

DISPOSITIVOS Y REDES INALÁMBRICOS

Detección de puntos de acceso falsos en redes WiFi

OBJETIVO DE LA ACTIVIDAD

Los alumnos comprenderán la peligrosidad que representa un falso punto de acceso operando en una ESS. Posteriormente, aprenderán a monitorizar su presencia y generar las correspondientes alarmas.

La actividad completa estima la siguiente dedicación por parte del alumno:

Actividad presencial	Actividad no presencial
4 horas	6 horas

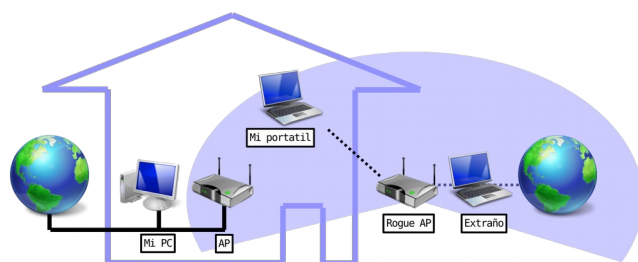
ACTIVIDAD NO PRESENCIAL

La actividad no presencial que deberá realizar el alumno antes de realizar esta actividad es la realización, en casa y de manera autónoma de los “Pasos Previos” de cada una de las partes en que se divide esta práctica.

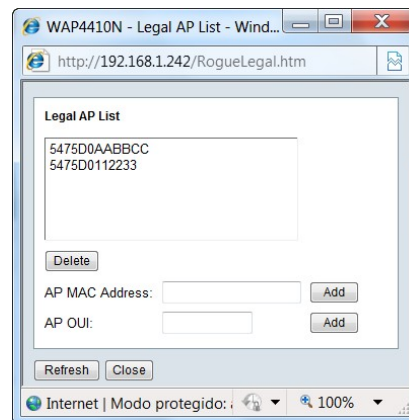
DESARROLLO DE LA ACTIVIDAD

Pasos previos

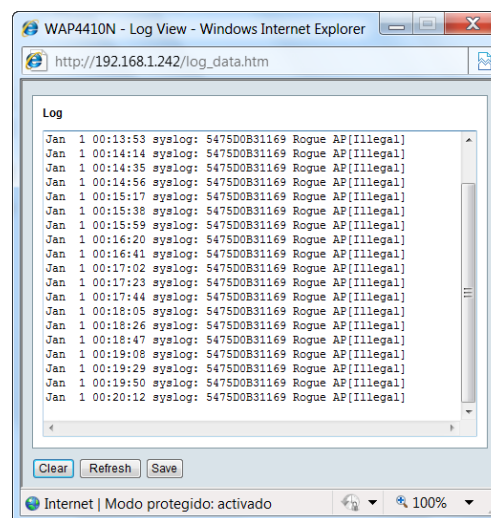
- Conocer en que consiste un ataque a una red WiFi mediante falso punto de acceso.



- Conocer la forma de configurar un AP para que monitorice la ESS y detecte la presencia de falsos APs.



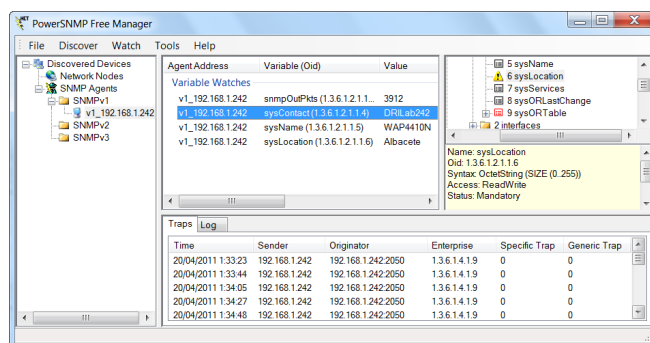
- Conocer como la detección de un falso AP queda registrada en el LOG de eventos del AP monitor.



- Conocer como se configura un AP monitor para que envíe traps SNMP al PC del administrador de la red.



- Conocer como instalar y configurar un software de gestión SNMP (como PowerSNMP) en el PC del administrador de la red.

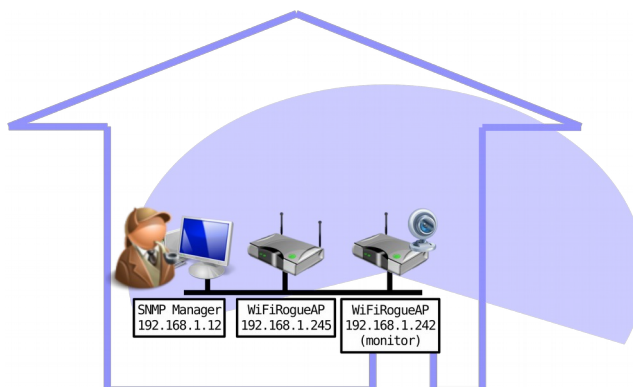


Bibliografía

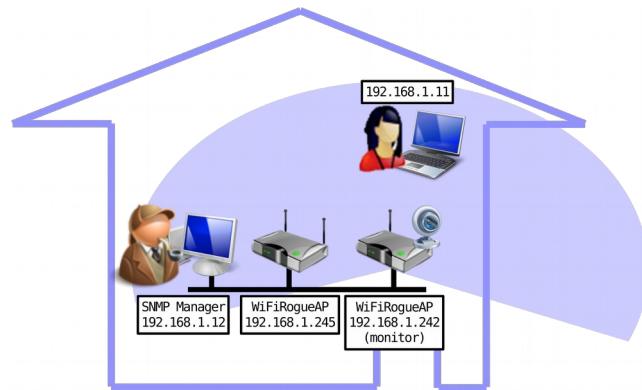
- Punto de acceso wifi falso + SSLTrip. <http://www.securitynull.net/punto-de-acceso-wifi-falso-ssltrip-backtrack-5/>. Último acceso 01/24/17.
- Amran Ahmad and Suhaidi Hassan. "Detecting Rogue Access Point (RAP) using Simple Network Management Protocol (SNMP)". in International Conference on Network Applications, Protocols and Services 2008 (NetApps2008). 2008: Executive Development Center, University Utara Malaysia. https://www.researchgate.net/profile/Amran_Ahmad/publication/228896862_Detecting_Rogue_Access_Point_RAP_using_Simple_Network_Management_Protocol_SNMP/links/5564b11508ae89e758fd953b.pdf. Último acceso 01/24/17. También en moodle asignatura.
- PowerSNMP Free Manager. Dart Communications. http://www.dart.com/psnet_free.aspx. Último acceso 01/24/17.
 - PowerSNMP Free Manager Help. http://www.dart.com/help/psnet_free/webframe.html. Último acceso 01/24/17
 - Práctica de laboratorio: Configuración de SNMP. <http://docplayer.es/2193069-Practica-de-laboratorio-configuracion-de-snm.html>. Último acceso 24/01/17
- Manual del punto de acceso Cisco WAP4410n. Moodle de la asignatura.
- Manual del punto de acceso Cisco WAP2000. Moodle de la asignatura.

Montajes a realizar

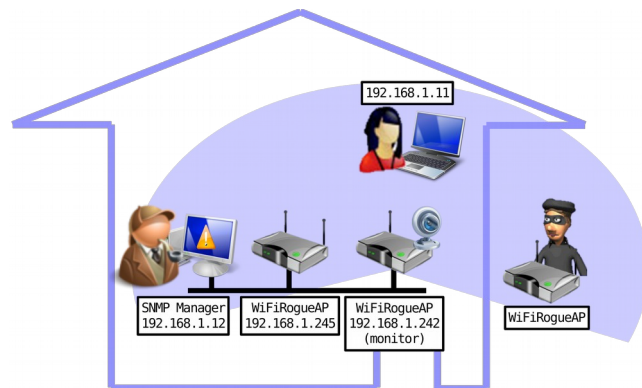
- Configurar una ESS con un AP estándar y otro en modo monitor. Configurar un gestor SNMP en la red.



- Comprobar como el AP monitor no es detectado por las estaciones.



- Introducir un falso AP en la cobertura del monitor (en caso de no disponer de 3 APs, puede eliminarse el AP estándar). Comprobar cómo se disparan las alarmas en el gestor SNMP.



ENTREGABLE

Fruto de esta actividad no se realizará ningún entregable, sino que cada vez que se obtenga una configuración se le deberá de enseñar al profesor, para que este compruebe su funcionamiento.