**Auditoría/Informe del proyecto del equipo Gryffindor CIT31-01**

# ÍNDICE

[ÍNDICE 2](#_Toc106127816)

[ÍNDICE DE FIGURAS 3](#_Toc106127817)

[ENUNCIADO 4](#_Toc106127818)

[RED PROPUESTA 5](#_Toc106127819)

[AUDITORIA 6](#_Toc106127820)

[1. Enumeración de redes, componentes, topologías y protocolos 6](#_Toc106127821)

[2. Identificación de los sistemas operativos instalados 6](#_Toc106127822)

[3. Análisis de servicios y aplicaciones 7](#_Toc106127823)

[4. Detección, comprobación y evaluación de vulnerabilidades 8](#_Toc106127824)

[5. Medidas específicas de corrección 9](#_Toc106127825)

[6. Recomendaciones sobre implantación de medidas preventivas. 10](#_Toc106127826)

[REFERENCIAS 12](#_Toc106127827)

# ÍNDICE DE FIGURAS

[Figura 1: Modelo esquemático de la red propuesta (Sánchez, 2022).](#_heading=h.2et92p0) 5

# ENUNCIADO

Usted trabaja para la una empresa de SmartBuildings. Ante la emergencia de Coronavirus se le pide desplegar un sistema de SmartCities para comunicar en tiempo real a los miembros del sistema sanitario. Para ello despliega en dos edificios sistemas basados en gateways Linux (puede escoger la distribución más apropiada). Dichos sistemas permiten enviar información mediante una interfaz web a una base de datos alojada en uno de los edificios. A dicha base de datos y servicio web solo se puede acceder desde la intranet del edificio. Además, en el servidor, debe alojar una plataforma web para que todo el público pueda enviar consultas y otra información para permitir servicios de telemedicina.

Debe planificar un sistema seguro que permita a los gateway enviar los datos al servidor, que además debe estar accesible a los habitantes del edificio y cualquier usuario doméstico (todos ellos usuarios de Windows). Dichos usuarios se conectan desde Intranet donde se dispone de una LAN WiFi que mantiene conectados los equipos mencionados y, además, dispositivos móviles.

Adicionalmente, el profesor dijo que tratásemos de hacer nuestro proyecto de mensajería alterando la infraestructura original lo menos posible (a ser posible no alterarla).

# RED PROPUESTA

Inicialmente nos centramos por un diseño como el mencionado en el enunciado, tanto por simplicidad como por petición del enunciado, en el que se comunica el exterior con el interior mediante una VPN para evitar tener que alterar la infraestructura original de la empresa, incluyendo firewalls.

Al comienzo tratamos de usar la VPN pre-instalada de Windows, pero por comodidad decidimos emplear el software profesional OpenVPN. Según las instrucciones de instalación (WunderTech, 2022), hemos decidido que nuestra VPN es 192.168.60.0/24 es la VPN, llamada OpenVPN Servidor, la Clave pre-compartida es “SorbeteDeLimon” y el resto queda por defecto. Estos parámetros los utilizamos para el Firewall de su edificio también. El usuario es SSR con nombre completo “Albus Dumbledore”.

El edificio remoto tiene red 192.168.57.0/24, el edificio de la empresa 192.168.56.0/24 y la internet la simulamos con la 100.200.0.0/24, inicialmente tratamos de hacer una conexión entre dos ordenadores físicos virtualizando los edificios y con un módem físico entre medias, pero no funcionó así que pasamos a virtualizarlo todo en una máquina y quitarnos el router de en medio.

Hemos supuesto que en la infraestructura original los gateways son del tipo pfSense y utilizan un único firewall por edificio de política restrictiva hacia adentro, para mayor seguridad (menos funcionalidades supone menos potenciales vulnerabilidades), permitiendo la entrada por el puerto 443 y 80 (también está el 3306 para el mySQL pero para acceso local); y sin suponer mayor profundidad en la red, para permitir virtualizar varias máquinas.

La BBDD es SQL mediante xampp.

El material de nuestra red puede encontrarse en el github:

https://github.com/tardisfromtornspace/ProyectoGryffindorCIT31-01.git

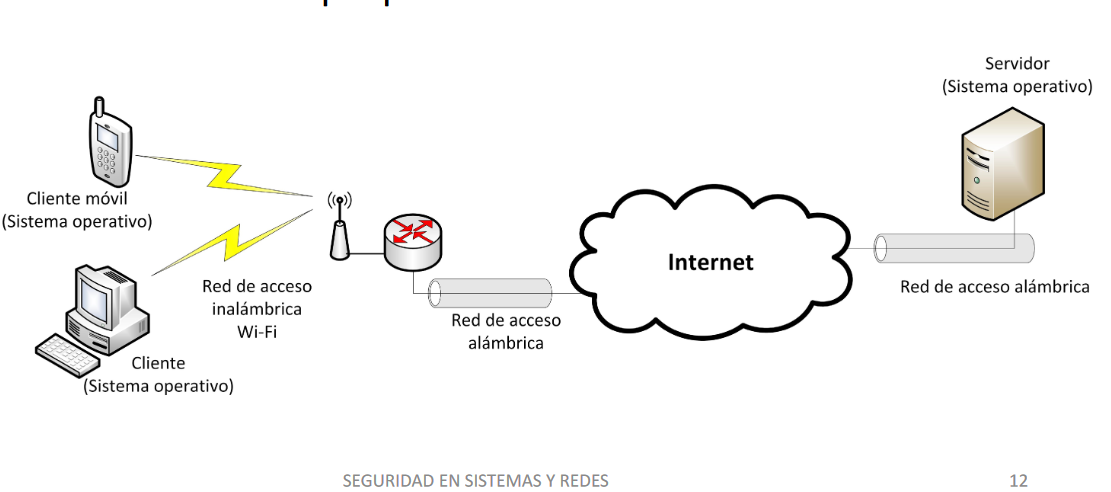


Figura 1: Modelo esquemático de la red propuesta **(Sánchez, 2022)**.

# AUDITORIA

Hemos decidido emplear una auditoría de caja blanca por falta de tiempo y para mayor eficiencia, con un conocimiento total de la red.

*Los ataques se hacen desde 3 sitios, edificio de la empresa, edifico remoto y desde la internet, con una Kali Linux o Windows donde corresponda*

## Enumeración de redes, componentes, topologías y protocolos

Hay 3 redes, mencionadas en el apartado red propuesta:

**LANA** – La red del edificio de la empresa 192.168.56.0/24 Tiene configurada una VPN. Tiene una máquina servidor (192.168.56.10) y el router pfSense1 (192.168.56.1)

**LANB** – La red edificio remoto 192.168.57.0/24. Tiene una máquina clienteRemoto (192.168.57.2) y el router pfSense2 (192.168.57.1)

**WAN** – Simulación del internet 100.200.0.0/24. Tiene a los dos routers (pfSense1 con 100.200.0.1 y pfSense2 con 100.200.0.2).

Todos ellos emplean topología en estrella, menos la conexión de WAN, simulada con un P2P. Todos ellos emplean máscara /24 por simplicidad.

Routers:

**pfSense1:** es el que conecta LANA con WAN

**pfSense2:** es el que conecta LANB con WAN

-Ambos actúan con el mismo tipo de firewall: política permisiva desde LAN y restrictiva desde WAN.

Usamos protocolo TCP/IP para las conexiones, salvo OpenVPN, que se especializa en el uso de datagramas UDP.

## Identificación de los sistemas operativos instalados

1. **pfSense1 (#R1):** pfSense 2.6.0-RELEASE FreeBSD 64-bit 12.3-STABLE
2. **pfSense2 (#R2)**: pfSense 2.5.2-RELEASE FreeBSD 64-bit 12.2-STABLE
3. **ClienteRemoto** **(#LANB1**): ~~Windows XP 32-bit con parche Service Pack 3~~ *No hemos usado el Windows XP por su gran número de vulnerabilidades conocidas y la imposibilidad de actualizar o parchear gran parte de ellas, así que hemos empleado un* Windows 7 Ultimate 32-bit bit 6.1.7601 Service Pack 1 Build 7601
4. **Servidor (#LANB2):** Windows 10 Education 64-bit, versión 1903, versión del SO 18362.592.

## Análisis de servicios y aplicaciones

|  |
| --- |
| **pfSense1 (#R1)**  ¿ESTE NMAP FUE POR EL LAN O EL WAN?   * PORT STATE SERVICE VERSION * **80**/tcp open http nginx * **443**/tcp open ssl/https?   Dispone solamente del servicio http en el puerto 80 para la configuración del pfsense. Lo mismo ocurre con el puerto 443, para la conexión por https que ha sido configurada en el pfSense1.  El puerto 1194 se encuentra abierto para la comunicación  por VPN, aunque Nmap no lo ha detectado.  COMPLETAR AÑADIENDO EL NMAP DESDE EL OTRO LADO INDICANDOLO COMO UNA SEGUNDA PARTE  PORT STATE SERVICE VERSION  **pfSense2 (#R2)**:  ¿ESTE NMAP FUE POR EL LAN O EL WAN?  PORT STATE SERVICE VERSION   * **53**/tcp open domain Unbound * **80**/tcp open http nginx * **443**/tcp open ssl/http nginx   Similar a pfSense1, pero en este caso el puerto 53 se encuentra abierto.  Este servicio se utiliza para comunicar tramas DNS.  El puerto 1194 se encuentra abierto para la comunicación  por VPN, aunque Nmap no lo ha detectado.  COMPLETAR AÑADIENDO EL NMAP DESDE EL OTRO LADO INDICANDOLO COMO UNA SEGUNDA PARTE  PORT STATE SERVICE VERSION  **ClienteRemoto** **(#LANB1**):  PORT STATE SERVICE VERSION   * **135**/tcp open msrpc Microsoft Windows RPC * **139**/tcp open netbios-ssn Microsoft Windows netbios-ssn * **445**/tcp open microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) * **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) * **49152**/tcp open msrpc Microsoft Windows RPC * **49153**/tcp open msrpc Microsoft Windows RPC * **49154**/tcp open msrpc Microsoft Windows RPC * **49155**/tcp open msrpc Microsoft Windows RPC * **49156**/tcp open msrpc Microsoft Windows RPC * **49157**/tcp open msrpc Microsoft Windows RPC   **AÑADIR APLICACIONES**  **Servidor (#LANB2):**  PORT STATE SERVICE VERSION   * **80**/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m * PHP/8.1.2) * **443**/tcp open ssl/http Apache httpd 2.4.52 ((Win64) * OpenSSL/1.1.1m PHP/8.1.2) * **3306**/tcp open mysql? * **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)   Los puertos 80 y 443 para la conexión http y https respectivamente.  En el puerto 3306 podemos encontrar la conexión a la base de datos  mysql. El puerto 5357 se utiliza para (¿se usa para qué? Esto se ha quedado a medias Ricardo)  **AÑADIR APLICACIONES** |
|  |
|  |

## Detección, comprobación y evaluación de vulnerabilidades

|  |
| --- |
| Para cada servicio y/o aplicación en cada una de las máquinas • Si la máquina es un S.O. o un dispositivo móvil, hay que utilizar las herramientas vistas en cada una de las unidades (p.ej. vulskan, ZAP, Sqlmap) • Para servicios WEB se puede usar la metodología OWASP como vimos • También análisis generales como de denegación de servicio con Apache Benchmarking  **pfSense1 (#R1):**   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. Eso sí si están abiertos por la parte de la WAN hay que corregirlo. 2. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS) 3. Además, hubo una vulnerabilidad posible, y es no haber cambiado las contraseñas de acceso al router de las por defecto (admin, pfsense). **Se corrigió antes de hacer el análisis (nueva contraseña es “Lapatata87pocha”) y por lo tanto no se ha tenido en cuenta en el apartado 5.** 4. También hubo una vulnerabilidad, y es usar un certificado autofirmado para el webConfigurator de conexión segura. Este se ha resuelto mediante el paso a autoridad de certificación propia generada y difundida por nosotros y que los navegadores de esa red la importaran para confiar en dicha autoridad de certificación, y en el nuevo certificado de servidor para conexión firmado por ésta. **Se corrigió antes de hacer el análisis y por lo tanto no se ha tenido en cuenta en el apartado 5.**   **pfSense2 (#R2)**:   1. 53/tcp open domain Unbound -> Potencial vulnerabilidad de dejar un puerto innecesario abierto, con todo lo que conlleva. Hay que corregirlo 2. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. FreeDOS) 3. Además, hubo una vulnerabilidad posible, y es no haber cambiado las contraseñas de acceso al router de las por defecto (admin, pfsense). **Se corrigió antes de hacer el análisis (nueva contraseña es “junio2020”) y por lo tanto no se ha tenido en cuenta en el apartado 5.** 4. También hubo una vulnerabilidad, y es que el conectar al firewall para configurarlo no se hacía en conexión segura, por lo que se podría fácilmente interceptar el mensaje y obtener la contraseña y clave no cifradas. Por lo tanto, pasamos a SSL/TLS y generamos un certificado a de otra CA propia generada y difundida por nosotros y que los navegadores de esa red la importaran para confiar en dicha autoridad de certificación, y en el nuevo certificado de servidor para conexión firmado por ésta. **Se corrigió antes de hacer el análisis y por lo tanto no se ha tenido en cuenta en el apartado 5.**   **ClienteRemoto** **(#LANB1**):   1. Microsoft Windows RPC - (HAY VULNERABILIDADES CON ESTO, PROGRESAD CON EL SW) 2. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. Windows 7)   **Servidor (#LANB2):**   1. (lista de servicios acá y vulnerabilidades… también incluyen vulnerabilidades conocidas de la versión del S.O. Windows 10) |

## Medidas específicas de corrección

|  |
| --- |
| • De las vulnerabilidades descubiertas en el apartado anterior, cuales se corrigen y por qué. • Y cuales no y por qué  **• En la entrega que se haga YA deben estar corregidas**  **pfSense1 (#R1):**   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. Eso sí si están abiertos por la parte de la WAN hay que corregirlo. 2. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   **pfSense2 (#R2)**:   1. Necesitamos los puertos 80 y 443 abiertos por el lado de LAN (evitar que se bloquee acceso al firewall desde dentro), por lo que no podemos cerrarlos desde allá. Eso sí si están abiertos por la parte de la WAN hay que corregirlo. 2. ***53/tcp open domain Unbound*** -> Nuestra empresa no necesita que se empleen servicios DNS de momento, por lo que dejar este puerto abierto es innecesario y podría llevar a vulnerabilidades. En una red real se podría dejar abierto si usásemos servidores DNS, eso sí. Hay que corregirlo 3. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   **ClienteRemoto** **(#LANB1**):   1. ***Microsoft Windows RPC:*** las interfaces MSRPC pueden usarse por un atacante para recolectar información importante y comprometer servidores (p.ej. robar la contraseña de la VPN y colarse). Se deben cerrar los puertos **135,**  **49152,** **49153,** **49154,** **49155,** **49156,** **49157**. Hay que corregirlo 2. ***5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)*** -> 1º el cliente que sepamos no necesita esto. 2º ese puerto y su servicio relacionado son propensos a fugas de información que permiten acceso remoto no autorizado, por lo que debe de ser cerrado si no se usa. Hay que corregirlo 3. **139**/tcp open netbios-ssn Microsoft Windows netbios-ssn -> Servicio empleado por RPC, si es posible debería cerrarse el puerto. Hay que corregirlo 4. **445**/tcp open microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) -> Nuestro cliente remoto se supone que no debe tener un “grupo de trabajo” fuera de acceder a nuestra VPN. Cerrar puerto si es posible. Hay que corregirlo 5. (lista de vulnerabilidades, indicando si se corrige o no y por qué)   **Servidor (#LANB2):**   1. **5357**/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) -> 1º es una versión más antigua de HTTP que la empleada para la versión actual de nuestro servidor, que solo debe hacer lo mínimo pedido. 2º ese puerto y su servicio relacionado son propensos a fugas de información que permiten acceso remoto no autorizado, por lo que debe de ser cerrado si no se usa. Hay que corregirlo 2. (lista de vulnerabilidades, indicando si se corrige o no y por qué) |

## Recomendaciones sobre implantación de medidas preventivas.

Entrenar a nuestros trabajadores en medidas de seguridad, entre ellas no dejar la contraseña de usuario por ahí ni dejarla grabada, y tratar de mantener su SW y HW actualizado.

Dejar los sistemas cerrados bajo llave (contraseña electrónica y llave física) dentro que una habitación con sistema de refrigeración y medidas anti-incendios, y filtros de aire (más una cámara de presión positiva) para prevenir polvo e insectos dentro de la cámara, con una trampa de luz ultravioleta para eliminar cualquier posible insecto que se cuele. El servidor debería estar desplegado en el edificio de la empresa, para mayor seguridad. Y tener cámaras con reconocimiento facial y otros métodos de seguridad biométrica.

También deberíamos añadir redundancias como medida extra en caso de caída o fallo (p. ej. backup de la BBDD, múltiples switches, generadores de emergencia) pero no lo hemos implementado porque o bien no se podían simular en máquina virtual, o se podrían simular pero a riesgo de falta de memoria (p.ej: un ordenador teniendo que soportar la red básica más los backups).

El control de acceso debería ser distribuido, de tal forma que dar privilegios más altos a alguien requiera de la colaboración de todos los administradores, para complicar corrupción permitiendo accesos maliciosos al sistema.

Para mejorar seguridad comunicaciones móviles, usaríamos la mejor encriptación, WPA3, y no escribas las contraseñas, y no hablar de los clientes públicamente ni de nada relacionado con las seguridad (nada fuera del entorno laboral). También los dispositivos móviles deberían tener una doble verificación de sistema biométrico y contraseña, y no estar rooteados. De hecho para mayor seguridad los móviles corporativos deberían resetearse cada mes para asegurarse de que no están rooteados.

Además como protección extra frente a alguien logrando robar credenciales de la VPN y acceder, deberíamos añadir un segundo firewall detrás del primero para evitar que alguien empleara el servicio VPN para mandar paquetes a servicios previamente inaccesibles; pero no lo hemos resuelto porque nos han pedido no alterar la infraestructura.

(Esta imagen de abajo es por referencia, no incluirla en la memoria final)Tabla

Descripción generada automáticamente)

# REFERENCIAS

Sánchez, B. B. (1 de 5 de 2022). *moodle.* Obtenido de Enunciado y propuesta Segundo Parcial: https://moodle.upm.es/titulaciones/oficiales/pluginfile.php/9386654/mod\_resource/content/3/Enunciado%20y%20propuesta%20Segundo%20parcial.pdf

WunderTech. (8 de 06 de 2022). *WunderTech*. Obtenido de WunderTech: https://www.youtube.com/watch?v=cxhIpmov4TY