2017

TRABAJO DE LABORATORIO Nº 2

Configuración básica de seguridad de redes Wireless

ACTIVIDAD DE FORMACION PRACTICA

1. Formación experimental (laboratorio).

OBJETIVOS

1. Identificar las principales amenazas y vulnerabilidades de las comunicaciones de datos que deben considerarse en implementaciones de redes IEEE.802.11x.
2. Incorporar habilidades para configurar dispositivos de acceso e interfaces de hardware (adaptadores) en redes WLAN.
3. Comprender el enfoque recomendado por los estándares de gestión de seguridad de la información para establecer políticas de comunicaciones seguras y hacerlas efectivas mediante los servicios de seguridad adecuados en redes Wireless LAN (WLAN).

CONOCIMIENTOS PREVIOS

1. Términos y definiciones de seguridad de la información contenidos en ISO/IEC 27001 e ISO/IEC 27002 (17799), tecnología WiFi, IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.11ac, IEEE802.11i, protocolos WEP y WPA, principales amenazas y vulnerabilidades de los ambientes WLAN.
2. Recomendaciones de seguridad Wi-Fi dadas por: http://www.wi-fi.org/discover-wi-fi/security.
3. Se sugieren las lecturas de los siguientes artículos:

   http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

   http://article.sciencepublishinggroup.com/html/10.11648.j.ajomis.20170201.11.html

   https://pdfs.semanticscholar.org/1b0d/e694f8ac13396df9fc8a821164d95dcd04f5.pdf

   http://www.cs.ucf.edu/~czou/CNT4704-15/DSCI_Seminar.pdf

TAREAS PRELIMINARES (EXTRA CLASE)

1. **Elaborar un listado de posibles amenazas a la seguridad de WLAN IEEE 802.11.**
2. **En base a las amenazas consideradas, identificar las vulnerabilidades a las que está expuesta la red del estudio de caso.**

(**Considerar los documentos sugeridos, de manera no excluyente**).

MATERIAL NECESARIO

1. Simulador Cisco Packet Tracer Student.

2. En caso de desplegarse el laboratorio real:
   a. Un Access Point (AP) marca Cisco / Linksys modelo WRT54 o similar, con software y manual.
   b. 5 PCs de escritorio con cable de red o adaptador wireless.
3. Resumen de amenazas y vulnerabilidades en redes WLAN:
   a. Archivo ***security-vulnerabilities-wireless-lan-technology_1629 SANS.pdf***

      https://www.sans.org/reading-room/whitepapers/wireless/security-vulnerabilitieswireless-lan-technology-1629
4. Guía de configuración de Access Point Cisco Linksys WRT54G:
   a. Archivo ***secure_linksys_wrt54g.pdf***
      http://www.infosecwriters.com/text_resources/pdf/secure_linksys_wrt54g.pdf
      a. Guías http://www.linksys.com/mx/search?text=WAP54G
      b. Documento: ***Wi-Fi Protected Access 2 (WPA 2) Configuration Example***, en

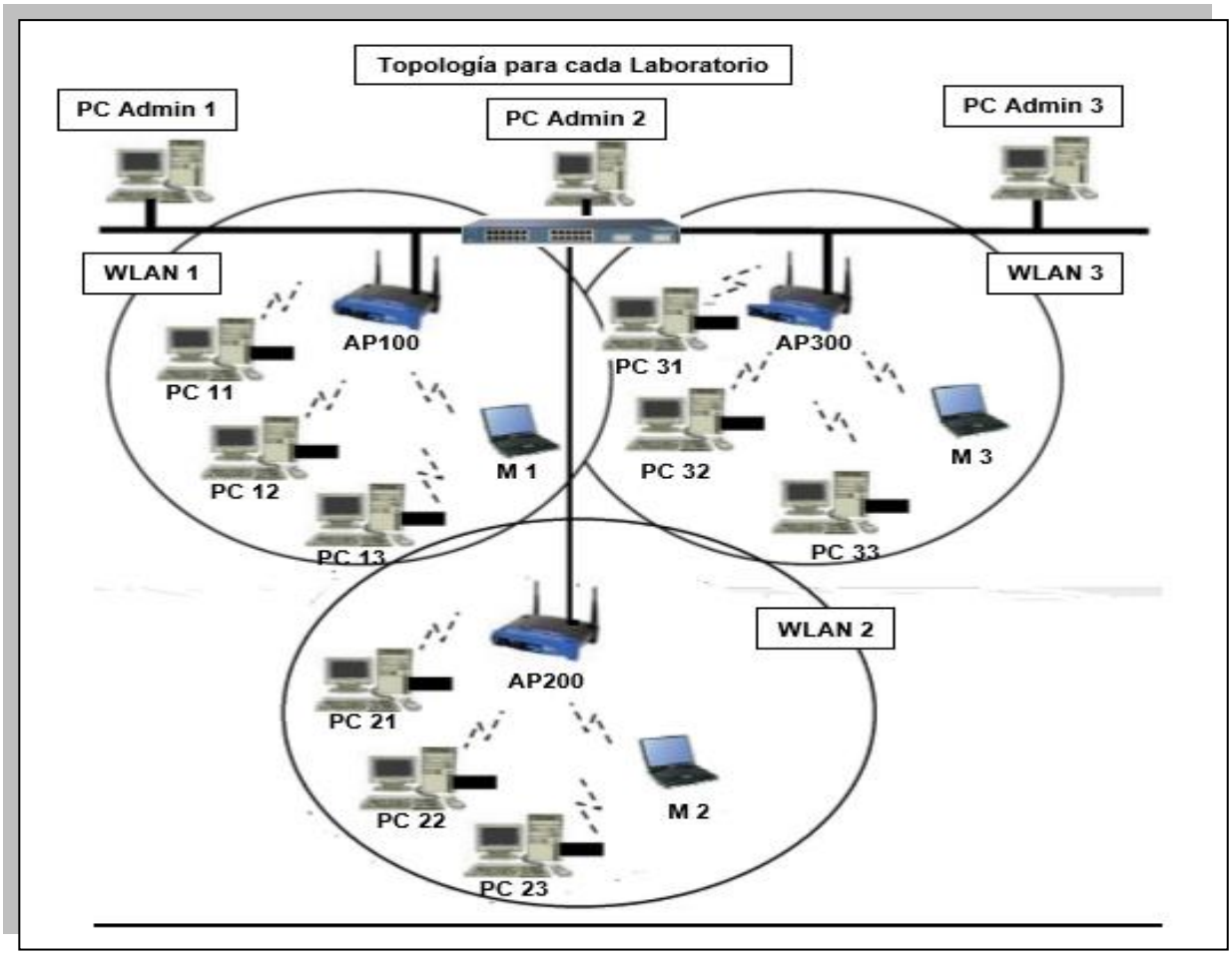
         http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/67134-wpa2-config.html

DESCRIPCION

Este trabajo requiere del desarrollo de tareas previas, según se enuncia en el punto **TAREAS PRELIMINARES EXTRA CLASE**. Luego, en clase será desarrollado en grupo de hasta cuatro alumnos en una PC con acceso al laboratorio WLAN y **evaluado individualmente** mediante demostraciones de funcionamiento correcto, preguntas orales y escritas.

1. Caso de Estudio

a. Cada grupo de alumnos deberá configurar sólo un segmento wireless, para satisfacer las necesidades de comunicaciones WLAN seguras para los integrantes de su Grupo.
b. En cada WLAN solo habrá una PC Administración con acceso web HTTPS seguro.
c. El ambiente de red será integrado por los Grupos de Usuarios 1, 2 y 3, mediante redes WLAN seguras por segmento, dedicadas SOLAMENTE a usuarios de su Grupo. Todos los segmentos WLAN están comunicados en un único segmento LAN. Los usuarios de cada Grupo sólo podrán acceder a la WLAN respectiva. Las direcciones de red de cada Grupo serán 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24, respectivamente. Contraseña de acceso a todas las WLAN: r3dr2d2
d. La Política General de Seguridad de la Información será del tipo RESTRICTIVA: “Todo lo que no está permitido, está prohibido”.
   1) Las PCs sólo podrán comunicarse dentro de la WLAN respectiva, pero no mediante la WLAN de otro Grupo.
   2) El Dispositivo M representa un usuario móvil que se comporta como intruso. Las intrusiones pueden realizarse en cualquiera de las WLANs. Se asume conocida la contraseña de acceso a la WLAN.
e. Se empleará como guía técnica de configuración del AP el documento **Securing your Linksys WRT54G.**



Requerimientos para el alumno (Objetivos Técnicos)

a. **Elaborar un listado de posibles amenazas a la seguridad de redes *WLAN IEEE802.11* e identificar las vulnerabilidades a las que está expuesta la red del estudio de caso.**

b. **Configurar los dispositivos en base a las tareas descriptas y lograr el funcionamiento correcto de la red en todos sus segmentos.**

c. **Demostrar el funcionamiento de la red, sus dispositivos y equipos en los siguientes puntos de verificación:**

   1) Acceso HTTPS desde la PC Administración al AP respectivo.
   2) Restricción de acceso web para toda otra PC.
   3) Acceso correcto (PING) dentro de la WLAN respectiva.
   4) Comunicación (PING) entre AL MENOS DOS PC de la WLAN respectiva.
   5) Restricción de comunicación, aún clave conocida, (acceso wireless fallido) entre DOS PC de distintas WLANs.
   6) Servicios de seguridad implementados según la guía, a requerimiento del docente.

d. **Resguardar las configuraciones para futuras actividades de laboratorio.**

e. **Responder el cuestionario escrito al finalizar las tareas.**

2. ***Tareas durante la clase***

a. Iniciar la administración del dispositivo AP

Encender el dispositivo de la siguiente manera:

1) Pulse y mantenga pulsado el botón MODE (detrás), mientras vuelve a conectar la energía al AP.
2) Mantenga pulsado el botón MODE hasta que el LED de estado se visualice de color rojo (aproximadamente 20 a 30 segundos), y suelte el botón MODE.
3) Deje que el AP finalice su inicialización.

Luego, desde una PC con conexión física al AP Linksys modelo WRT54 entrar a la configuración web del mismo, utilizando el Internet Explorer mediante la IP por defecto:
http://192.168.1.1
*Se ingresa con **admin/admin** y se accede a la configuración para definir los parámetros de la red inalámbrica en el AP y los requerimientos de seguridad. En caso de ser necesario, resetee los parámetros de administración a valores de fábrica.*

b. De acuerdo a los requerimientos básicos de seguridad del caso de estudio, configurar las siguientes medidas de seguridad *(los datos particulares para cada Grupo de Usuarios serán dados por el docente)*:

1) Parámetros de Administración del AP.
   a) Contraseña de administración distinta a valores por defecto.
   b) Acceso HTTPS.
   c) Desactivación de administración wireless, de modo remoto y UPnP.
2) Parámetros básicos de comunicaciones wireless:
   a) Modo de red.
   b) Modificación SSID.
   c) Canal wireless.
   d) Desactivación de la difusión del SSID.
3) Filtros de direcciones MAC, según políticas de seguridad.
4) De acuerdo a las amenazas y vulnerabilidades de las WLAN, seleccione los parámetros de cifrado mediante los protocolos y datos de mayor fortaleza.

c. Configurar las distintas PC y el dispositivo M, para demostrar el correcto funcionamiento de las medidas de seguridad. El usuario M podrá utilizar cualquier herramienta para escalar privilegios.

d. De acuerdo a las amenazas conocidas, a las vulnerabilidades identificadas en el archivo *security-vulnerabilities-wireless-lan-technology_1629 SANS.pdf* para el caso de estudio y en base a las demás opciones de configuración de seguridad del AP, indicar:

1) ¿Qué otras medidas de seguridad implementaría en el AP?

e. Evaluar el firmware del AP y consultar la página del fabricante sobre su actualización.

f. Resguardar la configuración del AP.

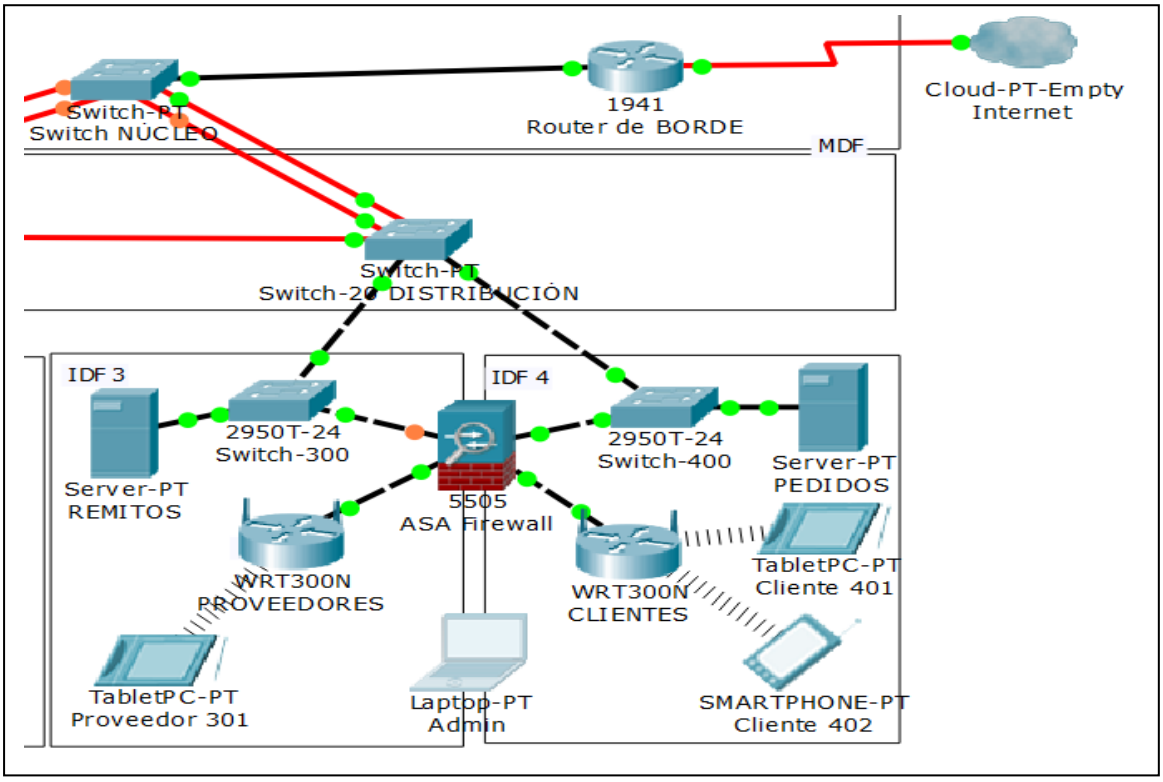
TIEMPO ASIGNADO: 120 minutos

LECTURAS RECOMENDADAS PARA DESPUÉS DE LA PRÁCTICA

- Amplíe su comprensión del problema de la seguridad en Internet y las mejores prácticas para mitigar riesgos: https://www.cisecurity.org/critical-controls.cfm
- Conozca cómo implementar un Wireless Access Point mediante software *open source*: http://www.wi-fiplanet.com/tutorials/article.php/3562391

ACTIVIDADES DE INTEGRACIÓN DE CONOCIMIENTOS PRÁCTICOS (Extraclase):

1. Desarrolle el ejercicio descripto en el documento ***practica_7.pdf***.
2. Adicionalmente, puede integrar el conocimiento de este laboratorio con las experiencias de otras actividades de formación experimental con el simulador Cisco Packet Tracer Student, ampliando el escenario del TL1, con los siguientes segmentos WLAN:



CRITERIO DE EVALUACION

Se aprobará el TLab si se alcanzan los siguientes resultados:

1. Ejecución correcta de las actividades experimentales y logro de los objetivos técnicos.
2. Respuestas satisfactorias a evaluaciones orales individuales sobre situaciones de configuración en el simulador.
3. Configuración completa de las medidas de seguridad WLAN, según requerimientos del Estudio de Caso. En su defecto, aprobación de evaluación individual con el porcentaje de eficacia mínimo requerido.