Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

Tipo de artículo: Artículo original
Temática: Tecnologías de la información y las telecomunicaciones
Recibido: 11/12/2017 | Aceptado: 22/01/2018

Montaje y control de una red Wi-Fi® asegurada a nivel empresarial con WPA2-Enterprise

Setup and control of a Wi-Fi® network at enterprise level was secured with WPA2 Enterprise

Luis Felipe Domínguez Vega

Desoft División Matanzas, Calle 151, # 29801 e/ 298 y 300 Pueblo Nuevo. Matanzas, Matanzas, Cuba

*__Autor para correspondencia__: luis.dominguez@mtz.desoft.cu, ldominguezvega@gmail.com

Resumen

El presente documento brinda los mecanismos para el montaje y monitoreo de una red Wi-Fi® en la empresa, abogando por un alto nivel de seguridad y control de todos los dispositivos referentes a dicha red inalámbrica. Se hace uso de routers inalámbricos con soporte de autenticación WPA2-Enterprise, así como la posibilidad de cambiar su firmware y sistema operativo hacia OpenWRT para una mayor eficiencia y seguridad del propio hardware. Se describe la puesta en marcha de un servidor RADIUS con el software freeradius bajo el sistema operativo GNU/Linux, en la distribución Debian en su versión stretch. También se demuestra la instalación de un servidor de base de datos ElasticSearch, con un servidor de ficheros log, Logstash y un visualizador de datos, Grafana. Se obtiene un sistema de autorización por certificado de usuario y cifrado independiente por dispositivo.

Palabras claves: certificado, control, seguridad, wifi, wpa2-enterprise.

Abstract

The present written paper offers the mechanisms for the set-up and monitoring of a network Wi-Fi in the company, supporting a high security level and control from all the referent devices to the aforementioned wireless net. WPA2-Enterprise, as well as the possibility of changing their firmware and operating system toward OpenWRT for a bigger efficiency and certainty of the own hardware does use of wireless routers with support of authentication itself. It explains him the starting of a RADIUS server with the freeradius software under the operating system GNU/Linux Debian Stretch. ElasticSearch, with a server also demonstrates the installation of a base server of data himself of card indexes

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

log, Logstash and a visual display unit of data, Grafana. A system of authorization through certificate property of user is obtained and independent encryption for device.

Keywords: *certified, control, security, wifi, wpa2-enterprise.*

Introducción

El desarrollo de la tecnología en torno a las telecomunicaciones ha permitido deshacernos de los cables casi en su totalidad a la hora de comunicar los distintos dispositivos informáticos producidos en la actualidad. En el presente documento se asume que el lector tenga conocimientos básicos acerca de las redes Wi-Fi® y la administración de servidores GNU/Linux. La seguridad es un tema polémico en la actualidad pues realmente nunca se está completamente seguro en la red, debido a que siempre existen "agujeros" por donde los malintencionados podrían aprovecharse de las vulnerabilidades de los sistemas; pero la mayor vulnerabilidad siempre recae en el propio usuario, que por un simple ejemplo, al poner una contraseña de baja complejidad no entendería que, a favor de su frase de acceso fácil de recordar, crea una brecha de seguridad que podría incurrir en graves delitos de la Seguridad Informática, como suplantación de identidad (la más común), utilización de los servicios empresariales por personas no autorizadas, entre otros.

Con la llegada de la era del *cable-less* (sin cables) se han aumentado los ataques a las redes, puesto que debido a su propia estructura, los ataques que se realizan no se puede saber con exactitud el origen de estos, debido a que todo ocurre a través de radiofrecuencia, que para determinar la ubicación exacta de un emisor o receptor es un tanto difícil, incluso utilizando equipamiento dirigido a esta faena (puesto que existen métodos, como variar la potencia de transmisión y recepción que crean falsos positivos en estos equipos). Hoy en día cualquier persona malintencionada sin conocimiento alguno del proceso interno de los protocolos de red, puede fácilmente violar su seguridad, debido a la inmensa cantidad de software realizado con este fin o con el de ser utilizado por auditores de seguridad, incluso distribuciones de GNU/Linux dedicadas explícitamente a esta faena, como lo son Kali [Linux, 2017] (anteriormente conocida como BackTrack) orientada a todo tipo de ataques y WifiSlax [seguridadwirelessnet, 2017] enfocada más a las redes Wi-Fi®.

El principal riesgo se encuentra a la hora de enfocar la seguridad en un entorno empresarial, puesto que si se implementa una red de este tipo en un entorno hogareño no se requiere un nivel tan seguro, debido a que los datos transmitidos no son de gran magnitud en su importancia. En cuanto a la empresa, donde se tramitan datos confidenciales, además de ser

objetivo de ataques, ya sea por temas de prueba, obtener información, contrarrevolución; el riesgo a que haya una vulnerabilidad es de un mayor interés, además de seguridad nacional.

El texto no incluye explicaciones muy internas sobre las herramientas, protocolos o fallas de seguridad, es responsabilidad del lector de querer indagar más en dichos temas.

Hardware instalado

Aunque la explicación en el documento es de manera genérica, para dar al lector una idea práctica sobre el hardware actual donde se encuentra desplegado todo lo expuesto en el presente trabajo, se detallan los dispositivos hardware, así como sus especificaciones.

Routers inalámbricos Se han desplegado 2 TP-Link® N600 (TL-WDR3600) brindando Wi-Fi® en las dos bandas (2.4Ghz y 5 Ghz).

Servidores Dos PC de escritorio (aunque se puede implementar en una sola PC, se mantiene lo más fiel posible a la estructura actual):

- El controlador de dominio con un procesador Intel® Core™ i7-4770 @ 3.40GHz (Aunque con un procesador AMD® o Intel® que mantenga una velocidad superior a 1.8 GHz es suficiente) y 4 Gbyte de RAM.
- El servidor RADIUS se ha virtualizado sobre Proxmox, otorgándose 512 Mb de RAM y 2 núcleos del procesador Intel® Core™ i5-4460 @ 3.20GHz. Debido al poco consumo de recursos del servidor RADIUS, se puede implementar sobre el propio controlador de dominio, pero por razones organizativas se decide su implementación de manera virtual. En un futuro se optará por la implementación de Docker para su "virtualización", lo que ahorraría más recursos al utilizar el propio kernel del Sistema Operativo (logrado igualmente con los contenedores LXC de Proxmox).

Software instalado

Todo el software utilizado se encuentra bajo licencias libres y se encuentra en el repositorio de paquetes del Sistema Operativo.

Sistema Operativo GNU/Linux Debian Stretch.

Controlador de Dominio Samba (en modo de Directorio Activo) en su versión 4.5.2+dfsg-2.

DNS Bind9 en su versión 9.10.3.dfsg.P4-10.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

RADIUS Freeradius en su versión 3.0.12+dfsg-4.

SSL OpenSSL en su versión 1.1.0c-2.

Base de Datos ElasticSearch en su versión 5.1.2.

Servidor Log LogStash en su versión 5.1.2.

Cliente Log FileBeat en su versión 5.1.2.

Visualización Grafana en su versión 4.1.0.

MÉTODOS DE SEGURIDAD EN LA WI-FI®

ES VÁLIDO ACLARAR ALGUNOS ASPECTOS RELACIONADOS CON LA SEGURIDAD DE LAS REDES WI-FI®, SI BIEN TODOS LOS QUE HEMOS CONFIGURADO UNA RED DE ESTE TIPO SIEMPRE AL LLEGAR AL APARTADO DE SEGURIDAD NOS DETENEMOS A VERIFICAR EL SOPORTE DEL SISTEMA, SE SABE QUE EXISTEN VARIOS TIPOS DE MECANISMOS DE SEGURIDAD (COMO WEP, WPA2, WPA2-ENTERPRISE, PORTALES CAUTIVOS, RESTRICCIÓN POR MAC, ETC.); REALIZANDO INVESTIGACIONES Y PRUEBAS PRÁCTICAS PARA DETERMINAR LA SEGURIDAD REAL DE DICHOS MÉTODOS, SE HA LLEGADO A LA CONCLUSIÓN QUE:

RESTRICCIÓN POR MAC ES UNO DE LOS MÉTODOS MÁS FÁCILES DE CONFIGURAR ADEMÁS DE ATACAR, PUESTO QUE EL CAMBIO DE MAC ES UNA TAREA REALMENTE SENCILLA. UN ATACANTE PODRÍA QUEDARSE “ESCUCHANDO” TODOS LOS PAQUETES EN EL AIRE E INTERCEPTAR AQUELLAS ESTACIONES QUE SE ENCUENTREN VINCULADAS AL AP Y CAMBIAR SU PROPIA MAC POR ÉSTA Y POR TANTO PASAR ESA BARRERA.

PORTALES CAUTIVOS EN EXPERIENCIA PROPIA DEL AUTOR DEL PRESENTE DOCUMENTO, HA REALIZADO UN EXTENSO ANÁLISIS DE DICHO SISTEMA, DEJANDO MUCHO QUE DESEAR EN CUANTO A LA SEGURIDAD QUE PRESENTA. EN SU OPINIÓN ES UN TANTO GRAVE LA SITUACIÓN QUE PRESENTAN, PUES DAN UNA FALSA EXPECTATIVA DE SEGURIDAD; DEBIDO A QUE EXISTEN MÉTODOS PARA SUPLANTAR EL IP Y LA MAC DE ALGUNO DE LOS CLIENTES CONECTADOS Y POR TANTO VIOLAR COMPLETAMENTE DICHO MECANISMO. HAN SURGIDO MÉTODOS INTENTANDO CONTRARRESTARLO, CÓMO EL DE EVITAR QUE LOS CLIENTES SE PUEDAN COMUNICAR ENTRE SÍ, PERO A LA HORA DE QUE MUCHOS DE ESTOS SISTEMAS SE

MONTAN SOBRE REDES ABIERTAS (SIN PROTECCIÓN, NI ENCRIPTADO) TODA LA INFORMACIÓN SE VISUALIZA A LA HORA DE UTILIZAR LAS TARJETAS WI-FI® EN SU MODO MONITOR Y POR TANTO EXTRAER TODA LA INFORMACIÓN NECESARIA PARA EVITAR ESAS BARRERAS. EN CONCLUSIÓN, ES MUY FÁCIL VIOLENTAR ESTE MECANISMO.

WEP ES UN MÉTODO DE CIFRADO EL CUAL SU RUPTURA ESTÁ MUY BIEN DOCUMENTADA [LUZ, 2010; TRAPANI, 2011; TARLOGIC, 2017], EL MÉTODO CONSISTE EN GUARDAR POR UN CORTO TIEMPO EL TRÁFICO QUE GENERA UN AP CON LOS CLIENTES UTILIZANDO ESTE NIVEL DE ENCRIPTADO; POR PROBLEMAS DE IMPLEMENTACIÓN EN EL CIFRADO SE OBTIENE LA CLAVE.

WPA2 AUNQUE ACTUALMENTE NO EXISTE UN MÉTODO PARA OBTENER LA FRASE DE ACCESO DE MANERA PASIVA (SIN INTENTAR ACCEDER AL AP), ESTE MÉTODO ES SUSCEPTIBLE A LA SUPLANTACIÓN DE AP [WIKIPEDIA, 2016; CHAUDHARY, 2014; DYNAMIC, 2011], DONDE LA PERSONA MALINTENCIONADA CREA UN AP CON EL MISMO NOMBRE (SSID) E IDENTIFICADOR (BSSID) Y POR TANTO EL CLIENTE CREE QUE ES EL AP REAL, PERO ESTA VEZ SE CONECTA SIN SEGURIDAD, A LA HORA DE UTILIZAR EL CUALQUIERA DE LOS SERVICIOS DE LA RED ES DIRIGIDO A UNA PÁGINA PREPARADA (ATAQUE DE INGENIERÍA SOCIAL) PARA PEDIR LA CONTRASEÑA DEL AP REAL. EXISTEN PROGRAMAS (COMO LINSET O EVIL TWIN) QUE ABSTRAEN A TODO USUARIO DEL CONOCIMIENTO PARA REALIZAR ESTOS ATAQUES, AUMENTANDO EL CAMPO DE ACCIÓN DE ORIGEN DE LOS ATAQUES.

WPA2-ENTERPRISE SIENDO ESCOGIDO POR EL AUTOR DEL TEXTO PARA SU IMPLEMENTACIÓN EN LA RED QUE ADMINISTRA EN SU INSTITUCIÓN, PRETENDE SER EL MÉTODO DE SEGURIDAD DE FACTO PARA UN NIVEL EMPRESARIAL DE SEGURIDAD, DEBIDO A QUE UTILIZA TODA LA POTENCIA DE ENCRIPTACIÓN DE WPA2 (DIRECTAMENTE REFIRIÉNDOSE A LA UTILIZACIÓN DE CCMP-AES) CON LA POSIBILIDAD DE UTILIZAR SUB-MECANISMOS DE AUTENTICACIÓN, EVITANDO COMPARTIR UNA MISMA FRASE DE ACCESO PARA TODOS LOS CLIENTES; EL IMPLEMENTADO POR EL AUTOR Y POR TANTO RECOMENDADO ES EL EAP-TLS. SE DARÁN LAS PAUTAS NECESARIAS PARA LA IMPLEMENTACIÓN DEL EAP-TTLS ADEMÁS PARA CASOS NECESARIOS.

- **EAP-SIM** AUNQUE NO SE ABORDA EN EL PRESENTE DOCUMENTO, ES UN MÉTODO QUE BASA SU SEGURIDAD SOBRE LAS CLAVES PRIVADAS ALOJADAS EN LAS PROPIAS TARJETAS SIM, LAS CUALES SON OFRECIDAS POR LA EMPRESA DE TELECOMUNICACIONES (EN NUESTRO CASO ETECSA).
- **EAP-TLS** UTILIZA UN CANAL CIFRADO A TRAVÉS DE CERTIFICADOS DE SEGURIDAD INSTALADOS EN EL EQUIPO CLIENTE.
- **EAP-TTLS** PARECIDO AL ANTERIOR, PERO AGREGA UNA CAPA DE TRANSPORTE SEGURO, MUY UTILIZADO PARA CUANDO NO SE USAN CERTIFICADOS, ES DECIR PARA EL USO DE USUARIO Y CONTRASEÑA.

AUNQUE ESTE MÉTODO ES SUSCEPTIBLE A ATAQUES DE AP FALSAS SIEMPRE Y CUANDO EL USUARIO NO LEE LAS ALERTAS PROPIAS DE LOS DISPOSITIVOS, ESTO OCURRE PORQUE A LA VEZ DE CONECTARSE A UN AP CON ESTE NIVEL DE SEGURIDAD, SE BRINDA UN CERTIFICADO DE SERVIDOR, INFORMANDO SOBRE LA ENTIDAD DE CERTIFICACIÓN, SI EL DISPOSITIVO CLIENTE ENCUENTRA UNA INVALIDEZ CON RESPECTO AL ENTREGADO POR EL ADMINISTRADOR DE RED PARA SU USO A LA HORA DE CONECTARSE EN EL AP, SE INFORMA, BRINDÁNDOLE AL USUARIO LA POSIBILIDAD DE IGNORAR DICHA ALERTA Y POR ENDE CONECTÁNDOSE, DE LO QUE PUDIERA DEVENIR EN QUE EL CLIENTE PRESENTE EN LA AUTENTICACIÓN SU CERTIFICADO Y POSIBILITANDO AL ATACANTE CAPTURARLO, PERO SI SE HA CREADO UN CERTIFICADO CON LAS NORMAS QUE SE EXPONDRÁN EN EL SIGUIENTE DOCUMENTO, CON UNA LLAVE DE 4096 BITS, NO SERÍA DE UTILIDAD AL ATACANTE, PUES TENDRÍA QUE, A TRAVÉS DE FUERZA BRUTA, DETECTAR LA PARTE PRIVADA DEL CERTIFICADO, LLEGANDO A SER UNA TAREA QUE LA ACTUALIDAD ES PRÁCTICAMENTE IMPOSIBLE DE DETERMINAR EN UN TIEMPO MENOR A LOS 1000 AÑOS.

DE AQUÍ SE DERIVA TAMBIÉN LA IMPORTANCIA DE TENER UNA POLÍTICA ROBUSTA DE CONTRASEÑAS EN EL DOMINIO, DEBIDO A QUE SI ADICIONA EL SOPORTE PARA USUARIO Y CONTRASEÑA EN LA AUTENTICACIÓN DE LA WI-FI® SE PODRÍA OBTENER LA CONTRASEÑA UTILIZANDO FUERZA BRUTA FÁCILMENTE SI FUERA DE BAJA COMPLEJIDAD.

Configuraciones generales

En primera instancia se debe decidir cuál será el método utilizado para la autenticación de los usuarios en la red Wi-Fi®, utilizando como protocolo de seguridad WPA2-Enterprise. Se recomienda por lo comentado anteriormente la utilización de EAP-TLS, además de si se requiere de autenticación de usuario y contraseña, EAP-TTLS, utilizando el controlador de dominio como origen de los datos.

Configurando el servidor de dominio *samba*

En el caso de que tengamos la necesidad de una autenticación de usuario y contraseña para conectarse al AP, tendríamos que instalar un servidor Samba en modo de *Active Directory*, de esta manera actuará como un servidor DNS, Kerberos y LDAP, así como los comunes en un controlador de dominio de Microsoft® Windows™ (la decisión acerca de la utilización de un servidor *samba* completo, en vez de un servidor OpenLDAP, es debido a la infraestructura de la red interna empresarial).

Primero se instala el paquete *samba*, luego con el comando (como root) *samba-tool domain provision* luego se adiciona un grupo al dominio con *samba-tool group add WiFi* el cual representará los usuarios con permisos de acceso a la Wi-Fi® adicionándolos con *samba-tool group addmembers WiFi usuario*.

Uniendo GNU/Linux al dominio de manera ligera

El autor se refiere con la unión ligera al dominio, en que se cree la cuenta de equipo en el dominio, pero que no autentique contra este los usuarios en el sistema, de esta manera se pueden usar los servicios de *winbind* para la consulta de usuarios y autenticación.

Lo primero es instalar el paquete *samba* y *winbindd* (servidor de *winbind*), luego modificamos el fichero alojado en la dirección **"/etc/samba/smb.conf"** que debería quedar parecido a lo siguiente:

```
 [global]
workgroup = DOMINIO
security = ads
realm = DOMINIO.CU
netbios name = NOMBRE_SERVIDOR
password server = IP_SERVIDOR_DOMINIO

winbind uid = 10000-20000
winbind gid = 10000-20000
winbind use default domain = yes
winbind enum users = yes
winbind enum groups = yes
domain master = no
```

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

Paso seguido se modifica **"/etc/krb5.conf"** quedando:

```
[libdefaults]
  default_realm = DOMINIO.CU
  dns_lookup_kdc = no
  dns_lookup_realm = no
  ticket_lifetime = 24h

[realms]
  DOMINIO.CU = {
    kdc = IP_SERVIDOR_DOMINIO
    admin_server = IP_SERVIDOR_DOMINIO
    default_domain = dominio.cu
  }

[domain_realm]
  .dominio.cu = DOMINIO.CU
  dominio.cu = DOMINIO.CU
```

Por último, se ejecuta el comando *net ads join -UAdministrator* y esperamos a que se cree la cuenta del servidor en el dominio. Para comprobar la unión al dominio, se puede utilizar el comando *wbinfo -u* listando todos los usuarios existentes en el dominio.

Configurando el servidor RADIUS *freeradius*

Lo primero es instalar el paquete *freeradius*, paso seguido debemos editar el fichero que contiene la configuración acerca de los clientes que se conectarán al servidor **"/etc/freeradius/3.0/clients.conf":**

```
client AP_REDES {
    ipaddr = IP.AP
    secret = "OpenWRT"

    limit {
          idle_timeout = 30
    }
}

client AP_DESARROLLO {
    ipaddr = IP.OTRO.AP
    secret = "OpenWRT"

    limit {
          idle_timeout = 30
```

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

```
    }
  }
```

Luego editamos el fichero "/etc/freeradius/3.0/sites-enabled/default" que define el sitio principal y desactivamos todos los métodos de acceso y autenticación que no sean ***eap***. Por último, se edita el fichero **"/etc/freeradius/3.0/mods-available/eap"** con todo lo referente a los certificados, al igual que el anterior se desactiva con todo lo que no sea referente a TLS o TTLS. Dichos ficheros están muy bien documentados, por lo que el usuario encontrará fluido el proceso de configuración de éstos.

Configurando la gestión de certificados de freeradius

BASÁNDONOS EN [FREERADIUS, 2014], EL PAQUETE TRAE CONSIGO UN CONJUNTO DE HERRAMIENTAS PARA LA CREACIÓN DE LOS CERTIFICADOS DE USUARIOS, SIN TENER QUE UTILIZAR DIRECTAMENTE LOS COMANDOS DE OPENSSL. EL PROCESO SE BASA EN LA MODIFICACIÓN DE VARIOS FICHEROS PARA IDENTIFICAR SU ENTIDAD A LA HORA DE LA EMISIÓN DE LOS CERTIFICADOS.

CONFIGURANDO LOS AP

EN EL CASO PRÁCTICO DE LA INSTITUCIÓN ADMINISTRADA POR EL AUTOR, LOS DISPOSITIVOS CON QUE CUENTA INCORPORAN SOPORTE PARA LA AUTENTICACIÓN DE WPA2-ENTERPRISE CON EL FIRMWARE ORIGINAL, PERO NO ES MUY ESTABLE. EL AUTOR SE INCLINA POR LA UTILIZACIÓN DE TECNOLOGÍAS LIBRES SIEMPRE Y CUANDO NO SUPONGAN UNA DISMINUCIÓN REAL DE LA SEGURIDAD O DE PRESTACIONES. PARA EL CASO DE OPENWRT (DISTRIBUCIÓN DE GNU/LINUX DEDICADA A LOS ROUTERS INALÁMBRICOS) TIENE SOPORTE COMPLETO PARA DICHO DISPOSITIVO, POR LO QUE SE DECIDE EL REEMPLAZO COMPLETO DEL FIRMWARE POR EL PRESENTADO PARA EL USO DE ESTE SISTEMA OPERATIVO (QUE EN PRUEBAS REALIZADAS SE ARGUMENTA QUE LA ESTABILIDAD DEL SERVICIO BRINDADO SOBRE ÉSTE ES ALTA)[1].

PARA LA INSTALACIÓN DE OPENWRT, BASTA CON DESCARGAR EL FICHERO DE ACTUALIZACIÓN DEL FIRMWARE DE SU PÁGINA WEB Y PROCEDER COMO UNA ACTUALIZACIÓN NORMAL DEL FIRMWARE DEL DISPOSITIVO, CON LA SALVEDAD DE QUE TODO EL SISTEMA SERÁ REMOVIDO. OPENWRT POR DEFECTO DESACTIVA LOS DISPOSITIVOS INALÁMBRICOS HASTA QUE NO ESTÉN CONFIGURADOS

[1] EXISTE OTROS SISTEMAS OPERATIVOS ORIENTADAS A DISPOSITIVOS COMO ESTOS, POR EJEMPLO, DD-WRT, PERO POR EXPERIENCIA NO MANTIENEN LA ESTABILIDAD BRINDADA POR EL ESCOGIDO POR EL AUTOR

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

CORRECTAMENTE. UNA VEZ INICIADO POR PRIMERA VEZ, EL DISPOSITIVO SE CONFIGURA CON UN IP DE **192.168.1.1**. HAY QUE TENER EN CUENTA QUE PARA AGREGARLE EL SOPORTE A OPENWRT PARA WPA2-ENTERPRISE ES NECESARIO DESINSTALAR EL PROGRAMA *WPAD-MINI* E INSTALAR SU VERSIÓN COMPLETA *WPAD*.

SE PROCEDE:

Figura 1. Autenticarse

Figura 2. Acceder a través del menú a la configuración de las interfaces inalámbricas

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

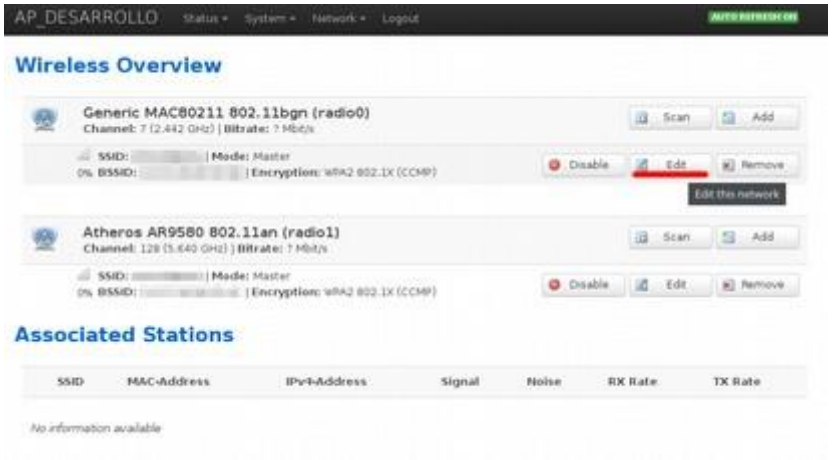

Figura 3. En la lista de interfaces editar las necesarias

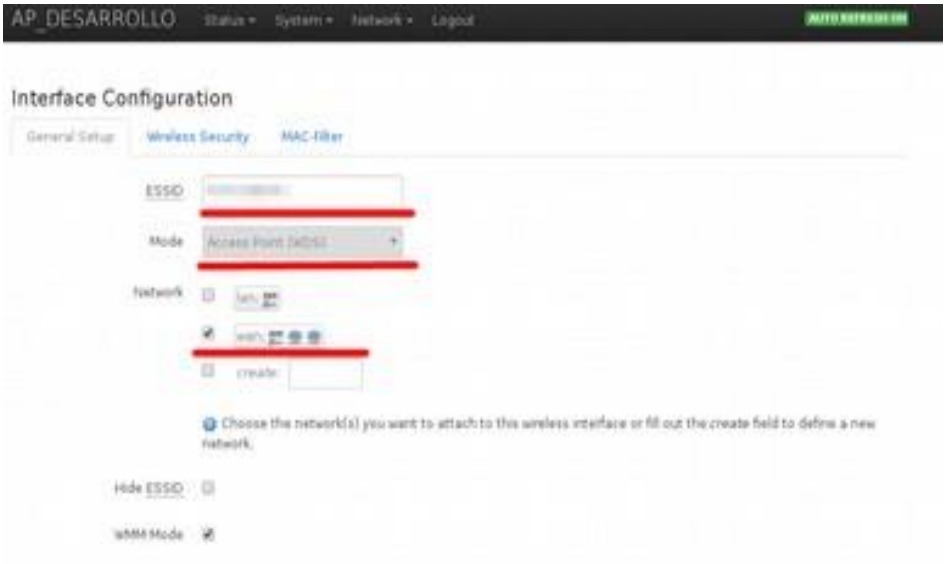

Figura 4. En la configuración general, tener en cuenta los aspectos principales

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

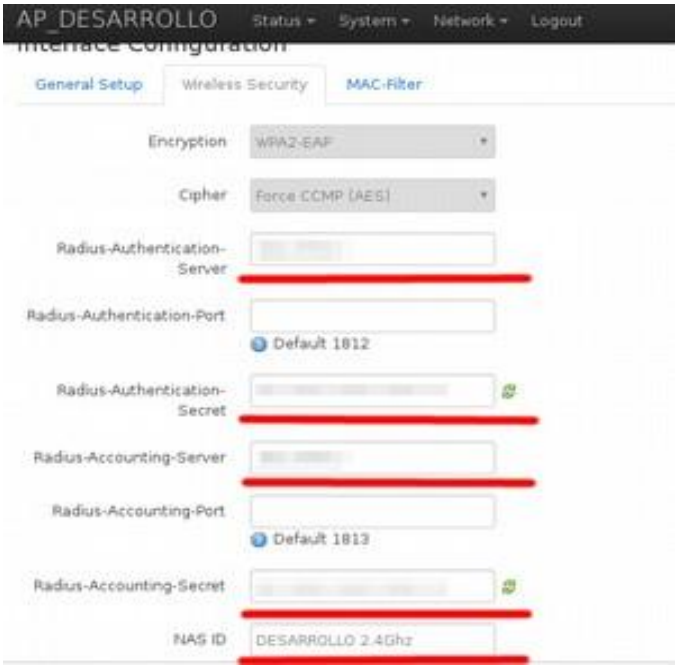

Figura 5. Configurar lo más importante, el apartado de seguridad con el servidor RADIUS

MONITOREO

LA INSTALACIÓN DEL SOFTWARE UTILIZADO PARA EL MONITOREO QUEDA FUERA DEL ÁMBITO DEL DOCUMENTO, SIMPLEMENTE AÑADIR QUE LOS PAQUETES UTILIZADOS (PARA ELASTICSEARCH, LOGSTASH, FILEBEAT Y GRAFANA) SE TUVIERON QUE DESCARGAR UTILIZANDO LA RED TOR, PUESTO QUE LOS SERVIDORES DONDE SE ENCUENTRAN ALOJADOS NO PERMITEN TRÁFICO HACIA NUESTRO PAÍS. SE INDICARÁN A CONTINUACIÓN LOS DETALLES MÁS RELEVANTES EN LA INSTALACIÓN DEL SISTEMA PARA PERMITIR AL ADMINISTRADOR DE RED TENER UNA VISUALIZACIÓN DEL ESTADO DE ESTA.

ELASTICSEARCH

LA INSTALACIÓN POR DEFECTO TIENE TODO LO NECESARIO, SOLO ACLARAR QUE DICHO SERVIDOR HACE UN USO ELEVADO DE RAM, DEBIDO A SU MOTOR DE BÚSQUEDA DE TEXTO COMPLETO LUCENE.

ADEMÁS DE LO ANTERIOR SE DEBE, PARA EVITAR PROBLEMAS DE SEGURIDAD, MODIFICAR EL FICHERO **“/ETC/ELASTICSEARCH/ELASTICSEARCH.YML”** Y CERCIORARSE DE QUE EL CAMPO DE

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

CONFIGURACIÓN ***NETWORK.HOST*** CONTENGA EL VALOR **127.0.0.1** PARA EVITAR QUE ESCUCHE DE MANERA EXTERNA NUESTRO SERVIDOR DE BASE DE DATOS NO SQL.

LOGSTASH

ESTE SERVIDOR ES EL ENCARGADO DE OBTENER TODOS LOS DATOS DE LOGS DE LOS SERVIDORES Y FILTRARLOS, ADEMÁS DE ORGANIZAR SU SALIDA PARA DISTINTOS ÍNDICES EN EL SERVIDOR DE ELASTICSEARCH. PARA EL CASO REFERENTE AL ACTUAL DOCUMENTO, DEBEMOS EDITAR EL FICHERO DE CONFIGURACIÓN **"/ETC/LOGSTASH/LOGSTASH.YML"** Y CONFIGURAR EL PARÁMETRO **HTTP.HOST** CON LA DIRECCIÓN POR LA CUAL ESCUCHARÁ EL SERVIDOR. ACTO SEGUIDO SE CREARÍAN LOS FICHEROS DE CONFIGURACIÓN ESPECÍFICOS PARA CADA CLIENTE [ELASTIC, 2017].

FILEBEAT

UNA VERSIÓN LIGERA DE LOGSTASH, ESCRITA EN C, CUYA MISIÓN SIMPLEMENTE ES LEER LOS FICHEROS DE LOGS PARA ENVIARLO HACIA UN SERVIDOR, YA SEA ELASTICSEARCH O LOGSTASH; DE ESTOS SERVIDORES EL AUTOR LO CONFIGURA PARA EL ENVÍO DE TODA LA INFORMACIÓN HACIA LOGSTASH, CENTRALIZANDO TODO HACIA ESTE ÚLTIMO, EL CUÁL ES EL ENCARGADO DE SALVAR EN ELASTICSEARCH TODO ESE CONTENIDO.

GRAFANA

ES UN SERVICIO WEB DEDICADO A LA VISUALIZACIÓN A TRAVÉS DE PANELES DE LOS DATOS OBTENIDOS A TRAVÉS DE SUS ORÍGENES DE DATOS, HAY QUE TENER EN CUENTA QUE EL SOPORTE PARA LA VERSIÓN 5.X DE ELASTICSEARCH HAY QUE TENER LA VERSIÓN SUPERIOR A 4.1 DE

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 1, Enero-Marzo, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 58-73
http://rcci.uci.cu

GRAFANA. EL PROCESO DE CONFIGURACIÓN DE LOS PANELES QUEDA FUERA DEL ALCANCE DEL DOCUMENTO, EJEMPLOS INSTALADOS EN LA RED:

Figura 6. Dashboard dedicado a la señal de la red inalámbrica

Figura 7. Dashboard dedicado a los routers en general

Conclusiones

Se podría decidir si implementar o no la propuesta aquí expuesta, se podría pensar en no pasar el trabajo de tener que implementar todos los servicios, ni tener que modificar tantos archivos, pero, el día que en la red ocurra un evento de violación de seguridad, se preguntarán ¿y no se podía haber asegurado un poco más la red?

Todo el sistema se basa en instalar el software en donde mejor se use; por ejemplo, para ElasticSearch existe un software parecido a Grafana, Kibana; pero éste no fue programado con la finalidad de la visualización de datos sobre el tiempo, por tanto, se opta por la solución descrita.

Con todo el sistema instalado y funcionando con las configuraciones correctas brinda una seguridad elevada y tranquilidad al administrador de red, además de aportarle la posibilidad a este del conocimiento del estado de la red en todo momento, guardando en ElasticSearch todo el historial para casos donde se requiera consultar datos pasados.

Desde la creación del presente documento hasta la fecha en que usted se encuentra leyéndolo, deben haberse creado otros mecanismos que fortalezcan ligeramente lo que aquí se expone; el autor con la propuesta presentada espera que el lector encuentre un nuevo campo de investigación y punto de vista de ver la seguridad, donde la investigación constante y la propia prueba de la red es la única que “asegura” un nivel elevado en cuanto a evitar sucesos indeseados en la red.

Referencias

Chaudhary, Shashwat. 2014. Evil Twin Tutorial - Kali Linux Hacking Tutorials. [Online] Julio 14, 2014. http://www.kalitutorials.net/2014/07/evil-twin-tutorial.html.

Dynamic, Technic. 2011. Hacking WPA 2 Key - Evil Twin Method (No Bruteforce). [Online] Diciembre 28, 2011. https://www.youtube.com/watch?v=R6I0GeEh22c.

Elastic. 2017. Configuring Logstash | Logstash Reference [5.1] | Elastic. [En línea] 2017. https://www.elastic.co/guide/en/logstash/current/configuration.html.

FreeRADIUS. 2014. Deploying RADIUS: Production Certificates. [En línea] 2014. http://deployingradius.com/documents/configuration/certificates.html.

Linux, Kali. 2017. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. [Online] 2017. https://www.kali.org/.

Luz, Sergio De. 2010. Cómo Hackear una red WiFi con encriptación WEP. [En línea] 6 de Octubre de 2010. https://www.redeszone.net/seguridad-informatica/hackea-una-red-wifi-protegida-con-wep/.

seguridadwireless.net. 2017. Live Wifislax. [En línea] 2017. http://www.wifislax.com/.

Tarlogic. 2017. Cómo hackear wifi y redes wifi WEP y WPA con Acrylic en windows. [En línea] 2017. https://www.tarlogic.com/programas-wifi/acrylic-wifi/hack-de-contrasenas-wifi-wep-y-wpa-con-acrylic-en-windows/.

Trapani, Gina. 2011. How to Crack a Wi-Fi Network's WEP Password with BackTrack. [Online] Octubre 2011. http://lifehacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack.

Wikipedia. 2016. Evil twin (wireless networks) --- Wikipedia, The Free Encyclopedia. [Online] 2016. https://en.wikipedia.org/w/index.php?title=Evil_twin_(wireless_networks)&oldid=745018078.