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

# ÍNDICE

[ÍNDICE 2](#_Toc102820786)

[ÍNDICE DE FIGURAS 3](#_Toc102820787)

[ENUNCIADO 4](#_Toc102820788)

[RED PROPUESTA 5](#_Toc102820789)

[AUDITORIA 6](#_Toc102820790)

[REFERENCIAS 7](#_Toc102820791)

# ÍNDICE DE FIGURAS

[Figura 1: Modelo esquemático de la red propuesta (Sánchez, 2022). 5](#_Toc102820792)

# 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 sin alterar la infraestructura original.

# 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.

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

Cada edificio en la versión final se simula en un edificio diferente.

La BBDD es SQL mediante xampp.

El material de nuestra red puede encontrarse en el github:

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

(PUEDE QUE ESTO OTRO SEA UTIL PARA LA RED https://openwrt.org/)

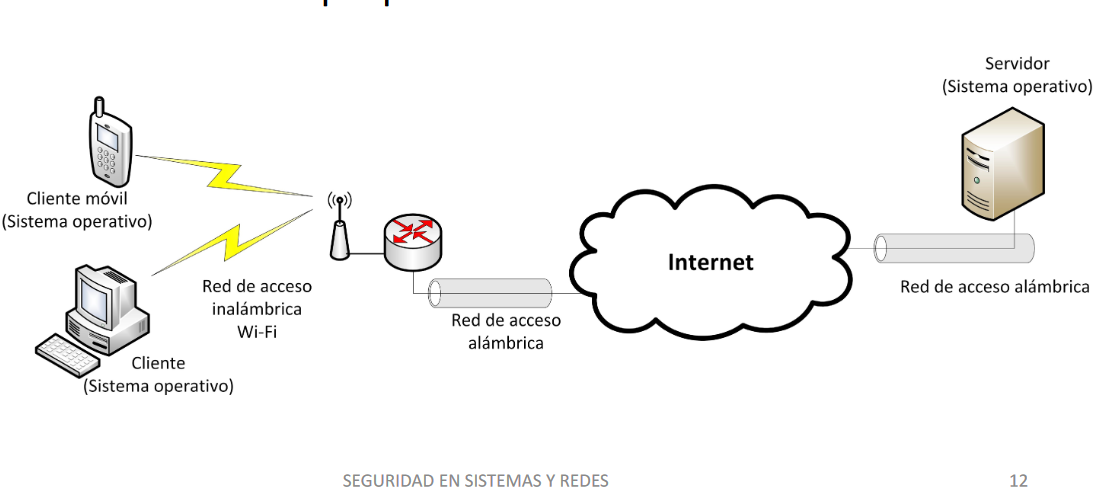


Figura 1: Modelo esquemático de la red propuesta (Sánchez, 2022).

# AUDITORIA

Hemos decidido emplear una auditoría de caja gris para mayor eficiencia, con un conocimiento parcial de la red; empleando nMap.

<<<Los ataques se hacen desde 3 sitios, edificio de la empresa, edifico remoto y desde la internet, con una Kali Linux>>>

ER – Firewall --->Móvil que simula la red <--- Firewall – EE

Kali (Alex S) Kali(Javier, adaptador puente) Kali (Víctor)

Es la auditoría que mezcla características de las dos  
anteriores  
• Posiblemente sea la más “eficiente” porque simulamos  
un ataque, dando a conocer parte de la información al  
auditor y pedirle que a partir de ella intente “escalar” al  
resto del sistema  
• Además se puede intentar este test comenzando desde  
varios puntos, red interna, red externa, a través del wifi,  
a través del puesto de un empleado, a través de la  
extranet, etc.

Enumeración de redes, componentes, topologías y  
protocolos

|  |
| --- |
| Se deben identificar las subredes participantes, las máquinas que hay en cada subred, los router que participan, los planes de numeración de cada subred, los firewall que están desplegados, las topologías de red, etc. • En “caja blanca” en análisis es heurístico • En “caja negra” se emplean herramientas como “traceroute” o ping para descubrir esta información |

• Verificación del cumplimiento de los estándares  
internacionales. ISO, COBIT, etc.  
• En esta asignatura será optativo  
• Identificación de los sistemas operativos instalados

|  |
| --- |
| PARA CADA MÁQUINA • Conviene identificar las máquinas con identificadores manejable. • “Cliente #1”, por ejemplo • Arquitectura, versión, parches instalados, etc. • En “caja blanca” en análisis es heurístico • En “caja negra” se emplean herramientas basadas en HTTP, que en el mensaje GET incluye esta información |

• Análisis de servicios y aplicaciones

|  |
| --- |
| • El análisis de aplicaciones y servicios en “caja negra” solo se puede hacer con Nmap u otras herramientas similares • En “caja blanca”, las aplicaciones pueden identificarse de forma sencilla viendo la lista ofrecida por el S.O. pero los servicios se estudian con Nmap • Posibles servicios “ocultos” |

• 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 • Para servicios WEB se puede usar la metodología OWASP como vimos • También análisis generales como de denegación de servicio • Con Apache Benchmarking |

• 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** |

• Recomendaciones sobre implantación de medidas  
preventivas.

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.

|  |
| --- |
| • Todas aquellas vulnerabilidades que NO se hayan podido resolver, o que no sean de tipo informático, se discuten aquí • Por ejemplo, la seguridad externa en sistemas operativos • ¿Dónde conviene desplegar un servidor? ¿Control de acceso? ¿Comunicaciones móviles seguras? • Si el escenario no admite este tipo de comentarios, NO se mencionan |

• Si se aplican varias metodologías, para cada una  
hay que repetir TODO el proceso  
• Pero también se puede ponderar qué alternativa es la  
más adecuada a cada escenario  
• Cuando auditamos activos que nos llegan del  
exterior, NORMALMENTE se aplica auditoría en caja  
gris  
• Porque algo de información tenemos, pero no completa

TODOS los miembros de cada equipo deben  
presentar su proyecto al finalizar el semestre  
• La presentación forma parte de la calificación  
• Independientemente del tipo de trabajo escogido

(Esta imagen de abajo es por referencia, no incluirla en la memoria final, y para analizar las auditorías de otros 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