



Bastionado de Redes y Sistemas

Trabajo 3

Seguridad en conexiones invisibles



Criterios de evaluación

4d. Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).



Índice

Descripción	3
Parte 1 - Seguridad en routers domésticos	3
Parte 2 - Seguridad wifi en redes empresariales	4
Formato de entrega	5
Evaluación	6
CE 4d. Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.)	6

Descripción

Parte 1 - Seguridad en routers domésticos

Los routers domésticos son un tipo de dispositivo que hay que evitar a toda costa en entornos profesionales. Están pensados para facilitar la conexión, tanto por cable como inalámbrica (sobre todo inalámbrica) a clientes particulares. Sin embargo, replican muchas de las medidas de seguridad que podemos aplicar en un entorno empresarial desde una interfaz de gestión bastante simple. Por lo tanto, se pueden realizar muchas pruebas útiles con este tipo de dispositivos. Además, son utilizados en un entorno empresarial por muchas PYMEs que no tienen un presupuesto demasiado alto y cuyos riesgos no compensan la adquisición de dispositivos más potentes.

Comienza leyendo con atención [esta web sobre seguridad en routers domésticos](#). Ofrece información muy completa e interesante sobre los elementos a tener en cuenta al tratar de configurar la mayor seguridad posible. Una frase clave que aparece es: “El mayor experto del mundo solo puede hacer un router seguro tanto como lo permita su firmware”. Lo que quiere decir que la elección del dispositivo es crítica, ya que no todos permiten aplicar todas las medidas necesarias.

En [este enlace](#) puedes encontrar también un listado de las páginas web en las que los fabricantes de routers publican sus avisos de seguridad. En el siguiente apartado, tienes un listado de emuladores web de diferentes consolas de gestión de varios dispositivos. Elige uno de ellos y realiza una de las siguientes opciones:

1. Elaborar una guía de hardening de ese modelo en el formato que prefieras (PDF, CodeLab, web, Documento de Google, ...etc).
2. Buscar una guía de seguridad de ese modelo previamente realizada y hacer un anexo en el que critiques alguna de las medidas propuestas o añadas otras nuevas. De nuevo, eres libre de elegir el formato.

Parte 2 - Seguridad wifi en redes empresariales

Cuando tenemos una red wifi empresarial, normalmente formada por uno o más puntos de acceso (en función del tamaño de la misma y sus requisitos), éstos se configuran desde un controlador central que los administra. En el mercado actualmente existen varias marcas (Aruba, Cisco, Ubiquiti...). En esta parte del trabajo la vamos a realizar sobre Ubiquiti, por los siguientes motivos:


- Permiten probar su software de gestión de forma gratuita.
- Es el único distribuidor de los mencionados que no tienen cuotas mensuales obligatorias para usar los dispositivos adquiridos.
- Gracias a su equilibrio entre calidad y precio, se está convirtiendo en una de las soluciones más utilizadas en el entorno empresarial.

Para poder acceder a sus herramientas de forma gratuita, es necesario previamente [crear una cuenta](#).

Una vez tengas la cuenta creada, [descarga](#) e instala el software de UniFi Controller. Este es el mismo software que se usa para gestionar este tipo de redes. Normalmente, o bien se instala en un servidor, o se adquiere un dispositivo CloudKey que viene con el software preinstalado y te facilita el acceso remoto al mismo.

Comenzamos diseñando y creando la infraestructura física de nuestra red wifi. Para ello, vamos a decidir cuántos APs vamos a necesitar y dónde los vamos a colocar. La versión moderna de la interfaz aún no permite hacerlo, te redirige a la web design.ui.com. En esta web se puede hacer una simulación física de una red y hasta te elabora el presupuesto del material que vas a necesitar para llevar la instalación a cabo. El problema es que no permite definir ninguna configuración en los puntos de acceso para delimitar su potencia y ver cómo influye en el mapa de calor de la cobertura. Sin embargo, podemos asumir que posteriormente se delimitará la potencia de cada punto de acceso lo suficiente para que la señal escape de las paredes en las que se encuentre (deberá adecuarse, por lo tanto, al material de dicha pared). Elabora una propuesta de instalación en un plano a tu elección y exporta los mapas de calor de las coberturas 2.4Ghz y 5GHz.

Para terminar este trabajo, vais a realizar un estudio de cómo asegurar lo máximo posible una instalación wifi de UniFi y el resultado de ese estudio se reflejará en [este repositorio](#). En definitiva, debéis colaborar para dar estructura al checklist. Podéis inspiraros a partir de [este ejemplo](#). Con una diferencia. Cada configuración propuesta en el checklist la realizaréis usando la extensión de Chrome [Tango](#). Después, la enlazaréis en el repositorio de forma ordenada. Cada



uno de vosotros debe elaborar como mínimo dos guías. Si necesitáis entrar en la configuración de un AP concreto, podéis utilizar [este portal demo](#).

Formato de entrega

Debes entregar en la tarea habilitada llamada “Trabajo 3”:

- Guía de hardening de un router doméstico a elegir en el formato preferido.
- Mapa de calor del diseño de la red wifi de la cobertura 2.4GHz.
- Mapa de calor del diseño de la red wifi de la cobertura 5GHz.
- Enlaces de las guías realizadas para el repositorio UniFi Hardening Checklist.

Evaluación

CE 4d. Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.)

Indicadores	Niveles de logro		
	Bien	Regular	Insuficiente
Seguridad en routers domésticos (2pt)	La guía de bastionado de un router doméstico es muy completa y correcta (2pt)	La guía de bastionado de un router doméstico no está demasiado completa o contiene incorrecciones (1pt)	No se entrega guía de bastionado de un router doméstico o es demasiado pobre (0pt)
Mapa de calor de una red inalámbrica (2pt)	Se han realizado dos mapas de calor en diferentes frecuencias con una distribución correcta para un red empresarial (2pt)	Se ha realizado un mapa de calor en una frecuencia con una distribución correcta para un red empresarial (1pt)	No se han realizado mapas de calor o la distribución es incorrecta para una red empresarial (0pt)
Aportación al checklist en el repositorio grupal (1pt)	Se han realizado commits al repositorio colaborando para dar estructura y dotarlo de contenido (1pt)	Se ha realizado una aportación muy pobre al repositorio (0.5pt)	No se ha realizado ninguna aportación al repositorio con el objetivo de estructurarlo y/o añadir contenido (0pt)
Guías elaboradas y enlazadas en el repositorio grupal (4pt)	Se han elaborado dos guías completas y correctas sobre dos aspectos de bastionado de una red UniFi (4pt)	Se ha elaborado una guía completa y correcta sobre uno de los aspectos de bastionado de una red UniFi (2pt)	No se ha elaborado ninguna guía o las que se han elaborado son demasiado pobres (0pt)