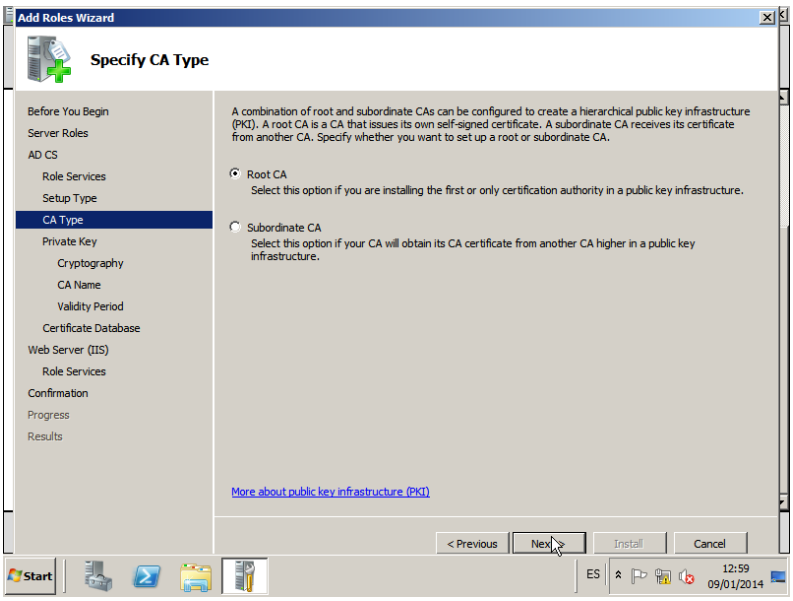
Instalación de Certification Authority 1

Se mostrará una ventana indicándonos que se requieren servicios adicionales para proceder con la instalación de los servicios que hemos elegido, el Web Sever y el Remote Server Administration Tools. Estos servicios son necesarios para la emisión de certificados vía Web. Seleccionamos “Add Require Role Services”.



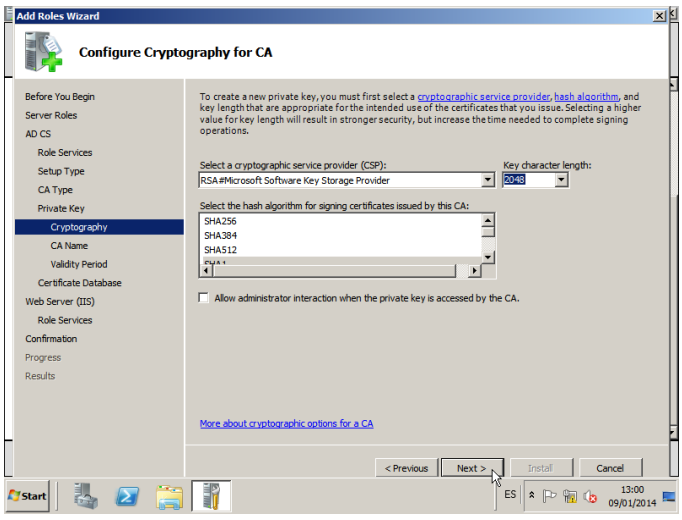
Instalación de Certification Authority 2

En el siguiente paso elegiremos el tipo de CA (Entidad de Certificación) que queremos instalar, elegimos Enterprise, este tipo de CA usa la información del Active Directory para emitir y manejar los certificados digitales. Luego estableceremos el rol que cumplirá el CA dentro de la infraestructura de clave pública (PKI), en este caso al ser el único CA dentro de la infraestructura será necesariamente Root CA.



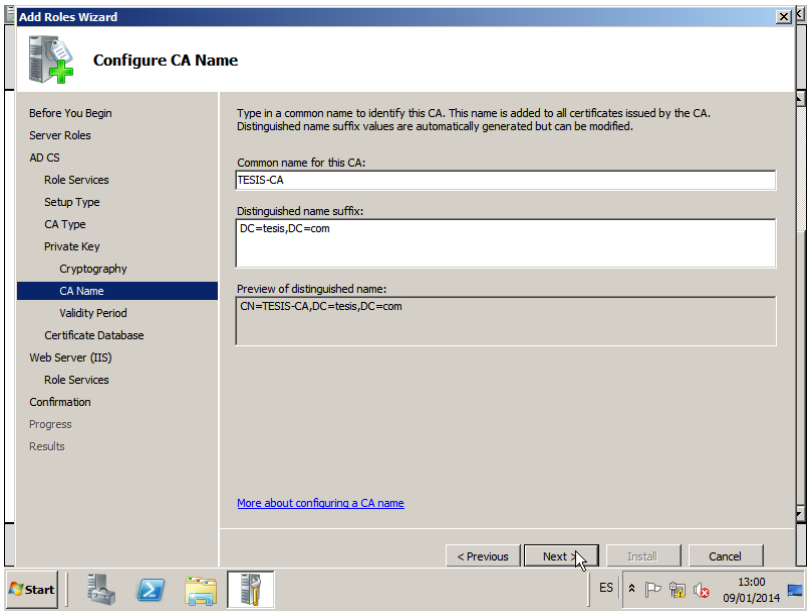
Instalación de Certification Authority 3

En los siguientes pasos se creará una clave pública para el CA, seleccionamos “Create a new prívate key” y a continuación seleccionamos las opciones de cifrado que usara el CA para la emisión de certificados.



Instalación de Certification Authority 4

Ahora ingresamos el nombre que identificará al CA y que será agregado a todos los certificados que emita. Para nuestra implementación usaremos el nombre “TESIS-CA”, damos clic en siguiente.

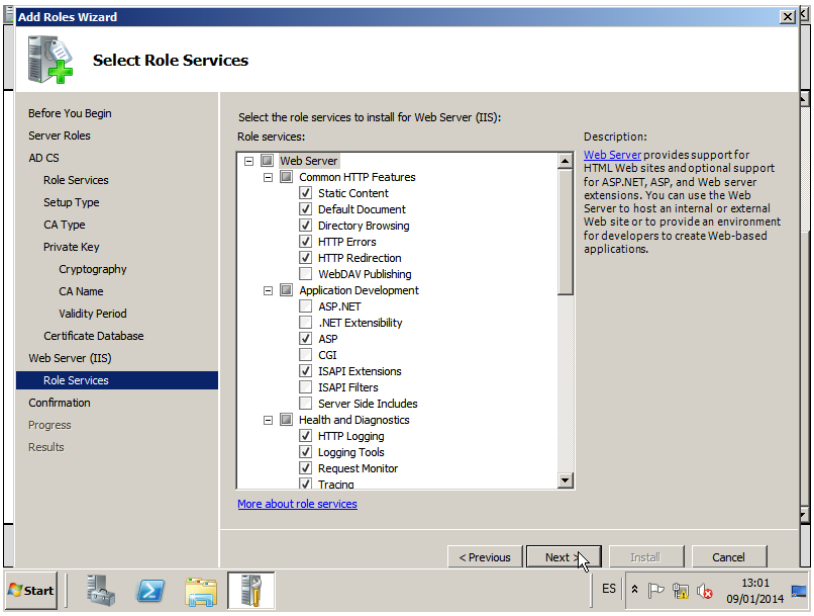


Instalación de Certification Authority 5

La siguiente ventana nos mostrará el periodo de validez que tendrá el certificado del CA, la dejamos en su valor predeterminado que es 5 años. Luego, en el último paso de la configuración para la instalación del CA podremos ver y modificar la ruta donde se almacenara la base de datos y registros del CA.

Al dar clic en siguiente comenzará el proceso de configuración para la instalación del rol Web server, que se nos solicitó instalar para el

funcionamiento del Certification Authority Web Enrollment. Dejamos las opciones predeterminadas y damos clic en siguiente.



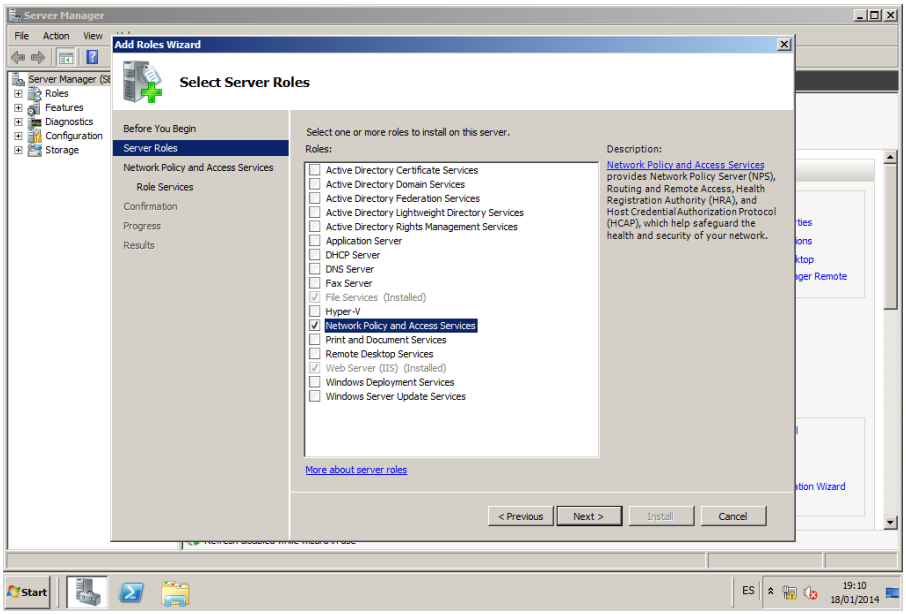
Instalación de Certification Authority 6

Aparecerá la ventana de confirmación en donde podremos comenzar con el proceso de instalación dando clic en instalar.

Si no hubo errores en el proceso de instalación, el servidor estará listo para funcionar sin requerir de ninguna configuración adicional.

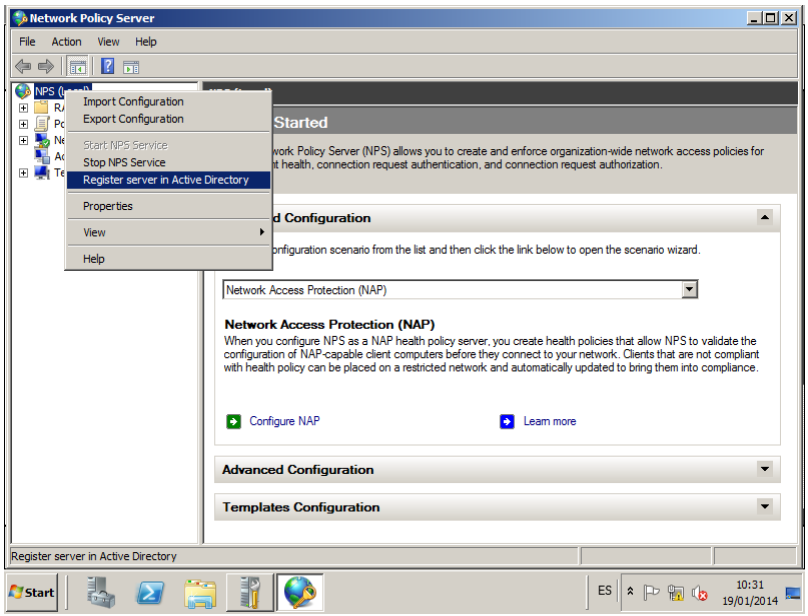
5.3 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN DE NETWORK POLICY SERVER

Abrimos el asistente para agregar roles y en la lista de roles seleccionamos “Network Policy and Access Services”.



Instalación de Network Policy Server 1

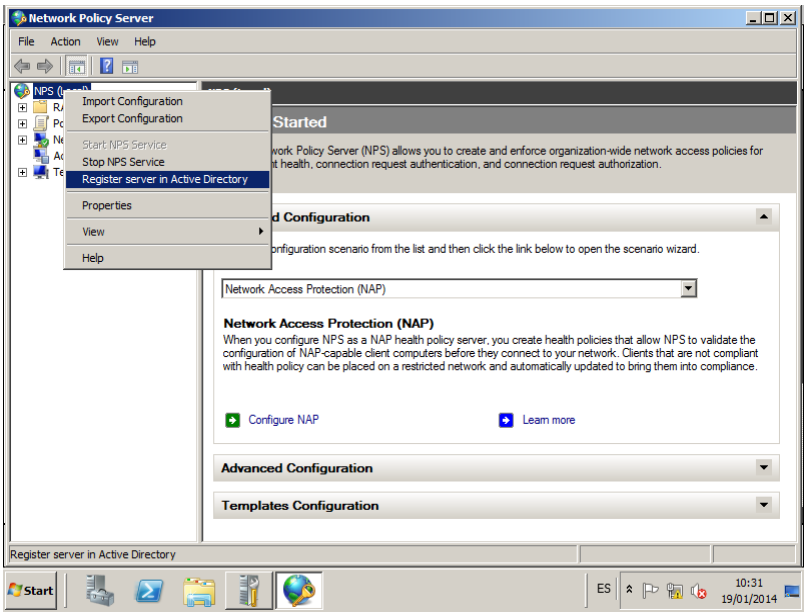
En la siguiente pantalla seleccionamos “Network Policy Server” y continuamos con la instalación dando clic en siguiente, y luego en instalar.



Instalación de Network Policy Server 2

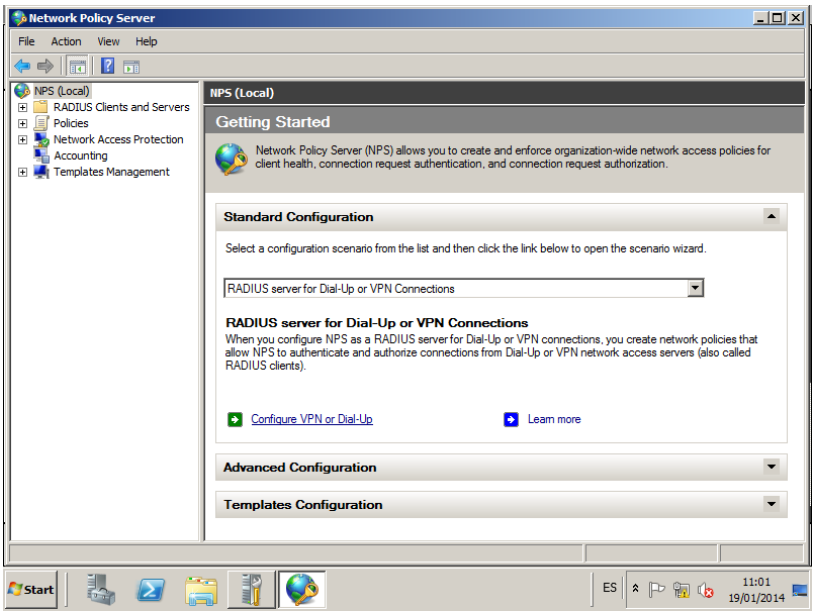
Luego de terminar el proceso, el Network Policy Server estará instalado y continuaremos con la configuración.

Abrimos la consola del Network Policy Server y lo primero que debemos hacer para que esté lista para funcionar en conjunto con el Active Directory es registrar el servidor en el Active Directory. Esto le permitirá al servidor NPS acceder a las credenciales de las cuentas de usuario almacenadas en el Active Directory. Para esto damos clic derecho en la opción “NPS (Local)” ubicada en el panel izquierdo de la consola y seleccionamos la opción “Register server in Active Directory”.



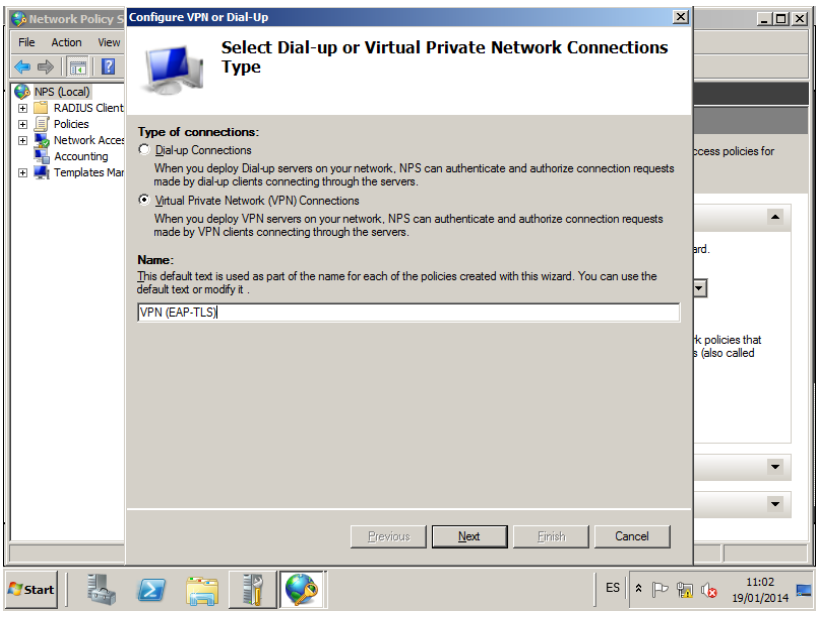
Configuración de Network Policy Server 1

En el panel “Standard Configuration”, en el menú desplegable, seleccionamos la opción “RADIUS Server for Dial-Up or VPN-Connections” y damos clic en “Configure VPN or Dial-Up”, esto abrirá un asistente que nos guiará en la configuración del NPS como servidor RADIUS. Seleccionamos “Virtual Private Network (VPN) Connections” y escribimos un nombre que será usado para identificar a las políticas.



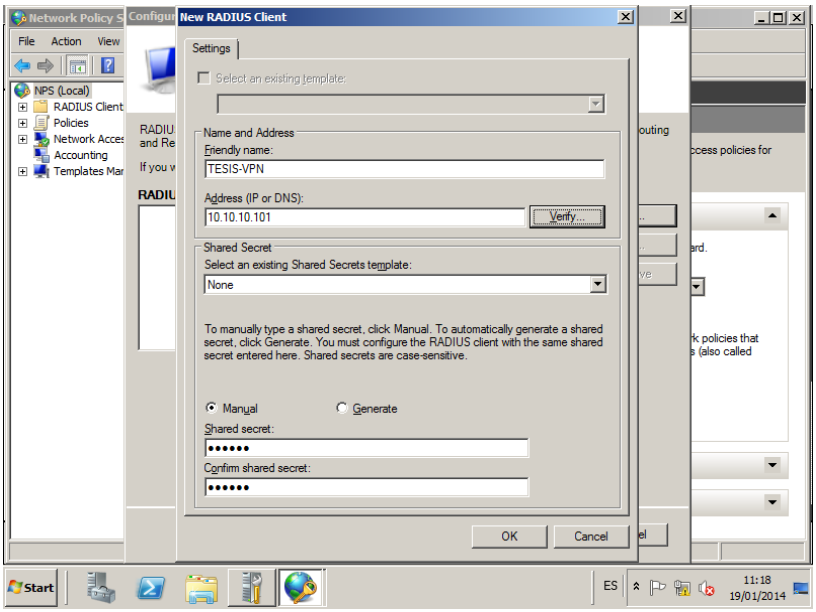
Configuración de Network Policy Server 2

En el siguiente paso se mostrarán los clientes VPN, para agregar uno nuevo damos clic en “Add”.



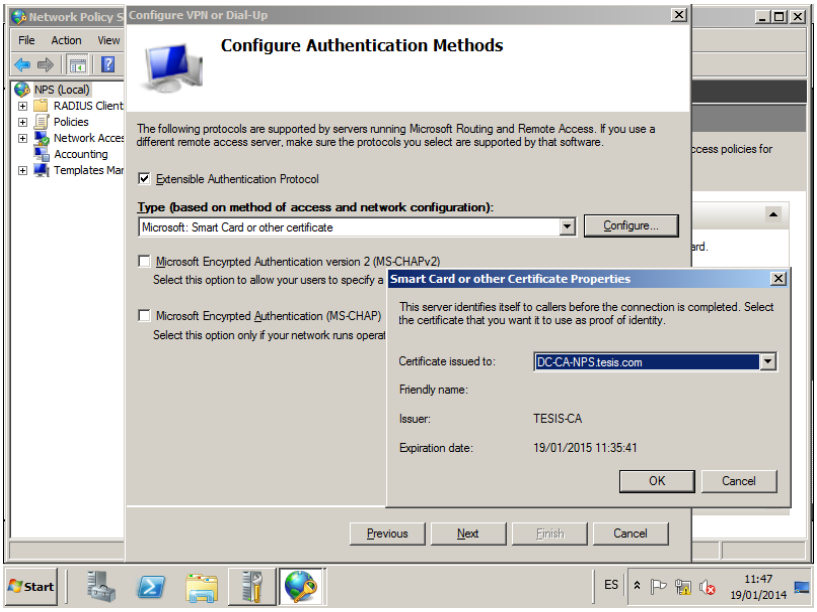
Configuración de Network Policy Server 3

Se abrirá una ventana en donde podremos usar el nombre de dominio o la dirección IP para agregar el nuevo cliente, además configuraremos la clave compartida que será usada para autenticar y cifrar las comunicaciones entre el servidor y el cliente RADIUS.



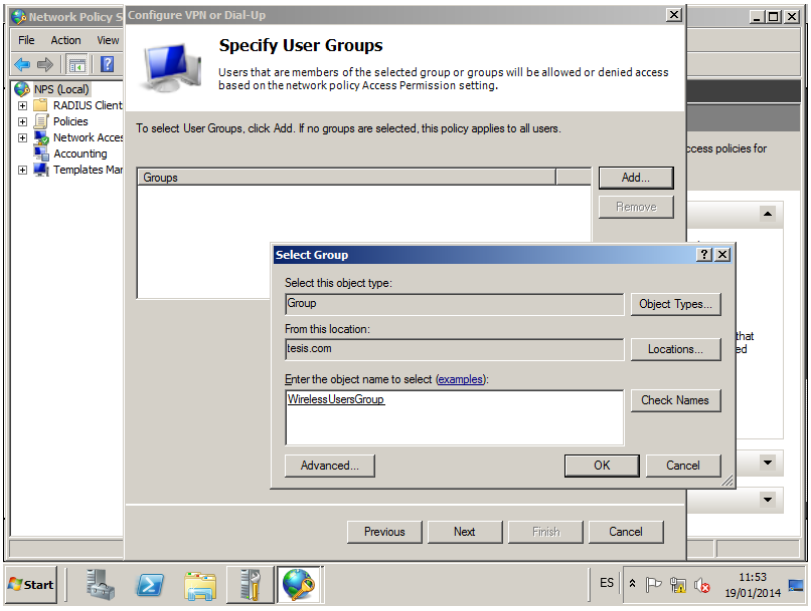
Configuración de Network Policy Server 4

Aceptamos y damos clic en siguiente. A continuación seleccionamos “Extensible Authentication Protocol” como método de autenticación y en la lista desplegable elegimos “Microsoft: Smart Card or other certificate”, de esta manera estableceremos la autenticación como EAP-TLS. Dando clic en configurar podremos seleccionar el certificado que usará el servidor para identificarse ante los clientes.



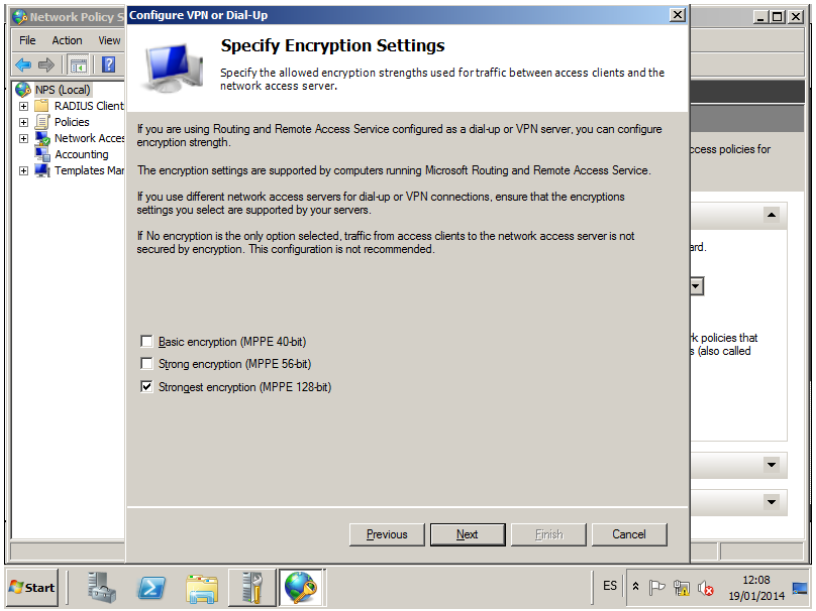
Configuración de Network Policy Server 5

En el siguiente paso agregaremos los grupos de usuarios que tendrán permisos para conectarse a través de la VPN, damos clic en "Add…" e ingresamos el nombre del grupo que creamos previamente para este propósito, "WirelessUsersGroup".



Configuración de Network Policy Server 6

El siguiente paso en la configuración solo es aplicable a una configuración con un servidor RRAS, por lo tanto solo damos clic en siguiente.



Configuración de Network Policy Server 7

Finalmente, configuraremos el nivel de cifrado que se usara entre los clientes de acceso y los servidores de acceso (Clientes RADIUS), deseleccionamos los dos primeros y solo dejamos el de 128 bits que es el más seguro.

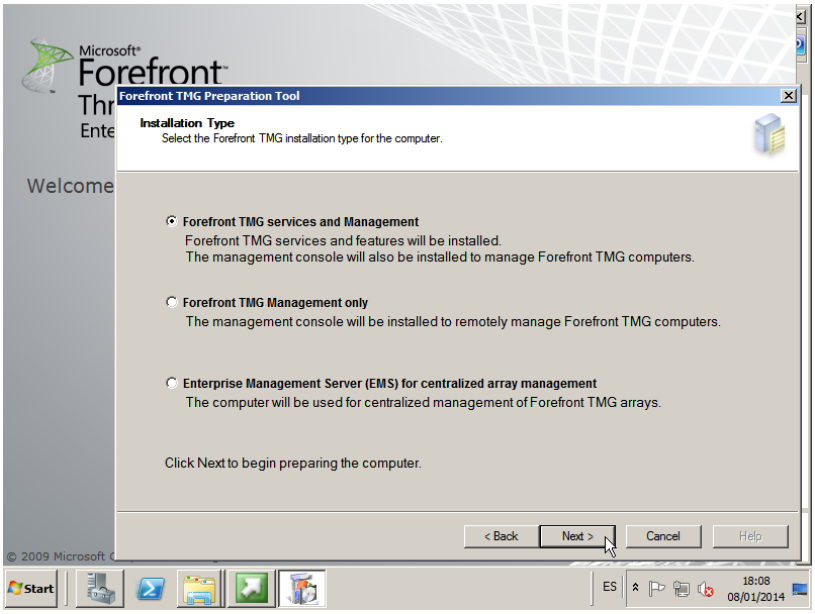
Al final se mostrara un resumen de la configuración realizada, con lo que el proceso de configuración estará completo. Al volver a la

ventana principal de la consola del Network Policy Server notaremos que se han agregado varias configuraciones, bajo “RADIUS Clients” estará el cliente que hemos agregado, igualmente bajo “Policies” encontraremos en “Connection Request Policies” y “Network Policies” las nuevas políticas creadas en donde podremos deshabilitarlas, modificarlas o eliminarlas.

5.4 PROCESO DE INSTALACIÓN Y CONFIGURACIÓN DE INSTALACIÓN Y CONFIGURACIÓN DE FOREFRONT TMG

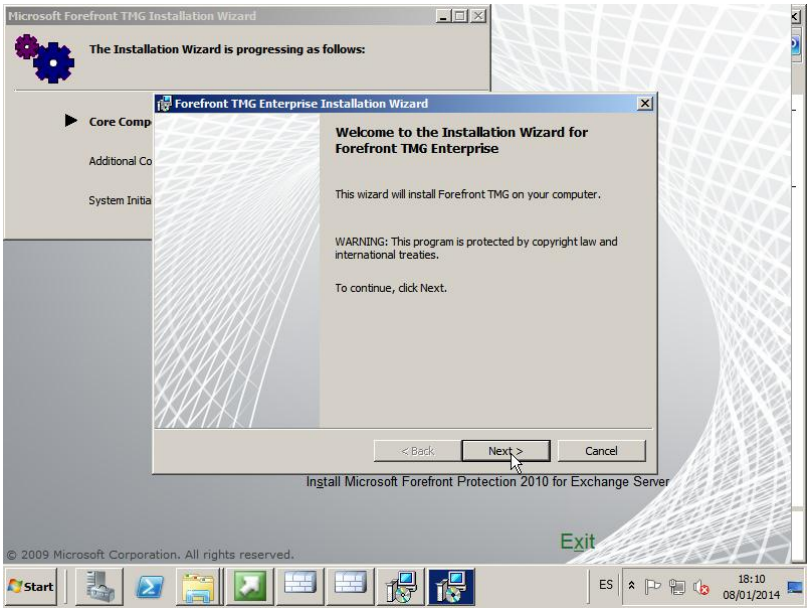
Si al insertar el disco de instalación no se ejecuta de manera automática, ingresamos al disco a través de un explorador y ejecutamos la aplicación “autorun”, se mostrara el menú de opciones para comenzar con la instalación.

Primero ejecutaremos la herramienta de preparación, esta verificará que los requisitos para la instalación estén instalados y configurados. En el asistente aceptamos los términos de la licencia y elegimos el tipo de instalación que en nuestro caso es “Forefront TMG services and Management”.



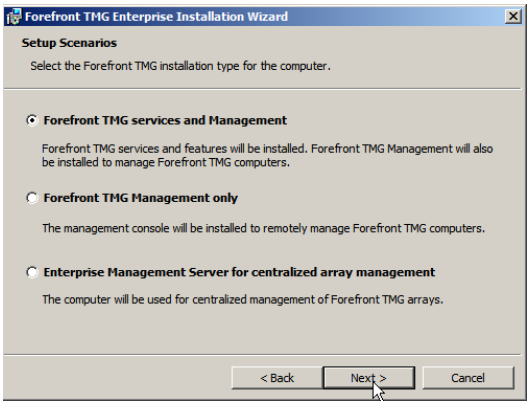
Instalación de Forefront TMG 1

Al finalizar la preparación, si se ha completado de manera correcta, se ejecutará el asistente de instalación del Forefront TGM.



Instalación de Forefront TMG 2

Luego de aceptar los términos del acuerdo de licencia e ingresar la información de registro solicitada seleccionaremos el tipo de instalación.

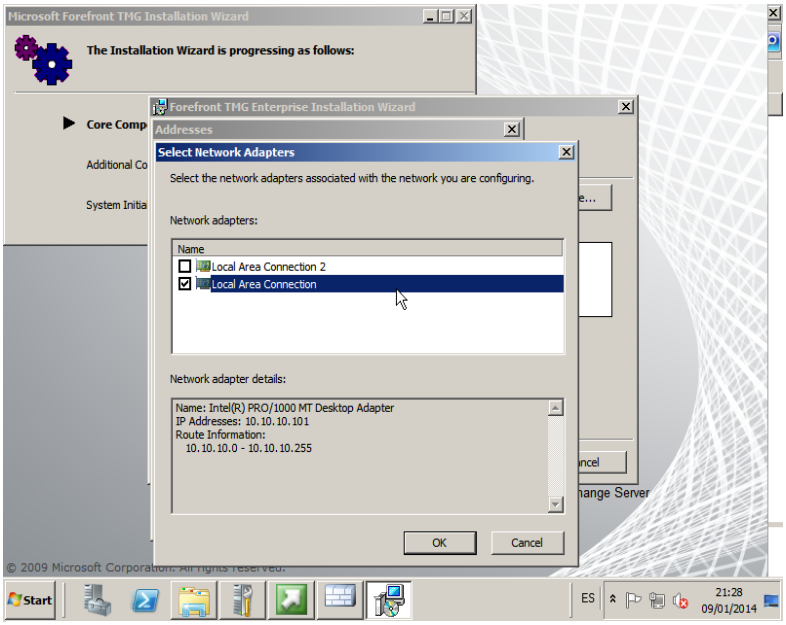


Instalación de Forefront TMG 3

En el siguiente paso podremos cambiar la ruta de instalación, dejamos la ruta predeterminada y damos clic en siguiente.

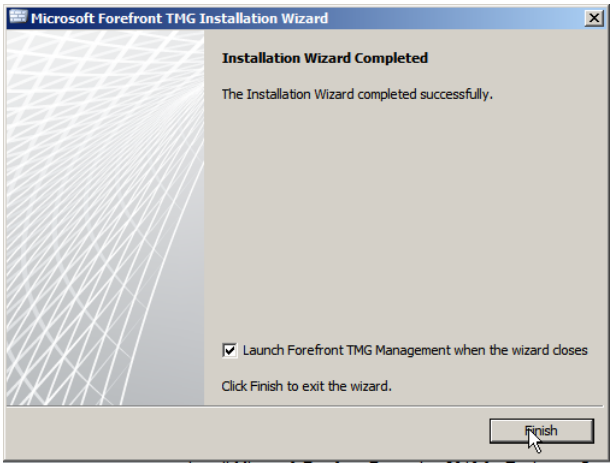
A continuación agregaremos los rangos de direcciones de nuestra red interna, para esto damos clic en “Add”. La mejor manera de completar este paso es usar la opción “Add adapter…”, de esta manera se agregarán los rangos de red asociados al adaptador que seleccionemos. Seleccionamos “Local Area Connection”, que es el adaptador a través de la cual el equipo se conecta con la red interna.

.



Instalación de Forefront TMG 4

Damos clic en siguiente y luego en instalar, con esto el proceso de instalación comenzará.



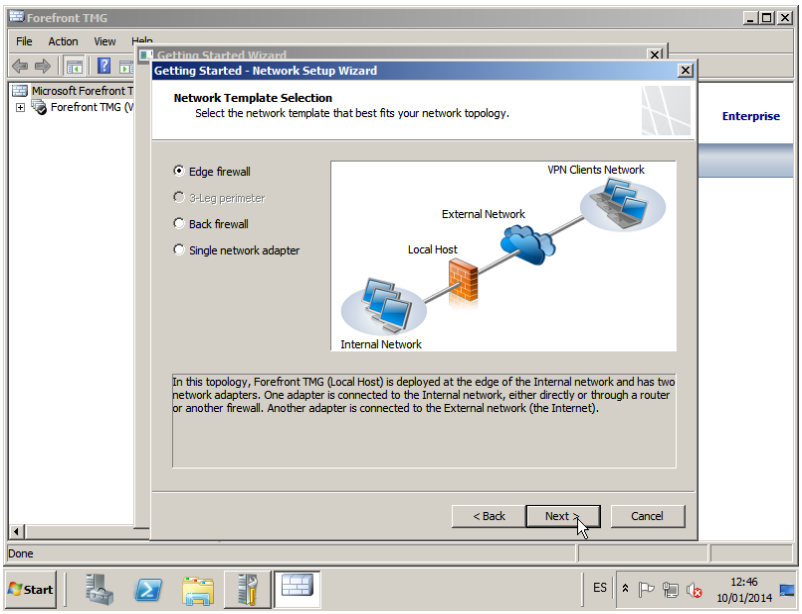
Instalación de Forefront TMG 5

Al finalizar el proceso, si no se presentaron errores durante la instalación, se mostrará una ventana indicando que la instalación ha sido completada con éxito.

Ahora podremos ejecutar el Forefront TGM Manager. La primera vez que lo ejecutemos nos mostrará un asistente para configurar aspectos básicos.

Configuración Básica de Forefront TMG 1

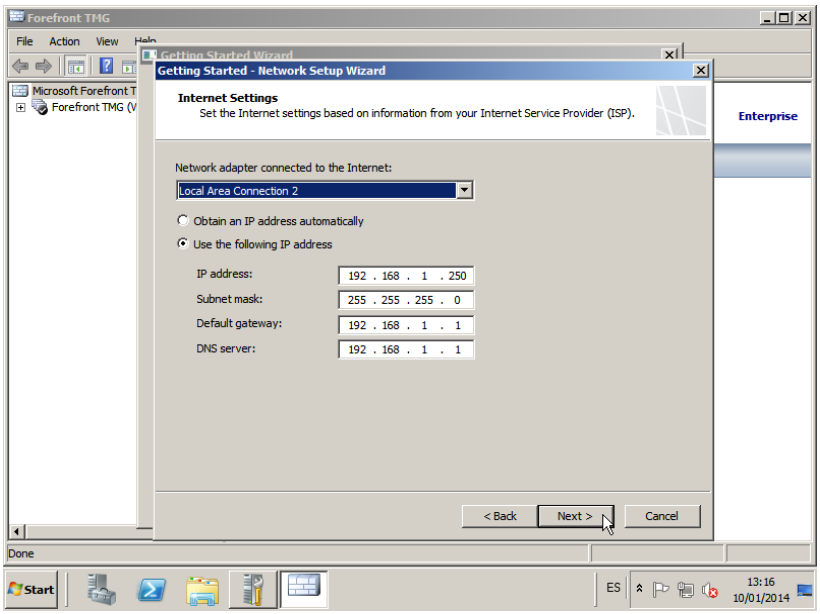
En el primer punto “Configure Network Settings”, comenzaremos eligiendo una plantilla de red de acuerdo a nuestra topología, seleccionamos “Edge Firewall”. Esta topología ubica al servidor Forefront TMG entre la red interna y la externa, en donde uno de los adaptadores de red está conectado a la red interna y otro a la red externa.



Configuración Básica del Forefront TMG 2

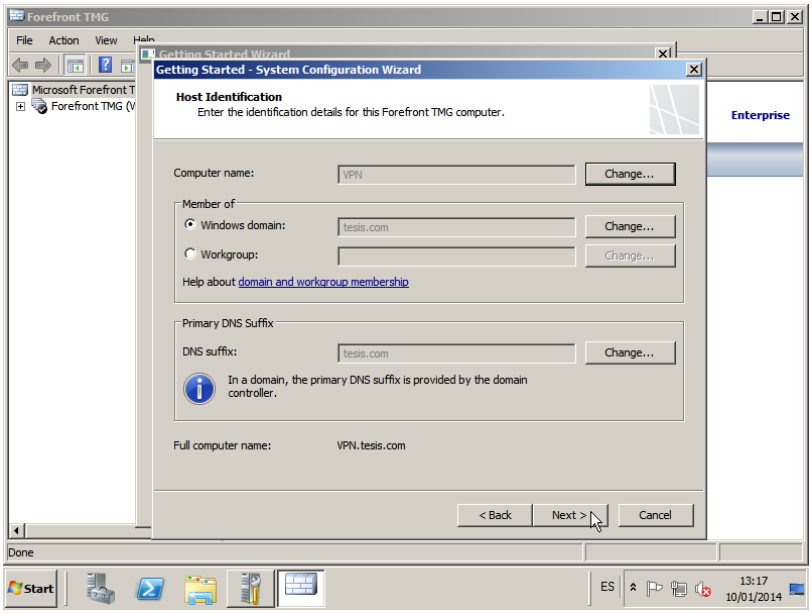
En el siguiente paso definiremos y configuraremos el adaptador que está conectado a nuestra red interna. Seleccionamos “Local Area Connection” y no hacemos ningún cambio en la configuración IP. A continuación haremos lo mismo con el adaptador de la red externa,

en donde seleccionaremos “Local Area Connection 2” que es la conexión que corresponde a nuestra red externa.



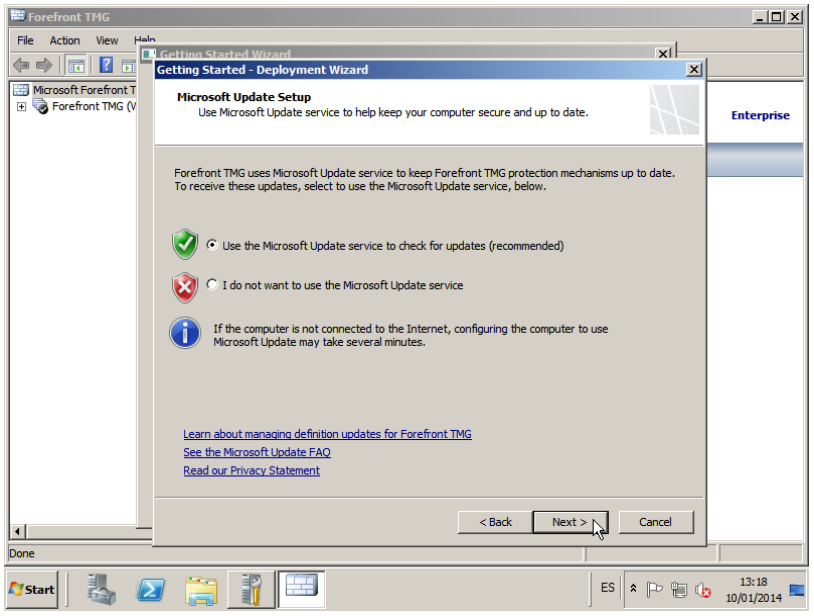
Configuración Básica de Forefron TMG 3

Con esto completaremos este punto y en el siguiente solo verificaremos la información del equipo como el nombre y dominio.



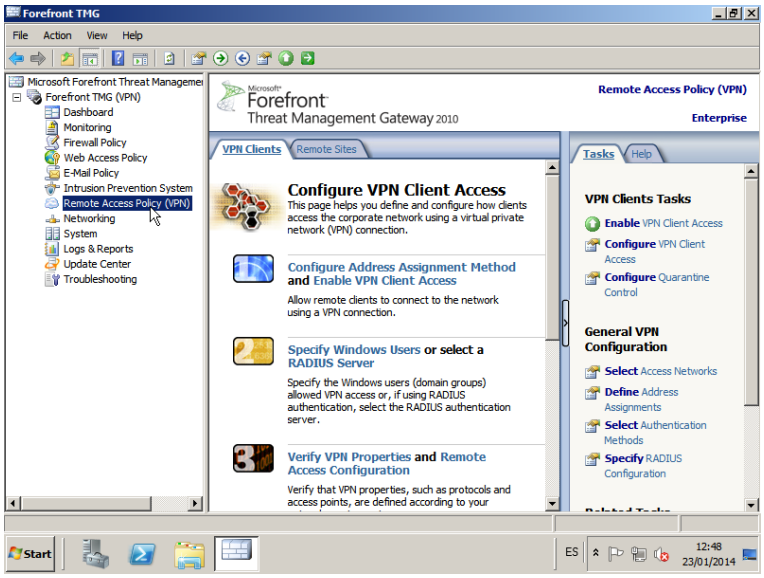
Configuración Básica de Forefront TMG 4

En el último punto “Define Deployment Options”, habilitaremos la comprobación automática de actualizaciones para el Forefront TMG.



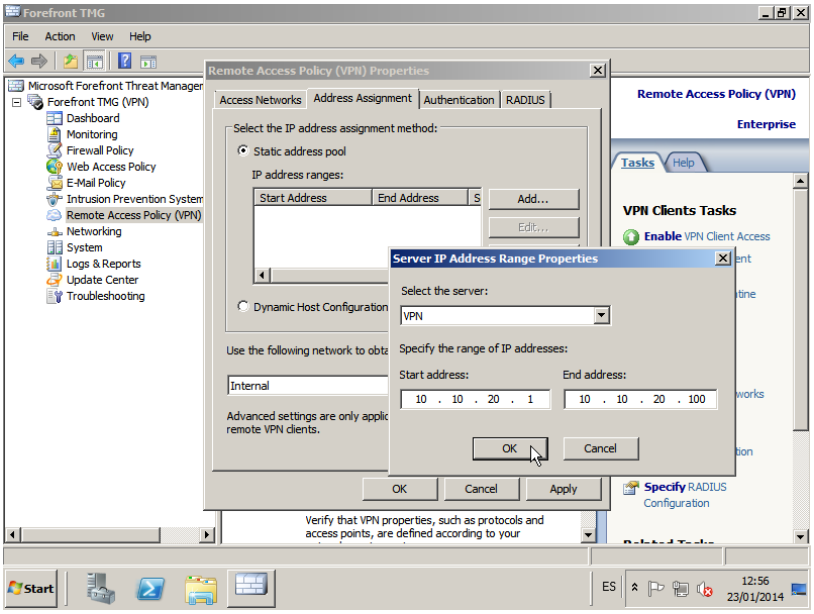
Configuración Básica de Forefront TMG 5

Luego de completar estos puntos podremos comenzar con la configuración del Forefront TMG como servidor VNP y Cortafuegos. Expandimos la sección “Forefront TMG (VPN)” en el panel izquierdo de la consola y seleccionamos “Remote Access Policy (VPN)”.



Configuración de servidor VPN/Cortafuegos 1

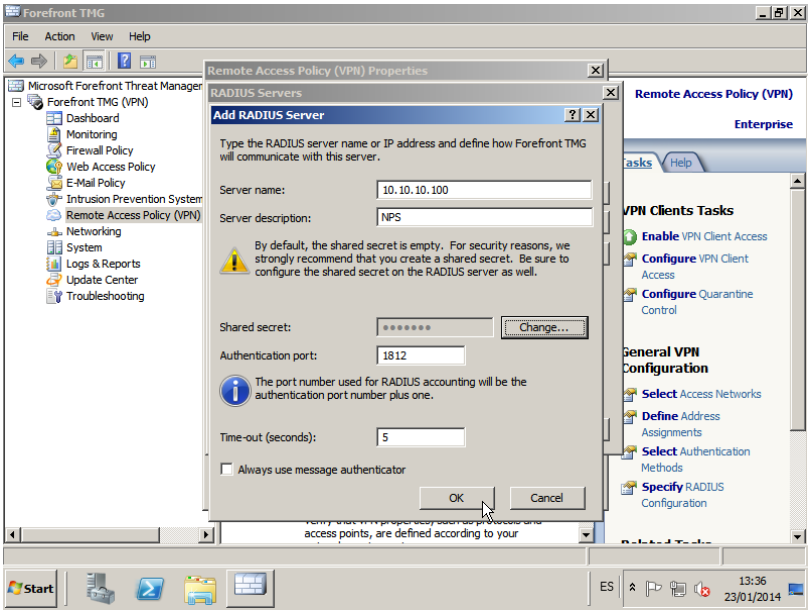
Se mostrarán varios puntos a configurar para habilitar el acceso de clientes VPN. En el primer punto configuraremos el método de asignación de direcciones IP para los clientes VPN. Damos clic en “Add…” y definimos el rango de direcciones 10.10.20.1 - 10.10.20.100.



Configuración de servidor VPN/Cortafuegos 2

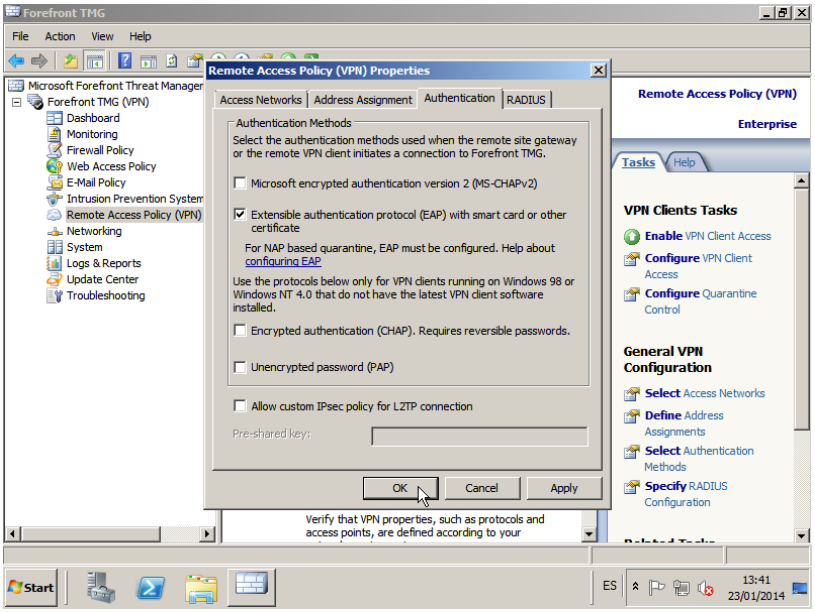
En el siguiente punto configuraremos el servidor RADIUS que se usara para autenticar a los usuarios VPN. Marcamos la casilla “Use RADIUS for Authentication” y damos clic en el botón “RADIUS Servers…”

Damos clic en el botón “Add…” para agregar un nuevo servidor RADIUS. En el campo “Server Name” escribimos en nombre DNS o la dirección IP de nuestro servidor RADIUS, y en “Shared Secret” damos clic en “Change” para ingresar la misma clave pre-compartida que usamos en la configuración del servidor RADIUS. Damos “OK” para regresar a la ventana anterior.



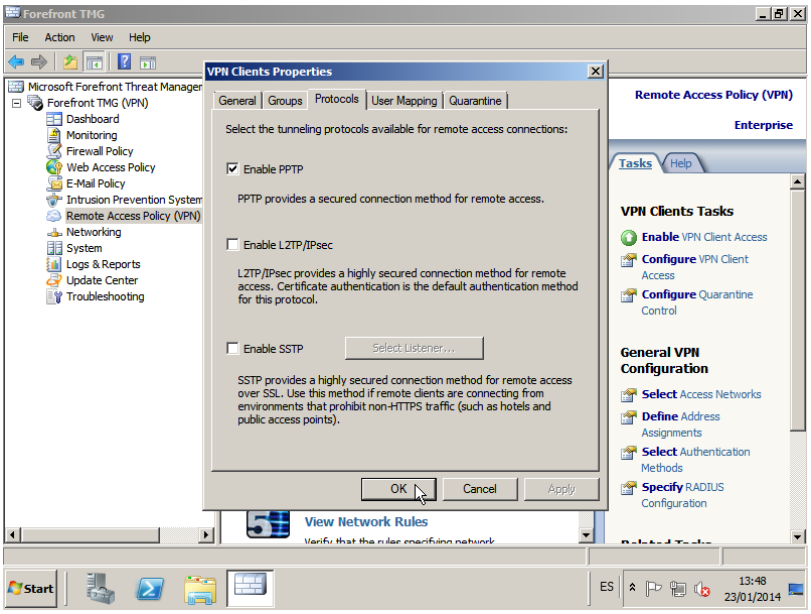
Configuración de servidor VPN/Cortafuegos 3

Vamos a la pestaña “Authentication” y dejamos solo la casilla de autenticación EAP habilitada, deshabilitamos las demás.



Configuración de servidor VPN/Cortafuegos 4

En el siguiente punto primero configuraremos los protocolos de túnel VPN admitidos para la conexión de los clientes, seleccionamos PPTP y deshabilitamos los demás.



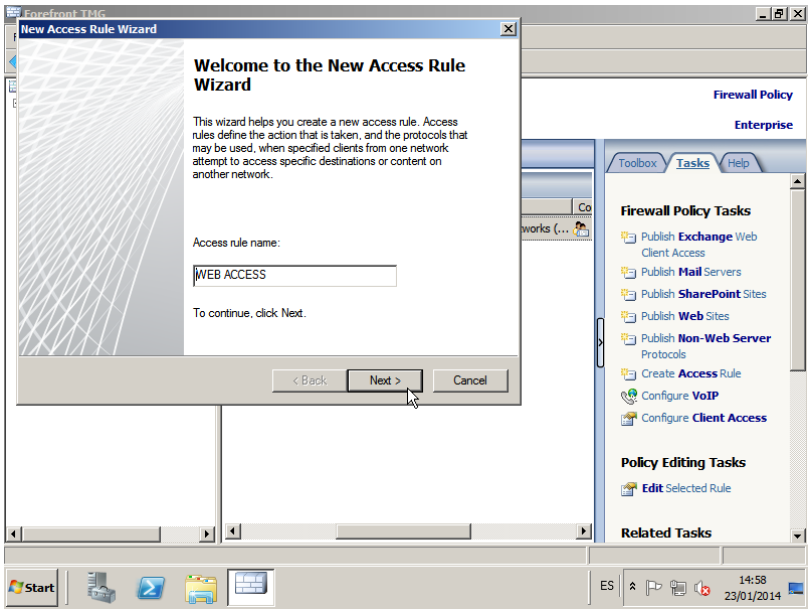
Configuración de servidor VPN/Cortafuegos 5

En la siguiente opción de este punto, “Remote Access Configuration”, verificamos que la red externa este seleccionada como la única red desde las que los clientes pueden iniciar conexiones VPN.

Finalmente, en el punto 4, configuraremos las reglas de acceso del cortafuegos para especificar los protocolos permitidos a través de conexiones VPN. Agregaremos una regla que permita a los clientes

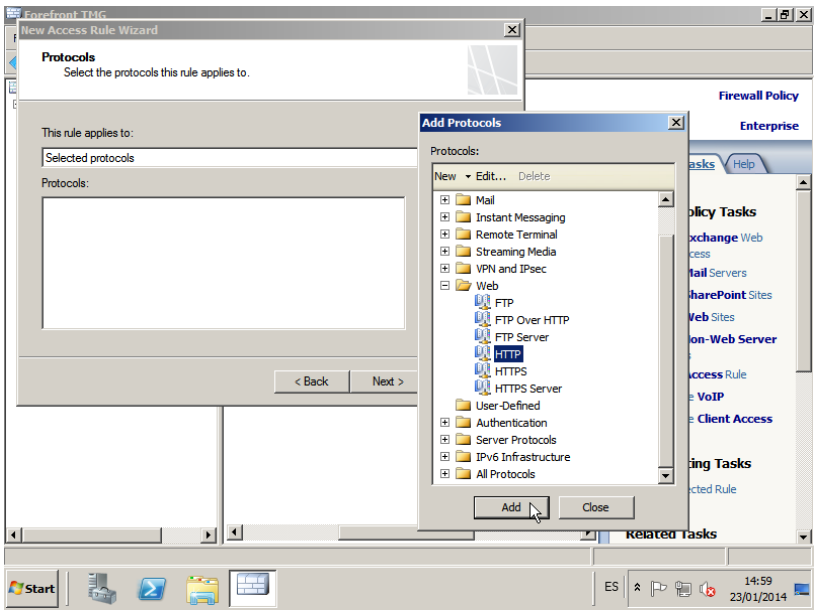
VPN conectarse a un servidor web, por lo que permitiremos el protocolo HTTP.

Damos clic derecho en Firewall Policy, en el submenú “New” damos clic en “Access Rule…”. Se abrirá el asistente para creación de reglas de acceso.



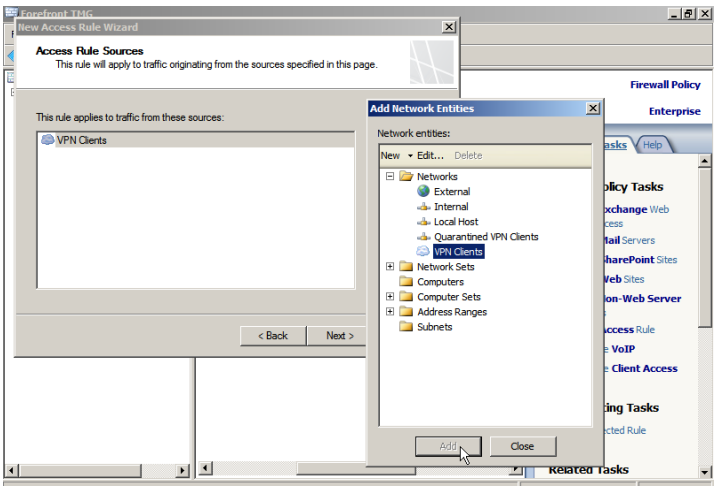
Configuración de servidor VPN/Cortafuegos 6

Escribimos el nombre con el que identificaremos a la regla que estamos creando y damos clic en siguiente. En la siguiente ventana seleccionamos la acción que se tomara cuando las condiciones de la regla se cumplan. Seleccionamos “Allow”. A continuación agregaremos los protocolos sobre los que se aplicara la regla.



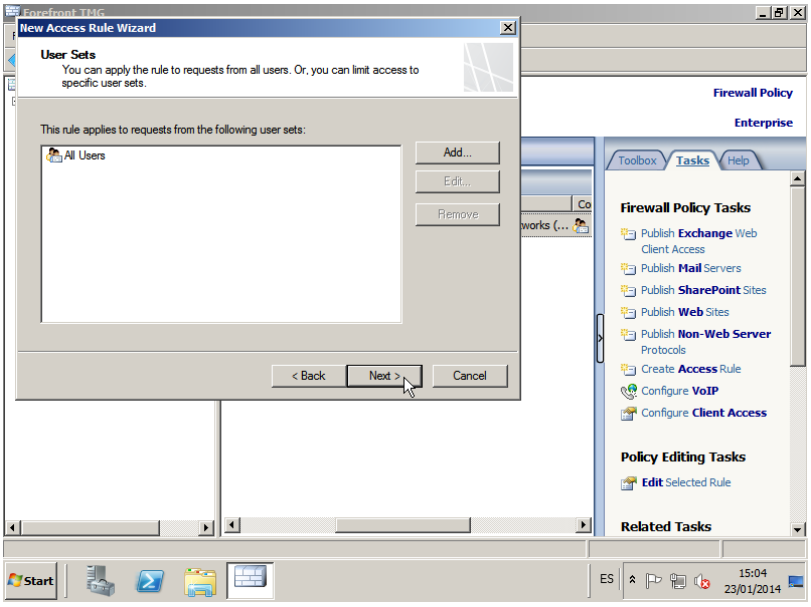
Configuración de servidor VPN/Cortafuegos 7

Los siguientes pasos nos permitirán elegir el origen y el destino del tráfico para los cuales será aplicada la regla. Seleccionamos “VPN Clients” como origen y “Internal” como destino.



Configuración de servidor VPN/Cortafuegos 8

Como último paso podremos seleccionar a que usuarios específicos queremos aplicar la regla o si se aplicará a todos los usuarios.

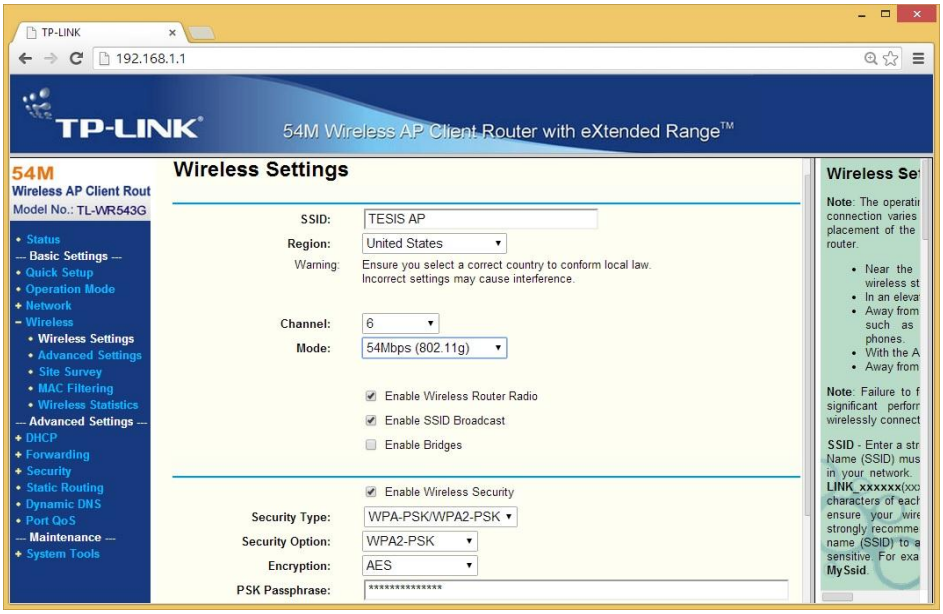


Configuración de servidor VPN/Cortafuegos 9

Finalizamos el asistente y con esto la regla de acceso estará creada. Finalmente regresaremos a la opción “Remote Access Policy (VPN)” y en el panel derecho damos clic en “Enable VPN Client Access”.

Habilitando el acceso a clientes VPN

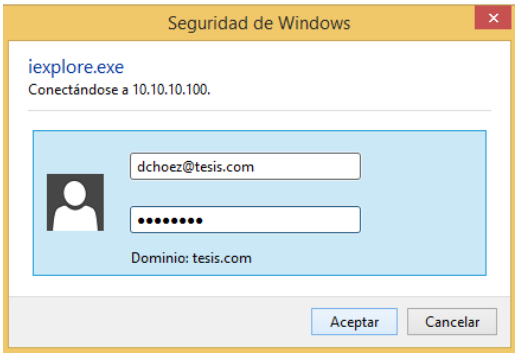
5.5 CONFIGURACIÓN DE PUNTO DE ACCESO INALÁMBRICO



Configuración de Punto de Acceso Inalámbrico

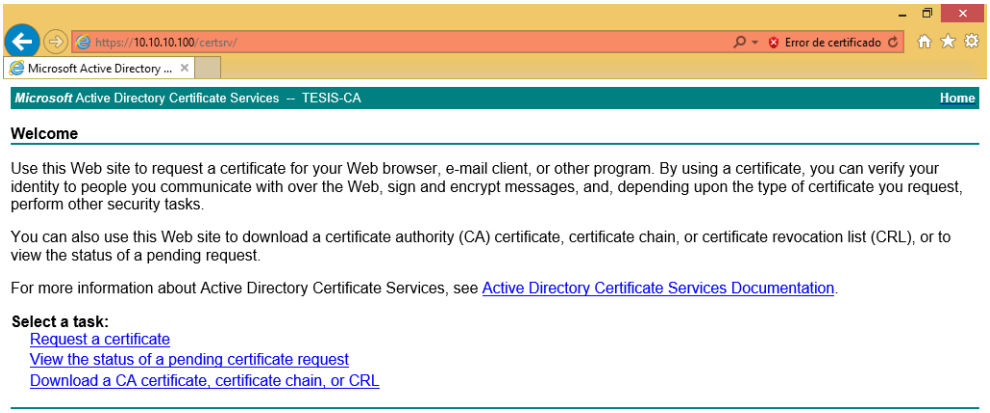
5.6 PROCESO DE CONFIGURACIÓN DE DE VPN EN EL CLIENTE

Accedemos a través del Internet Explorer a la dirección https://10.10.10.100/certsrv, se nos solicitará usuario y contraseña para acceder al sitio. Ingresamos el usuario para el cual queremos obtener un certificado.



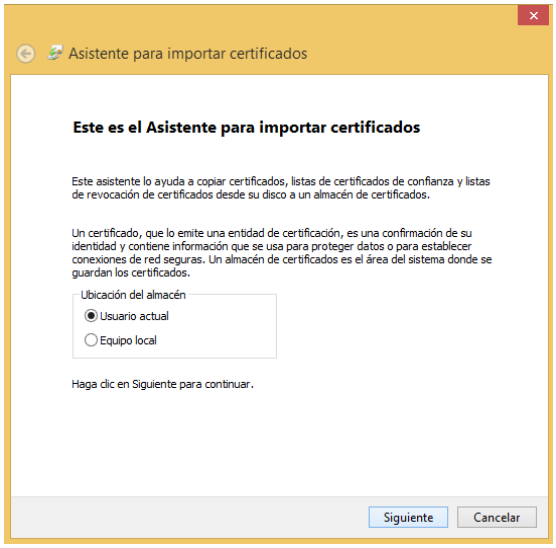
Instalación de certificados digitales en el cliente 1

Primero instalaremos el certificado del CA, esto permitirá que el equipo pueda identificar y confiar en los certificados emitidos por esta autoridad de certificación. Damos clic en “Download a CA certificate, certifícate chain, or CRL”



Instalación de certificados digitales en el cliente 2

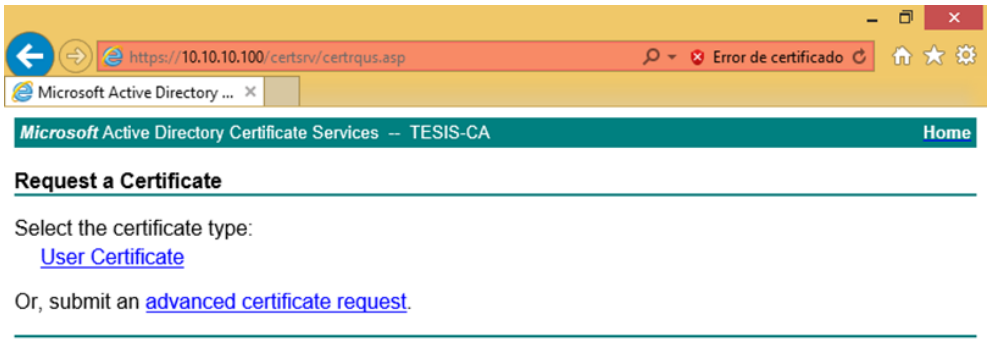
Damos clic en “install this CA certificate” y elegimos guardar el certificado. Damos clic derecho en el archivo descargado y seleccionamos “Instalar certificado”. Se abrirá el asistente para importar certificados.



Instalación de Certificados Digitales en el cliente 3

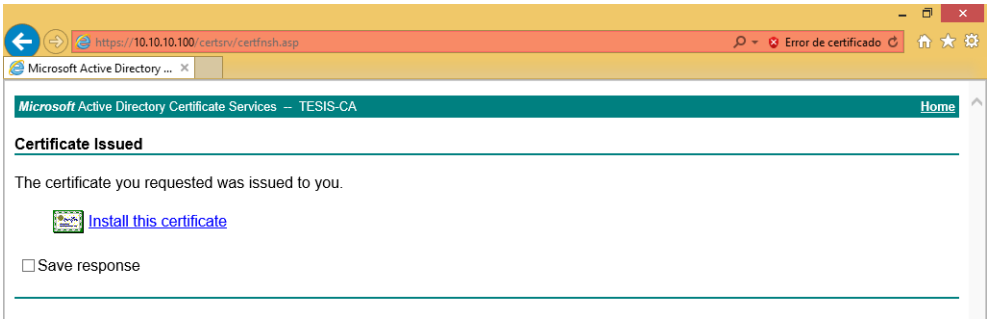
Seleccionamos como ubicación del almacén “Usuario actual” y en el siguiente paso dejaremos que Windows seleccione automáticamente el almacén donde se guardará el certificado. Al dar clic en siguiente se mostrará un mensaje confirmando la correcta importación del certificado y el certificado del CA se habrá agregado a las entidades certificadoras de confianza.

Volvemos a ingresar a la dirección https://10.10.10.100/certsrv, y esta vez elegimos la opción “Request a certificate”.



Instalación de Certificados Digitales en el cliente 4

Seleccionamos “User Certificate” y a continuación “submit”, Durante este proceso es posible que se nos solicite confirmación para que el sitio web realice operaciones en nuestro nombre, aceptamos para continuar.

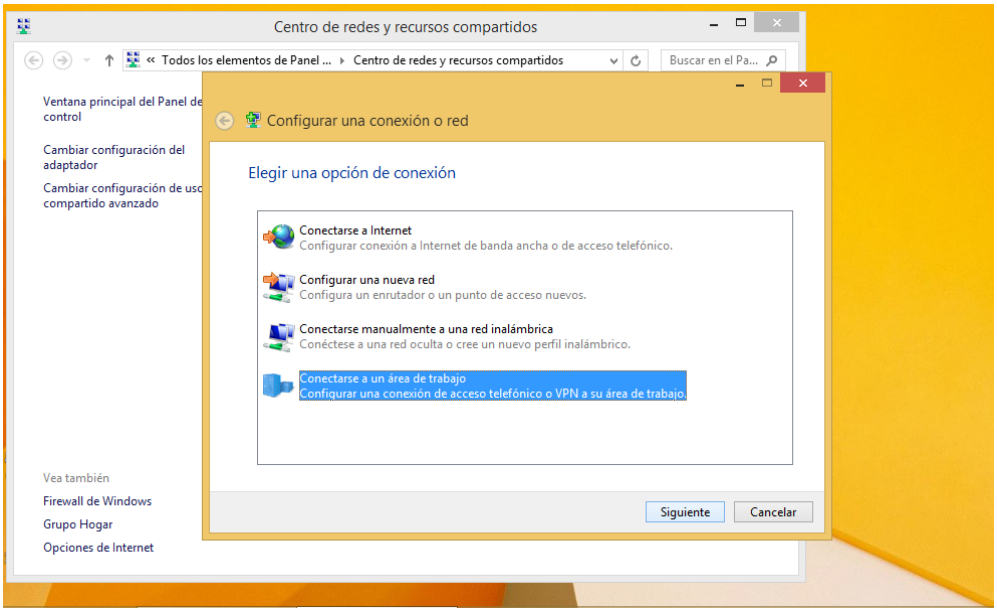


Instalación de Certificados Digitales en el cliente 5

Finalmente, damos clic en “Install this certificate” para que el certificado se instale automáticamente en el equipo.

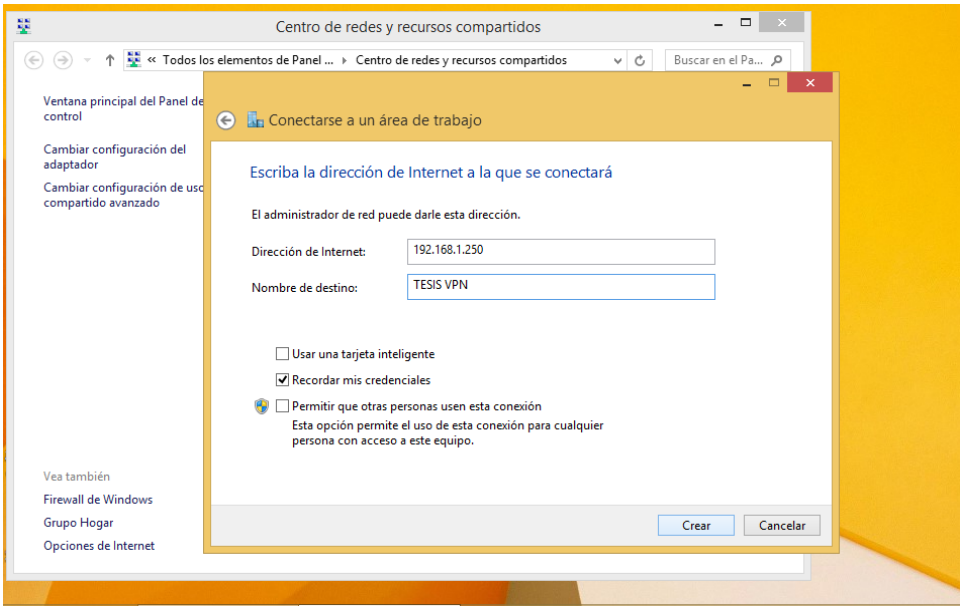
Con el certificado de usuario en el equipo ya podemos autenticarnos para establecer la conexión VPN.

Abrimos el Centro de redes y recursos compartidos y damos clic en “Configurar una nueva conexión o red” para comenzar con la configuración de la conexión VPN.



Configuración de VPN en el cliente 1

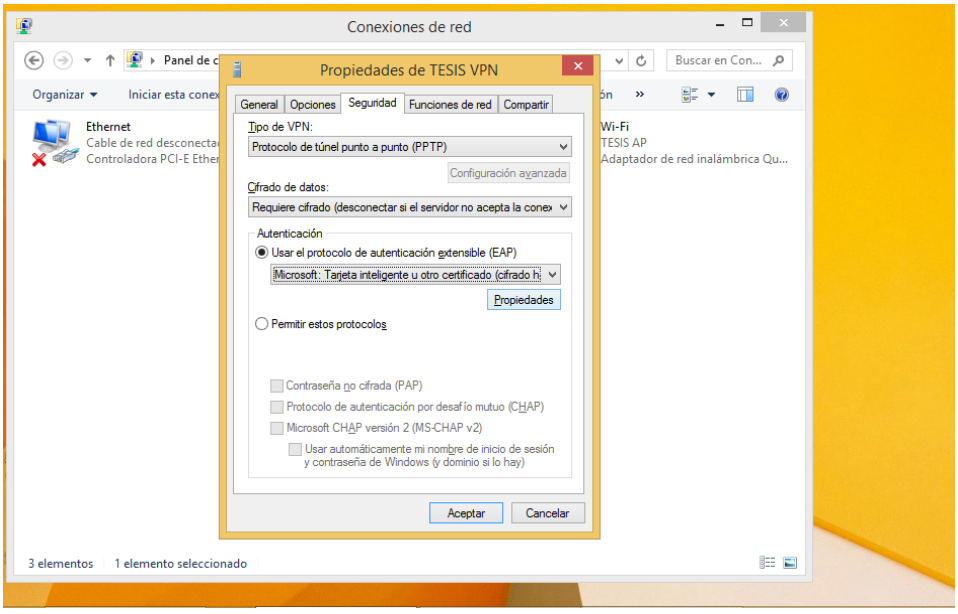
En las opciones de conexión seleccionamos “Conectarse a un área de trabajo” y luego “Usar mi conexión a Internet (VPN)”. Se nos solicitará ingresar la dirección IP del servidor VPN y un nombre para identificar la conexión. Luego damos clic en crear, con lo que se cerrara el asistente.



Configuración de VPN en el cliente 2

En Conexiones de Red se habrá creado la nueva conexión con el nombre que elegimos, le damos clic derecho y seleccionamos propiedades para configurar las opciones de la conexión VPN. Aquí podremos configurar y modificar varios aspectos de la conexión VPN pero nos centraremos en la configuración de seguridad.

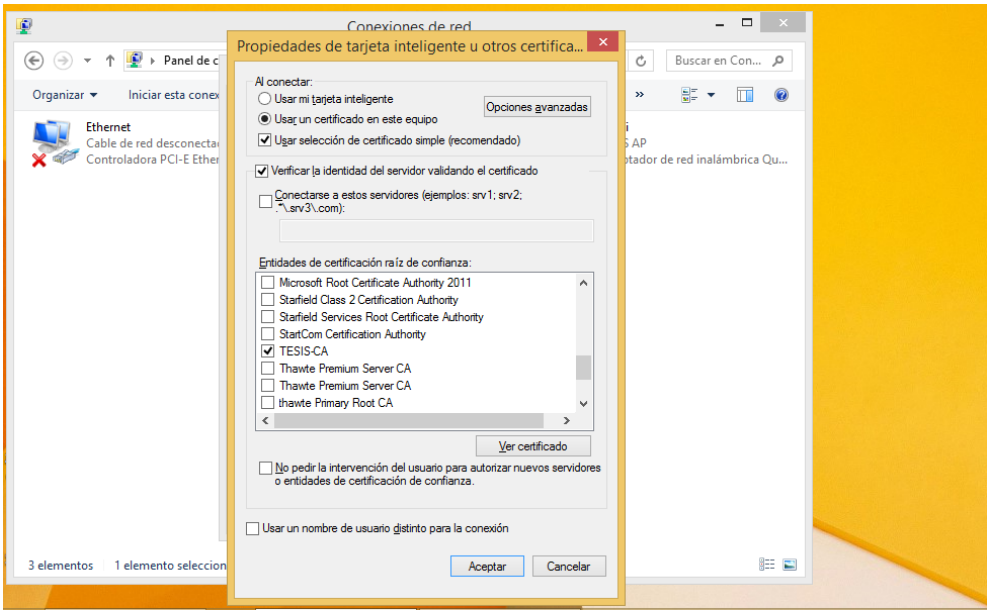
Vamos a la pestaña “Seguridad” en donde configuraremos “Protocolo de túnel punto a punto “(PPTP)” como tipo de VPN. En “Cifrado de datos” seleccionamos “Requiere cifrado”, esto indica que si el servidor no soporta cifrado la conexión no podrá establecerse. Elegimos “Usar el protocolo de autenticación extensible (EAP)” como protocolo de autenticación, y como tipo de EAP seleccionamos “Microsoft: Tarjeta inteligente u otro certificado”.



Configuración de VPN en el cliente 3

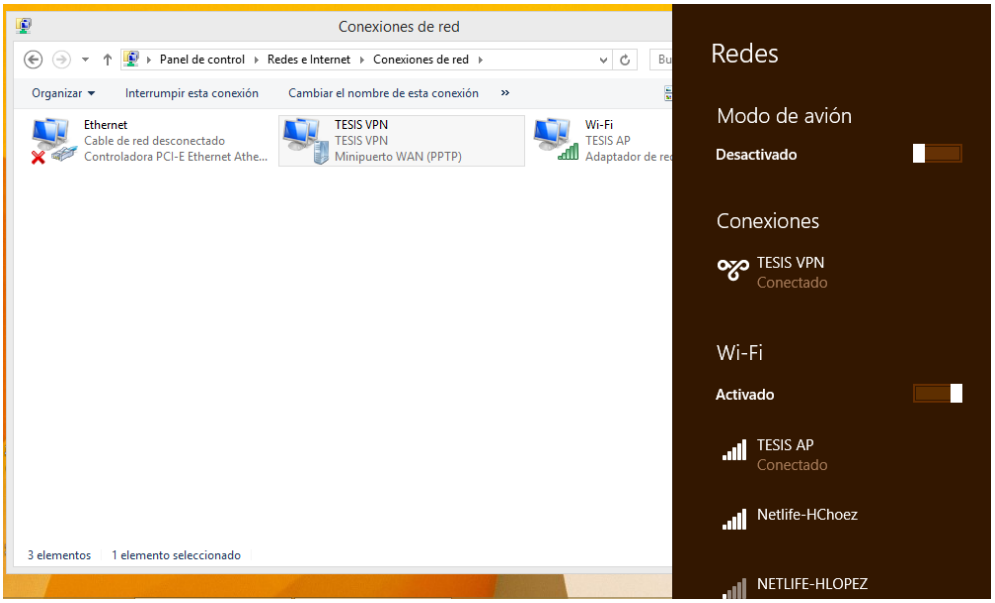
Damos clic en el botón “Propiedades” para configurar las opciones de autenticación. En la sección “Al conectar:” seleccionamos “Usar un certificado en este equipo” y marcamos la casilla “Usar selección de certificado simple”, esto permitirá que el sistema operativo elija el certificado adecuado para la conexión de nuestro almacén de certificados.

Habilitamos la casilla “Verificar la identidad del servidor validando el certificado”, y de la lista de entidades de certificación de confianza marcamos TESIS-CA, esta aparece en la lista gracias a que instalamos el certificado del CA en nuestro equipo. Damos clic en aceptar y con esto la conexión estará configurada.



Configuración de VPN en el cliente 4

Para estabelcer la conexión VPN con el servidor damos clic derecho en el icono de la conexión y seleccionamos conectar.



Configuración de VPN en el cliente 5

La conexión VPN estará establecida y para comprobar el acceso a los recursos de la red interna accederemos a un servidor web instalado en la maquina SERVER. Ingresamos la direccion IP del servidor en la barra de direcciones de navegador y si se ha realizado el proceso de manera correcta podremos ver la pagina de inicio del servidor.

Acceso a la red interna desde un cliente VPN

BIBLIOGRAFÍA

[1] Gonzáles Pérez Pablo, Sánchez Garcés Germán, Soriano de la Cámara José Miguel. Pentesting con Kali, 2013.

[2] Conocimientos Informáticos, Cuál es la diferencia entre WPA y WPA2 – Personal, http://ordenador.wingwit.com/Redes/network-security/75623.html, fecha de consulta diciembre 2014.

[3] IngeniaTIC, WiFi Protected Access (WPA), http://ingeniatic.euitt.upm.es/index.php/tecnologias/item/665-wifi-protected-access-wpa, fecha de consulta enero 2014.

[4] María Cano Baños y Natalio López Martínez, Seguridad en Redes de Comunicaciones - Práctica 2: Autenticación RADIUS y EAP, http://ocw.bib.upct.es/pluginfile.php/6726/mod_resource/content/1/Practica2.pdf, fecha de consulta enero 2014.

[5] IEEE, https://datatracker.ietf.org/doc/rfc3580/?include_text=1, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, fecha de consulta enero 2014.

[6] Microsoft TechNet, Componentes de una infraestructura RADIUS, http://technet.microsoft.com/es-es/library/cc757652(v=ws.10).aspx, fecha de consulta enero 2014.

[7] Kioskea, 802.1X/EAP, http://es.kioskea.net/contents/785-802-1x-eap, fecha de consulta enero 2014.

[8] Tecnología Hecha Palabra, EAP: Extensible Authentication Protocol, http://www.tecnologiahechapalabra.com/tecnologia/glosario_tecnico/articulo.asp?i=724, fecha de consulta enero 2014.

[9] Matthew Gast, TTLS and PEAP Comparison, http://www.opus1.com/www/whitepapers/ttlsandpeap.pdf, fecha de consulta enero 2014.

[10] Intel corporation, Descripción de la seguridad Wi-Fi, http://www.intel.com/support/sp/wireless/wlan/sb/cs-032784.htm, fecha de consulta enero 2014.

[11] ALEGSA, Diccionario de Informática – Definición de TKIP, http://www.alegsa.com.ar/Dic/tkip.php, fecha de consulta enero 2014.

[12] Jhon Fredy Herrera, AES (Advanced Encryption Standard), http://jfherrera.wordpress.com/2010/08/28/aesadvanced-encryption-standard, fecha de consulta enero 2014.

[13] Ramachandran Vivek; Backtrack 5 Wireless Penetration Testing Beginner's Guide, 2011, pag 55, 168, 173, 180.

[14] Aircrack-ng, Descripción y uso del Airplay-ng, http://www.aircrack-ng.org/doku.php?id=es:aireplay-ng , fecha de consulta julio 2014.

[15] Aircrack-ng, Descripción de Airodump-ng, http://www.aircrack-ng.org/doku.php?id=es:airodump-ng, fecha de consulta julio 2014.

[16] Fernando Andreu, Izaskun Pellejero y Amaia Lesta, Fundamentos y Aplicaciones de Seguridad en Redes WLAN, MARCOMBO S.A, 2006.

[17] Joel Snyder, NAC Deployment - A Five Step Methodology, http://www.opus1.com/nac/vendorwhitepapers/opusone_nacdeployment.pdf, fecha de consulta enero 2014.

[18] Mike Fratto, Tutorial: Network Access Control (NAC), http://m.softchoice.com/files/pdf/advisor/Tutorial_Network_Access_Control.pdf, fecha de consulta enero 2014.

[19] EC – Council, Certified Ethical Hacker, Hacking Wireless Network, 2013,