PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERIA

ESCUELA DE SISTEMAS



PLAN DE DISERTACIÓN

SOLUCIONES PARA DETECCION Y MITIGACION DE CIBERATAQUES CASO DE ESTUDIO HOTEL TOURBLANCHE

AUTOR

JUAN JOSE SERRANO

QUITO DM, 2023

Dedicatoria

Gracias a mi familia, por apoyarme en cada paso y cada tropiezo de mi vida. Nunca habría llegado hasta este punto sin su ayuda, y estaré siempre agradecido por ustedes.

A cada una de mis amistades, por ser la razón para seguir adelante y esforzarme para conseguir mis metas. Me quedo sin espacio para nombrar a todos y sin palabras para expresar el cariño que les tengo.

Agradecimiento

Agradezco a la Pontificia Universidad Católica del Ecuador, y a los docentes de la Facultad de Ingeniería, por ayudarme durante este periodo de desarrollo académico a moldearme en no solo un profesional, sino en una mejor persona.

Tabla de Contenidos

Dedicatoria 2

Agradecimiento 3

Índice de Figuras 7

Índice de Tablas 8

Capítulo 1: Introducción 9

JUSTIFICACION 9

PLANTEAMIENTO DEL PROBLEMA 10

OBJETIVO GENERAL 10

OBJETIVOS ESPECIFICOS 10

ANTECEDENTES 11

Situación Actual de la Empresa 13

Estado Actual del Equipamiento Tecnológico dentro de la Empresa 13

Capítulo 2: Marco Teórico 15

MARCO TEORICO 15

Normas ISO Relacionadas 17

ISO/ IEC 27032 17

ISO 17799:2005 18

NIST 19

OWASP 20

FMEA 21
Capítulo 3: Metodologías y Herramientas a Utilizarse 22
Herramientas Por Utilizarse para las Pruebas 22
Kali Linux 22
Wireshark 23
SSLScan 23
TheHarvester 24
BED 24
Aplicación y Procedimiento de la Metodología 25
Aplicación de Herramientas 29
Aplicación de The Harvester 29
Aplicación de SSLScan 31
Aplicación de Wireshark 33
Aplicación de BED: 34
Aplicación de Nmap: 38
Capítulo 4: Análisis de Resultados 42
Aplicación de la Metodología 42
Presentación de Matrices de Trabajo 42
Vulnerabilidades Descubiertas Sin Herramientas 43
Vulnerabilidades Descubiertas por Herramientas 44

Clasificación de Posibles Problemas según Nivel de Riesgo 45

Posibles Soluciones 45

Problemas Físicos: 45

Problemas Internos (Encontrados por Herramientas) 47

Conclusiones 48

Recomendaciones 49

Bibliografía 50

Índice de Figuras

Figura 1: Lista de Dominios Pertenecientes encontrados por TheHarvester ……28

Figura 2: Resultados del Análisis por SSLScan Parte 1 ……29

Figura 3: Resultados del Análisis por SSLScan Parte 2 ……30

Figura 4: Resultados del Análisis por Wireshark ……32

Figura 5: Resultado del Análisis de Dirección IP ……33

Figura 6: Resultados del Análisis por BED Parte 1 ……34

Figura 7: Resultados del Análisis por BED Parte 2 ……35

Figura 8: Resultados del Análisis por BED Parte 3 ……36

Figura 9: Resultados del Análisis por Nmap Parte 1 ……37

Figura 10: Resultados del Análisis por Nmap Parte 2 ……38

Figura 11: Resultados del Análisis por Nmap Parte 3 ……38

Figura 12: Resultados del Análisis por Nmap Parte 4 ……39

Figura 13: Resultados del Análisis por Nmap Parte 5 ……39

Índice de Tablas

Tabla 1: Clasificación de las PYMES, Pequeña y Mediana Empresa (S.F)..... 16

Tabla 2: Modelo de Evaluación de FMAE para el Hotel Tourblanche (Serrano, 2023)..... 28

Tabla 3: Vulnerabilidades Descubiertas Sin Herramientas 43

Tabla 4: Vulnerabilidades Descubiertas por Herramientas 44

Capítulo 1: Introducción

JUSTIFICACION

Debido a la cada vez mayor importancia de la seguridad informática en nuestra sociedad, es igual de necesario tomar las medidas adecuadas para resguardar la integridad de los datos dentro de cualquier empresa.

Los datos son la fundación de cualquier organización, por más insignificantes que puedan todavía parecer. Y he ahí porque existen todavía millones de hackers esperando a la oportunidad de robar nuestra información personal, o en otros casos, nuestra información corporativa.

La seguridad informática es un tema del cual no se le da la suficiente importancia al momento de implementar una infraestructura tecnológica en una empresa, y de vez en cuando es pasado por alto en innumerables instancias. Comúnmente la ideología es aquella donde una persona no se preocupa por algún problema hasta que este le afecte personalmente, por eso este proyecto busca proveer una solución inteligente para pequeñas y medianas empresas que logre consolidar una fundación sólida para la protección ante ciberataques y la temprana detección y prevención de estos.

El proyecto busca la concientización del público en general acerca de posibles brechas y ataques tecnológicos dirigidos a comerciantes de menor escala, los cuales usualmente pasan estos problemas por alto y no cuentan con los suficientes recursos para permitirse el lujo de un sistema de seguridad complejo.

PLANTEAMIENTO DEL PROBLEMA

La investigación por realizarse con este trabajo de titulación consiste en la determinación del nivel de vulnerabilidad informática para el Hotel Tourblanche. Se ha planteado la siguiente pregunta principal para este trabajo:

¿En qué forma podemos reducir el nivel de vulnerabilidades tecnológicas en el Hotel Tourblanche?

Además, se propone las siguientes preguntas secundarias:

- ¿Qué modelo analítico se va a utilizar para el desarrollo de este trabajo?
- ¿A que estándares de calidad nos vamos a apegar para la evaluación de la solución propuesta?
- ¿La solución propuesta ayuda a la Pyme a cumplir sus objetivos de negocio?

OBJETIVO GENERAL

Aplicar herramientas de ciberseguridad dentro del Hotel Tourblanche para realizar un análisis de vulnerabilidades comprensivo.

OBJETIVOS ESPECIFICOS

- Analizar las características tecnológicas del Hotel para producir un análisis de vulnerabilidades.
- Aplicar el modelo propuesto de soluciones dentro del entorno del Hotel para comprobar su funcionamiento.

- Realizar un plan de mejora continua aplicable a la situación del Hotel para mantener un nivel consistente de seguridad en el futuro.

ANTECEDENTES

Este trabajo de titulación hará uso de materiales bibliográficos orientados a distintos modelos de ciberseguridad que han visto uso dentro de distintos contextos y organizaciones para realizar una comparación analítica de los métodos y soluciones propuestas, con el fin de proveer una serie de pautas a seguir para mantener un nivel alto de seguridad informática.

A lo largo de las últimas décadas, el concepto de ciberseguridad ha ido ganando peso en infinidad de ámbitos, tales como la industria o las telecomunicaciones … A pesar de que no es posible garantizar una seguridad total, la ciberseguridad tiene como objetivo evitar los ataques maliciosos, reducir la vulnerabilidad de la información, … y paliar los daños ocasionados como consecuencia de estos. (Jove, et al., 2021)

La seguridad de la información se presenta a través de un análisis de riesgo de los activos que posean. La ciber seguridad se compone de la evaluación de amenazas (factores externos) que crean ataques, los cuales a su vez explotan vulnerabilidades (debilidades, factores internos) que tienen un impacto sobre las organizaciones y/o personas. (Olivares Rojas, Archundia, Gutiérrez Gnecchi, Molina Moreno, & Cerda Jacobo, 2020)

Debido a la naturaleza especifica del estudio actual, resulta complicado realizar paralelos a otras implementaciones para seguridad tecnológica, especialmente cuando varias soluciones han sido mantenidas privadas dentro de sus propios contextos.

No obstante, se seguirá la guía de otros trabajos como estos siguientes:

A Review of Trends and Issues of Cybersecurity in Academic Libraries (Ajie, 2019)

A pesar de enfocarse en la seguridad de las áreas de bibliotecas digitales, este estudio nos brinda una buena percepción acerca de ataques y soluciones modernas, además de una idea de qué políticas y comportamientos se pueden establecer para reducir estos incidentes.

Ciberseguridad en Plataformas Educativas Institucionales de Educación Superior de la Provincia de Tungurahua – Ecuador (Morales, Medina, 2021)

Como Morales y Medina (2021) indican, los principales riesgos de ciberseguridad que sufren las plataformas web educativas serían principalmente el mal control de las aplicaciones, la falta de personal calificado para tareas de seguridad y varios otros inconvenientes de raíz humana. Por lo que este trabajo nos daría una idea del tipo de controles y guías que debemos seguir al momento de evaluar la seguridad tecnológica.

Cybersecurity in the Dental Healthcare Sector: The Need of Knowledge for Small Practitioners (Melon, Hernandez, 2020)

Este estudio nos brinda una perspectiva distinta desde la pequeña industria de la odontología, donde el mayor problema es la falta de conocimiento. Según Melon y Hernández existe una falta critica de información en el sector odontológico acerca de información acerca de posibles ataques o peligros que pueden correr estos practicantes o pequeñas empresas, y proponen la inversión de recursos monetarios con el fin de inculcar a estos practicantes con conocimiento, la mejor solución y método de prevención para estos tipos de incidentes. Para este caso, nosotros podemos aplicar estos principios a otros sectores, ya que la situación de desconocimiento es prevalente en varias áreas de trabajo.

Situación Actual de la Empresa

El Hotel Tourblanche fue establecido en el año 2001 para ofrecer sus servicios de hospedaje, alimentación y catering al público en general. Se estableció en ese entonces como una opción accesible pero moderna y elegante tanto para turistas como locales, ubicada en la zona del antiguo Aeropuerto Mariscal Sucre en la ciudad de Quito.

Sin embargo, con la llegada de la nueva terminal para el Aeropuerto el Hotel ha perdido su ubicación estratégica y por consecuencia su atractivo en relación con otros establecimientos dentro del Distrito Metropolitano. No obstante, esto no ha impedido al negocio aventurarse con nuevos proyectos e ideas innovadoras, tales como la inauguración de una cafetería y heladería artesanal junto con la elaboración de productos para su comercialización con marcas reconocidas como Paccari, además de una sucursal del Hotel ubicada en el barrio de San Juan, donde se puede aprovechar la ubicación clave para acomodar mejor a huéspedes.

Es así como este negocio familiar ha logrado mantenerse a flote contra la adversidad y las lastimosas circunstancias que han afectado al sector hotelero en la ciudad de Quito.

Estado Actual del Equipamiento Tecnológico dentro de la Empresa

Dentro del Hotel Tourblanche se cuenta con una infraestructura simple para realizar tareas básicas de computación que se requieren para mantener los procesos del Hotel corriendo a todo momento. A continuación, se listarán los equipos de hardware con los que se cuenta en las instalaciones e información detallada en ciertos casos donde fuese necesario.

- Computadora Personal Dell con Periféricos para Manejo de Procesos Contables y Financieros.
  - Sistema operativo Windows 10 Pro
  - Procesador Intel Core i3 2da generación 3.50 GHz
  - Memoria RAM de 4GB
- Computadora Personal Dell con Periféricos para usos varios en la Recepción.
  - Sistema operativo Windows 7 Professional
  - Procesador Intel Core i5 4ta generación 3.10 GHz
  - Memoria RAM de 8GB
- Impresoras HP Laserjet 1536dnf MFP para manejo de documentos.
- Impresora Epson para manejo de recibos y facturas.
- Router Huawei para recepción del servicio de Internet por parte del proveedor.
- Switch Fast Ethernet Trendnet
- 2 Router Cisco para distribución de redes internas de WiFi.

Dentro de los dispositivos observados, cabe destacar que ambas impresoras son modelos que no cuentan con capacidades de red inalámbrica, por lo que su seguridad dependerá de las configuraciones extendidas a todos los canales de la red cerrada del Hotel.

Además, el Hotel próximamente contará con una página web, la cual será administrada de manera externa a los otros servicios del hotel, pero igual se tomará en cuenta para el propósito de este trabajo.

Capítulo 2: Marco Teórico

MARCO TEORICO

No está fuera de lo común decir que la información es parte esencial de todo tipo de empresas y organizaciones. Estos datos y documentos son bases importantes para varias funciones de cualquier tipo de empresa alrededor del mundo, y permiten el correcto funcionamiento de los departamentos independientemente, sino también comunican y distribuyen información requerida a través de los canales de información.

Es así como hacemos hincapié en la importancia de proteger estos datos y documentos para una organización. Una simple brecha o ataque puede ser devastadora ya que los efectos de un ciberataque se pueden sentir en un nivel elevado, rompiendo los enlaces de confianza con nuestros clientes y empleados, por ejemplo.

Con el fin de resguardar la información y su integridad, se ha establecido el concepto de ciberseguridad. La ciberseguridad se define como un conjunto de buenas prácticas con el propósito de defender computadoras, teléfonos móviles, sistemas de información, servidores, redes y varios otros dispositivos electrónicos de los daños que provocan los ciberataques maliciosos.

“El conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada a los usuarios de las ciber tecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o

recurso de valor para una persona, empresa u organización.” (Gayoso Martínez, Hernández Encinas, & Arroyo Guardeño, 2020)

Esto se logra dentro de una organización mediante el uso y aplicación de un Sistema de Gestión de Seguridad de Información, o SGSI por sus siglas. El SGSI actúa como un sistema de ayuda para la implementación y mejora de la seguridad de la información dentro de una organización, para que esta pueda enfocarse en cumplir con sus objetivos de negocio y progresar de manera positiva dentro de los procesos que realice.

Generalmente, cualquier SGSI se debería regir bajo ciertos estándares de calidad para la seguridad informática, tales como las normas propuestas por NIST o por ISO dentro de sus estándares 27001 y 27002, los cuales comprenden los requerimientos para el despliegue y manejo de un SGSI y las mejores prácticas para la implementación de este sistema, respectivamente.

Dentro de las pautas propuestas por la Cámara de Comercio de Quito, una Pyme se define por tres variables, como se puede observar en la Tabla 1:

Variables	**Microempresa**	**Pequeña Empresa**	**Mediana Empresa**	**Grandes Empresas**
Personal Ocupado	De 1 - 9	De 10 - 49	De 50 – 199	≥ 199
Valor bruto de ventas anuales	≤ 100.000	100.001 – 1.000.000	1.000.001 – 5.000.000	> 5.000.000
Monto de activos	Hasta $100.000	De $100.001 hasta $750.000	De $750.001 hasta $3.999.999	≥ 4.000.000

Tabla 1: Clasificación de las PYMES, Pequeña y Mediana Empresa (S.F)

Para este estudio se utilizará al Hotel Tourblanche como caso de estudio, basados en las métricas anteriormente proporcionadas se tomará en cuenta a esta empresa como una pequeña empresa, debido a la cantidad de colaboradores y trabajadores que conforman el equipo de trabajo. De igual forma, la empresa se encuentra comprendida dentro del Distrito Metropolitano de Quito, y maneja sus actividades comerciales dentro de esta área.

Normas ISO Relacionadas

ISO/ IEC 27032

La norma ISO 27032 está enfocada en la seguridad dentro del ciberespacio y problemas de ciberseguridad que se concentran en atender problemas y riesgos comunes, tales como:

- Ataques de ingeniería social.
- Hacking.
- La proliferación de software malicioso (Malware).
- Spyware
- Otro software potencialmente no deseado.

La guía técnica provee controles para manejar estos riesgos, incluyendo controles como:

- Prepararse para ataques por malware, personas malintencionadas u organizaciones criminales en el Internet.
- Detección y monitoreo de ataques
- Respuestas adecuadas a estos ataques.

Este estándar también se enfoca en la colaboración, ya que existe una necesidad de comunicación, coordinación y manejo de incidentes eficiente y eficaz por parte de todas las partes interesadas de una compañía. Esto con el fin de preservar la privacidad e integridad de los involucrados, que pueden ser personas internas de la empresa como proveedores, y los consumidores o usuarios del producto final. (ISO, Information Technology - Security Techniques - Guidelines for Cybersecurity, 2012)

El estándar también provee un framework para controles de alto nivel, que incluye guías para el manejo de information sharing, coordinación y manejo de incidentes, incluyendo elementos claves para establecer confianza y procesos necesarios para la colaboración e intercambio de información con sus requerimientos técnicos para integración e interoperabilidad entre personas.

El estándar internacional ISO/ IEC 27032 trata los aspectos en particular de:

- Seguridad de la Información
- Seguridad de Redes
- Seguridad del Internet
- Protección de Infraestructuras de Información Critica (CIIP)

ISO 17799:2005

ISO/IEC 17799:2005 establece parámetros y principios generales para la inicialización, implementación, mantenimiento y mejora del manejo de seguridad de la información dentro de una organización. Los objetivos delineados proveen direcciones generales en los objetivos comúnmente aceptados de la seguridad de la información. La norma ISO/IEC 17799:2005 contiene una serie de buenas prácticas para los objetivos de control y se maneja en las siguientes

áreas del manejo de seguridad de la información (ISO, Information Technology - Security Techniques - Code of practice for information security management, 2005):

- Políticas de seguridad.
- Organización de seguridad de la información.
- Manejo de activos.
- Seguridad de recursos humanos.
- Seguridad física y ambiental.
- Manejo de operaciones y comunicaciones.
- Control de accesos.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Manejo de incidentes de seguridad de la información.
- Manejo de continuidad del negocio.
- Conformidad.

NIST

NIST es el acrónimo para el National Institute of Standards of Technology o Instituto Nacional de Estándares de Tecnología, es una agencia regulatoria del Departamento de Comercio de los Estados Unidos que se dedica a promover la innovación en avances científicos y tecnológicos. Sus actividades consisten en desarrollar y mantener estándares de medida, servicios de calidad e investigación tecnológica en áreas como ciberseguridad, biotecnología, nanotecnología, manufactura avanzada, y ciertas otras. NIST ofrece pericia y recursos para apoyar a agencias académicas, industriales y gubernamentales en áreas pertenecientes a la tecnología. Forman un rol crucial en la promoción de estándares y buenas prácticas para asegurar la confiabilidad,

seguridad e interoperabilidad de sistemas y tecnologías en varios entornos del mundo actual. Es por lo que sus publicaciones son reconocidas mundialmente. (Lord, 2023)

Dentro del contexto de esta investigación, se utilizará publicaciones de NIST como la SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs), la cual establece pautas de configuración y monitoreo para redes locales (Souppaya & Scarfone, 2012), o la NISTIR 7621, el cual detalla recomendaciones para pequeñas empresas en cuanto a seguridad de la información y ciberseguridad (Paulsen & Toth, 2016).

OWASP

OWASP es el acrónimo para la Open Worldwide Application Security Project o en español el Proyecto Abierto de Seguridad para Aplicaciones del Mundo es fundación sin ánimo de lucro, cuyo objetivo principal es el de mejorar la seguridad de software alrededor del mundo. Sus actividades incluyen:

- Proyecto de software open source liderados por la comunidad.
- Más de 250 secciones locales en todo el mundo.
- Miles de miembros.
- Conferencias educacionales y entrenamientos con líderes de la industria.

La Fundación OWASP fue lanzada en el 1ro de Diciembre del 2001, y se ha dedicado desde ese entonces a ayudar a varias organizaciones a desarrollar, adquirir, operar y mantener aplicaciones que sean confiables y seguras para su uso público. Todos los materiales que provee OWASP son

gratis y abiertos para cualquiera que desee obtener conocimientos adicionales en seguridad informática. (The OWASP Foundation, s.f.)

FMEA

FMEA son las siglas para el Failure Mode and Effects Analysis o Modo de Fallo y Análisis de Efectos en español. Se define como una aproximación paso por paso para identificar fallos en un diseño, un proceso de manufactura o de ensamblaje, o un producto o servicio. Fue inventado en los años 40s por la Armada Militar de los Estados Unidos y todavía sigue viendo uso en instituciones de renombre en ese país como la NASA.

Dentro de esta metodología se priorizan los fallos de acuerdo con que tan serias sus consecuencias pueden resultar, que tan frecuentemente pueden ocurrir y que tan fácilmente pueden ser detectadas. De manera general, el propósito de FMEA es tomar acciones para eliminar y reducir fallos, empezando con aquellos de mayor impacto y prioridad.

Dentro de FMEA se manejan dos conceptos los cuales son:

- Modos de fallo: Son aquellas formas en que algún proceso puede fallar. Este fallo se define por algún error o defecto, especialmente unos que afectan al cliente o usuario.
- Análisis de efectos: Es un estudio detallado de las consecuencias producidas por los fallos.

Estos dos procesos incluyen también una documentación de conocimientos actuales y acciones a tomarse en caso de riesgos, con el fin de utilizar estas bases en otro proceso de mejoramiento continuo. La metodología se usa también durante las fases de diseño para prevenir fallos en vez de corregirlos, pero se utiliza a través de la vida del producto o servicio como una herramienta de control. (Tague, 2005)

Capítulo 3: Metodologías y Herramientas a Utilizarse

Herramientas Por Utilizarse para las Pruebas

Para realizar las pruebas de penetración y comprobación de seguridad, se hará uso de ciertas herramientas gratuitas que han sido desarrolladas para usarlas de manera libre. El propósito de la utilización de programas que no suponen costo alguno tanto para la empresa como para el evaluador es que, desde la definición de una PYME en el Ecuador, varias empresas simplemente no cuentan con los recursos necesarios para adquirir software que puede tener un costo de hasta miles de dólares. Esta gran cantidad de capital, que puede ser alocado en otros lugares de las empresas que requieran atención más urgente, solo disuade aún más al público sobre la importancia de estos procesos y seguimientos de seguridad informática. Al mantener el costo de esta operación en cero, se esperaría que en un futuro este tipo de estudios haya tomado raíz dentro de la cultura empresarial del país, y que la seguridad de los datos y bienes tecnológicos no se quede en segundo plano.

Kali Linux

Kali Linux es una distribución open source ampliamente conocida para manejar tareas como pruebas de penetración y tareas de ciberseguridad. Se usa mayormente por profesionales en la industria de la ciberseguridad y hackers éticos para evaluaciones de vulnerabilidades en redes y procesos de ingeniería en reversa, en casos más avanzados. Kali Linux es popular porque incluye un vasto número de herramientas y software preinstalado, sirviendo como un punto de entrada

para expertos y novatos buscando una suite de herramientas de seguridad informática de manera gratuita y accesible para todos. (g0tmi1k, 2023)

Nmap:

Nmap o Network Mapper es una utilidad que se encuentra por defecto instalada en Kali Linux. El uso principal para esta herramienta durante esta investigación es el de descubrir y analizar hosts y servicios en la red del Hotel. Nmap es capaz además de expandir su funcionabilidad para buscar vulnerabilidades en redes o firewalls, determinar que puertos se encuentran abiertos, o simular tráfico para generar un análisis de respuesta de la red ante este. (Lyon, n.d.)

Wireshark

Wireshark es una herramienta para analizar paquetes open source que puede ser utilizada para troubleshooting en redes y análisis de protocolos de comunicación. Wireshark es popular debido a que es compatible en varias plataformas, incluyendo Mac, Windows y Linux, y es capaz de manejarse de forma “cross-plataforma”. Se utiliza esta herramienta para colocar controladores de interfaces de red para lograr observar todo el tráfico que pasa por una interfaz de red. Combinado con la interfaz gráfica del programa, uno puede analizar el tráfico de una red para detectar posibles sitios web vulnerables que se pueda estar accediendo en un dispositivo. (Combs, s.f.)

SSLScan

SSLScan es un software que realiza pruebas sobre los servicios de SSL y TLS en servidores que proveen un servicio de red. El propósito de esta herramienta es el de encontrar los SSL Ciphers que se utilizan dentro de un servidor. Estos ciphers son una serie de algoritmos o instrucciones que ayudan a establecer una conexión segura entre dos entidades. En este caso, se utiliza esta herramienta para calificar los métodos de conexión dentro de la red del Hotel. (Testa, 2023)

TheHarvester

TheHarvester es una herramienta principalmente usada para el reconocimiento de factores y elementos relacionados a una red, como, por ejemplo:

- Nombres de personas dentro de una organización.
- Correos pertenecientes al dominio de la organización.
- Direcciones IP y subdominios pertenecientes.

Esta herramienta lleva a cabo esta búsqueda mediante un proceso de recolección de inteligencia por fuentes abiertas. Es decir, la información que TheHarvester recolecta es aquella que una persona cualquiera puede descubrir por su cuenta en el internet. (Brown, Townsend, & Baird, 2023)

BED

BED o Bruteforce Exploit Detector es un software que es parte de Kali Linux y sirve para detectar vulnerabilidades mediante la revisión de ciertos daemons. BED trata de encontrar overflows en el buffer o en números enteros, errores en el formato de variables o strings, etc.

Este programa es mayormente usado dentro de tests de penetración para encontrar los tipos de vulnerabilidades más simples en un servidor. (Klimaszewski, 2023)

Aplicación y Procedimiento de la Metodología

La aplicación de esta metodología se realizará siguiendo los pasos siguientes:

1. Determinar qué necesita ser atendido:

   Dentro de esta fase se analizará las áreas de la organización donde se realizará esta actividad. Se requiere la revisión de procesos, sistemas o cualquier elemento de la empresa que requiera atención bajo nuestro criterio, con el fin de mantener el enfoque de la actividad dentro de estas áreas. En este caso, el análisis se centrará en los recursos tecnológicos del Hotel, ya sean equipos de computación, redes, o páginas web, con un enfoque adicional en el área de la seguridad tecnológica que engloba estos elementos.

2. Analizar los procesos y sistemas:

   Para esta fase, se utilizará varios recursos para la recolección de datos, que nos permitan observar que áreas de la parte tecnológica del Hotel son las que sufren en cuanto a temas de vulnerabilidad, baja seguridad, o falta de precaución. En esta fase se determinará los modos de fallo de cada uno de los procesos evaluados, anotando las formas en que un determinado sistema puede estar en riesgo o puede fallar en cualquier momento.

3. Hallar el nivel de prioridad para los procesos:

En esta etapa de análisis se confiere una puntuación general a cada uno de los procesos y sus modos de fallo analizados en el anterior paso. Esto con el fin de ordenar a cada uno de los problemas según esta puntuación para determinar que problemas existen con mayor riesgo a la organización y ayudar a la toma de decisiones cuando sea tiempo de plantear soluciones a estos problemas.

4. Proponer cambios o soluciones:

   Una vez se haya establecido los problemas dentro del área, se procederá a listar posibles soluciones que la empresa puede aplicar para mejorar o resolver estos obstáculos, considerando las posibilidades de la organización y cuidando que estos cambios sean accesibles para el Hotel.

5. Monitorear la posible implementación y efectividad de los cambios:

   Terminado el proceso de mejora, dentro del futuro se puede buscar una evaluación próxima a los cambios propuestos, ya sea que estos se hayan implementado o no. De ser necesario, se puede repetir periódicamente los procesos anteriores para evaluar una vez más el estado del área tecnológica del Hotel.

Cabe destacar también que normalmente la metodología FMEA se realiza en conjunto con un equipo de trabajo, formado por un profesional que lidera el grupo y es usualmente quien tiene mayor conocimiento acerca del área o de los procesos que se van a evaluar, además de miembros propios del grupo o empresa a observarse, quienes pueden proveer contexto acerca del ambiente en el que se desarrollan los procesos o sistemas. En este caso, debido a que el Hotel no cuenta con un departamento dedicado a la tecnología o ninguna persona a cargo, se ha omitido estas fases de creación de un grupo de trabajo, ya que es un análisis primerizo para la empresa.

Para esta aplicación de FMEA se utilizará un procedimiento regular que se moldeará para ajustarse a las necesidades del Hotel. La implementación seguirá los pasos recomendados para la aplicación del procedimiento para cada uno de los fallos encontrados por las herramientas anteriormente listadas. Se utilizará un formato como el siguiente para presentar la información de resultados obtenidos, fallos registrados, consecuencias relacionadas, entre otros, además de la definición para ciertos conceptos que se utilizan en su realización. Este procedimiento modificado puede ser observado en la Tabla 2.

Severidad: El impacto que tiene un evento de fallo. Se puntúa en una escala del 1 al 10, siendo un 10 la calificación máxima para un evento del mayor riesgo.

Ocurrencia: Frecuencia en la que ocurre un evento de fallo. Se puntúa en una escala del 1 al 10, entendiéndose que un 10 significa un evento con gran probabilidad de ocurrencia.

Detección: Habilidad de procesar el control de detección de ocurrencias para eventos de fallo. Se asigna una calificación del 1 al 10, donde un evento con menor calificación es aquello que puede ser detectado fácilmente por el control de procesos.

Numero de prioridad de riesgo: La puntuación promedio de un proceso evaluado. Se calcula multiplicando las puntuaciones para la severidad, ocurrencia y detección. Un evento que puntúa alto en esta categoría es uno que demanda atención inmediata, mientras que uno con menor puntuación es menos riesgoso.

Proceso Por Evaluarse	Modos de Fallo Potenciales	Consecuencias Potenciales	Nivel de Severidad	Causas Potenciales	Nivel de Ocurrencia	Controles Existentes	Probabilidad de Detección	Numero de Prioridad de Riesgo	Acción Recomendada
Aquel parte de un sistema o proceso del Hotel que se va a evaluar.	¿En qué manera puede fallar el proceso anterior?	¿Cuál es el impacto sobre el usuario si el fallo no es prevenidos o corregido?	¿Qué tan severo es el efecto sobre el usuario?	¿Qué es lo que causa que el fallo ocurra?	¿Qué tan frecuentemente puede ocurrir el fallo?	¿Cuáles son las pautas existentes que prevén o detectan a un fallo?	¿Qué tan probable es la detección del fallo o de su causa?	Número de prioridad de riesgo calculado.	¿Cuáles son las acciones para reducir la ocurrencia o para mejorar su detección?

Tabla 2: Modelo de Evaluación de FMAE para el Hotel Tourblanche (Serrano, 2023)

Aplicación de Herramientas

En esta sección se mostrarán los resultados de la aplicación del software escogido sobre los recintos del Hotel, y se observará de manera breve los resultados que se han obtenido.

Aplicación de The Harvester

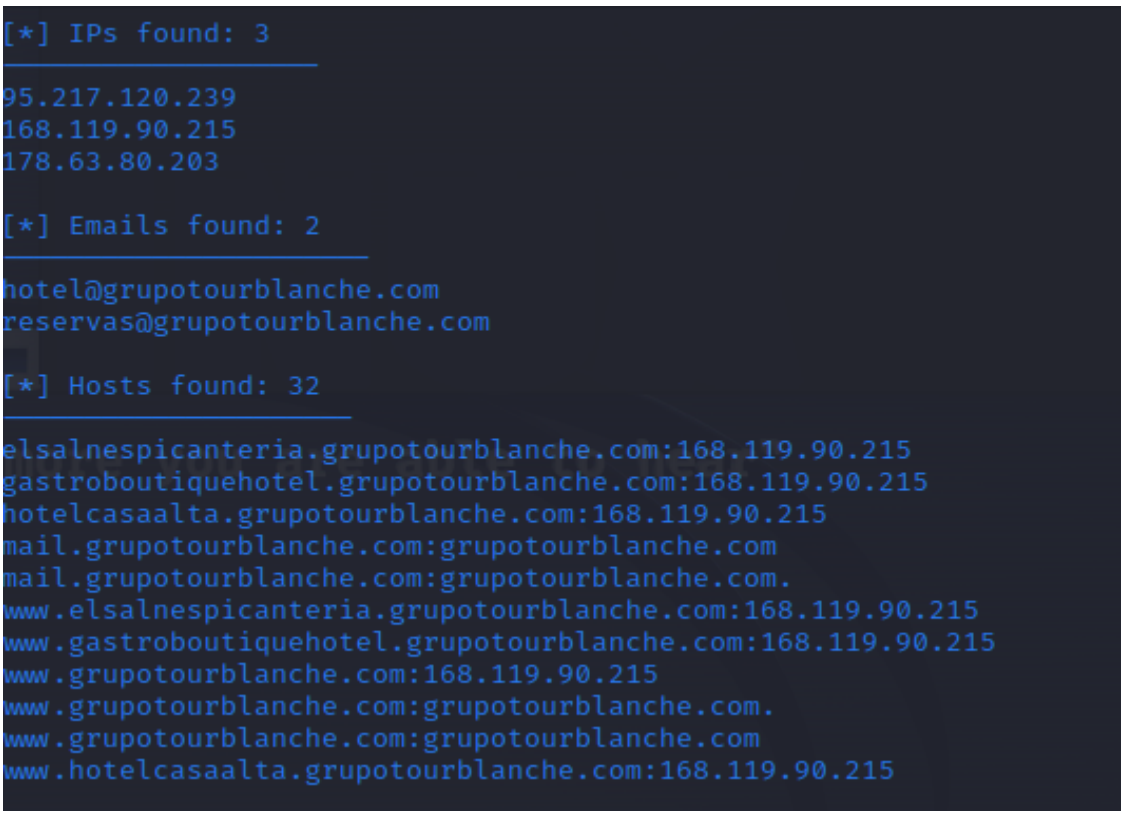


Figura 1: Lista de Dominios Pertenecientes encontrados por TheHarvester

Para comenzar con el proceso de análisis, se procedió a recolectar información sobre el Hotel y sus direcciones de red con TheHarvester, el cual nos provee información que podemos utilizar dentro de las otras herramientas. Se pueden observar estos resultados en la Figura 1.

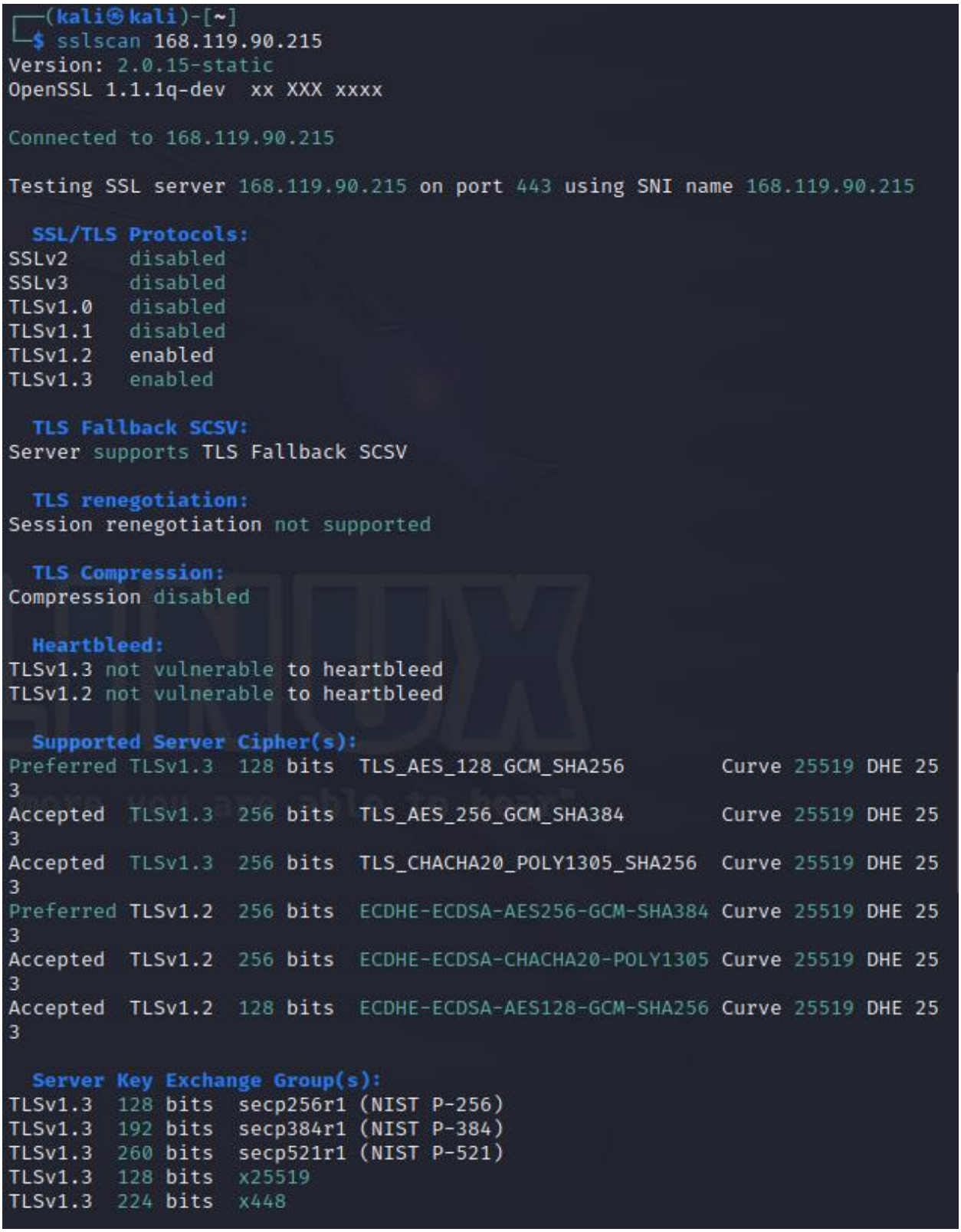


Figura 2: Resultados del Análisis por SSLScan Parte 1

Aplicación de SSLScan

Primeramente, en SSLScan podemos notar en las Figuras 2 y 3 que los protocolos de SSL y TLS están debidamente desactivados en caso de no necesitarlos, que es lo que ocurre en este caso, solo se está usando TLS 1.2. Se puede observar también que en la sección de ciphers soportados podemos utilizar el protocolo TLS 1.3, el cual es más recomendado en la época actual y si valiese la pena, ya que cuenta con el suficiente soporte para ser una mejora significativa. Si el servidor lo soporta, se puede usar la versión de TLS AES de TLS. Podemos observar también que existen ciertos elementos de TLS que pueden ser o no compatibles con tanto la versión de TLS que se está utilizando para comunicación como con las características del servidor que se está evaluando. Dentro de este escaneo se pueden observar tres funciones: El TLS Fallback, TLS Renegotiation y TLS Compression. A continuación, se incluirá detalles acerca de estos elementos y su impacto:

- TLS Fallback SCSV es una señal que protege a un servidor de una posible vulnerabilidad causada por un protocolo de menor nivel siendo usado para una comunicación. Usualmente durante una transmisión, ambos servidores anuncian la versión de TLS más avanzada y segura que tienen, para utilizar una versión que ambos hosts soporten. Es así como un servidor con una versión avanzada y más segura puede volverse vulnerable si acepta una

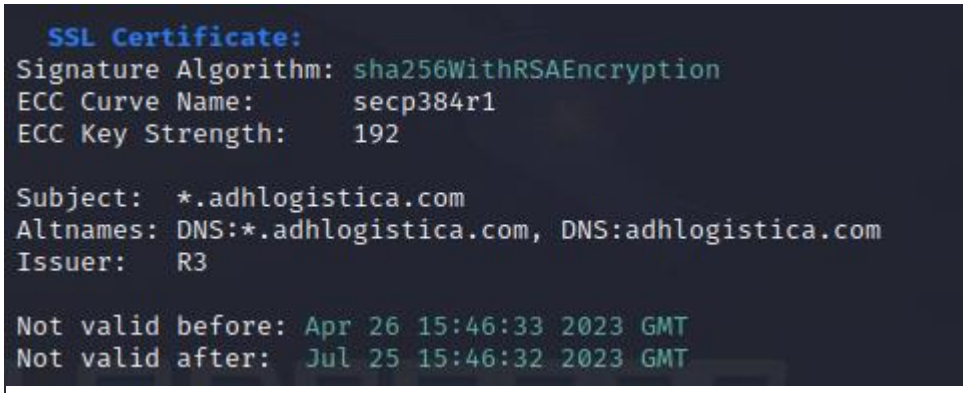


Figura 3: Resultados del Análisis por SSLScan Parte 2

conexión de un servidor antiguo. La señal de Fallback prevé entonces cualquier conexión con un servidor que no tenga una versión similar a la que posee, por lo que es bastante recomendado tener configurada esta señal en un servidor. (Moeller & Langley, 2015)

- TLS Renegotiation es un proceso donde un servidor realiza un nuevo handshake, o verificación del servidor con el que se está conectando durante una sesión segura ya existente. El cliente o el servidor pueden iniciar este proceso, y sirve para verificar las credenciales y la seguridad de una conexión mientras la conexión se realiza, y no solo cuando se establece. (IBM, 2021) Sin embargo, no todas las implementaciones de SSL y TLS soportan esta interacción. Específicamente, TLSv1.3 no está soportado a pesar de ser la versión más nueva del protocolo, y la versión de TLS actualmente usada por el Hotel tampoco lo soporta, por lo que podemos presentar esta falta como una vulnerabilidad.
- TLS Compression es una característica de TLS que permite reducir el tamaño de datos encriptados mediante un algoritmo de compresión antes de la encriptación de los datos. Esto tiene la ventaja de mejorar el rendimiento de una aplicación, usando más eficientemente los recursos de banda ancha para transmisión. (Linkedin Collaborative Articles, 2023)

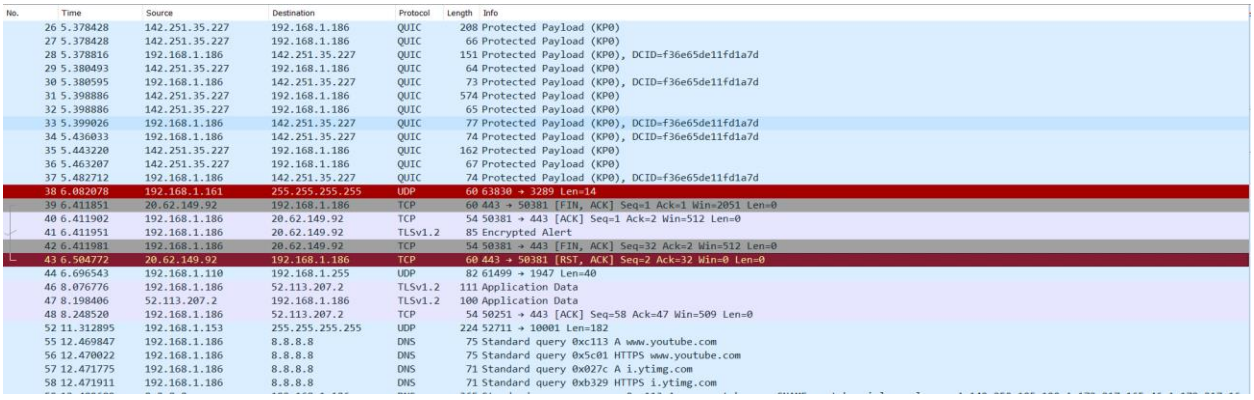
  Sin embargo, debido a ciertas vulnerabilidades que pueden presentarse debido al uso de exploradores de internet antiguos, es recomendable no utilizar el método de compresión, debido a que existen ciertos tipos de ataques que utilizan cookies de usuario hackeadas para tomar control de la información en un servidor web, lo cual es solamente posible si se tienen ciertos tipos de métodos de compresión habilitados. (Hollenbeck, 2004)

En su mayoría se utilizan las nuevas versiones de SHA, como SHA256 y SHA384, las cuales son bastante seguras y son recomendadas universalmente. de 256 bits, pero existe una de 128 bits

en caso de que la versión superior cause ralentizaciones. Por último, en esta sección, podemos notar el tipo de algoritmo de hashing que utiliza esa implementación de que la versión superior cause ralentizaciones. por último, en esta sección, podemos notar el tipo de algoritmo de hashing que utiliza esa implementación (The SSL Store, 2020).

Aplicación de Wireshark

Dentro de Wireshark podemos observar un intercambio de paquetes que se encuentra marcado como rojo, o potencialmente peligroso dentro de la Figura 4. Analizando más a profundidad las direcciones de donde provienen estas conexiones podemos determinar que la primera dirección que ha sido reportada como posiblemente peligrosa es la dirección de broadcast reservada, la cual es usada por ciertos protocolos para transmitir información a cada uno de los dispositivos de una red local, donde esta información es privada y solo se extiende hacia los dispositivos conectados dentro de la red. La siguiente dirección marcada como posiblemente peligrosa es una dirección IP de verdad, por lo que podemos determinar información acerca de esta mediante el uso de una herramienta gratuita en el Internet. Para este caso se ha utilizado el sitio web gratuito Whatismyipaddress.com, y el resultado se puede observar en la Figura 5:



No.	Time	Source	Destination	Protocol	Length	Info
26	5.378428	142.251.35.227	192.168.1.186	QUIC	208	Protected Payload (KP0)
27	5.378428	142.251.35.227	192.168.1.186	QUIC	66	Protected Payload (KP0)
28	5.378816	192.168.1.186	142.251.35.227	QUIC	151	Protected Payload (KP0), DCID=f36e65de11fd1a7d
29	5.380493	142.251.35.227	192.168.1.186	QUIC	64	Protected Payload (KP0)
30	5.380595	192.168.1.186	142.251.35.227	QUIC	73	Protected Payload (KP0), DCID=f36e65de11fd1a7d
31	5.398886	142.251.35.227	192.168.1.186	QUIC	574	Protected Payload (KP0)
32	5.398886	142.251.35.227	192.168.1.186	QUIC	65	Protected Payload (KP0)
33	5.399026	192.168.1.186	142.251.35.227	QUIC	77	Protected Payload (KP0), DCID=f36e65de11fd1a7d
34	5.436033	192.168.1.186	142.251.35.227	QUIC	74	Protected Payload (KP0), DCID=f36e65de11fd1a7d
35	5.443220	142.251.35.227	192.168.1.186	QUIC	162	Protected Payload (KP0)
36	5.463207	142.251.35.227	192.168.1.186	QUIC	67	Protected Payload (KP0)
37	5.482712	192.168.1.186	142.251.35.227	QUIC	74	Protected Payload (KP0), DCID=f36e65de11fd1a7d
38	6.082078	192.168.1.161	255.255.255.255	UDP	60	63830 → 3289 Len=14
39	6.411851	20.62.149.92	192.168.1.186	TCP	60	443 → 50381 [FIN, ACK] Seq=1 Ack=1 Win=2051 Len=0
40	6.411902	192.168.1.186	20.62.149.92	TCP	54	50381 → 443 [ACK] Seq=1 Ack=2 Win=512 Len=0
41	6.411951	192.168.1.186	20.62.149.92	TLSv1.2	85	Encrypted Alert
42	6.411981	192.168.1.186	20.62.149.92	TCP	54	50381 → 443 [FIN, ACK] Seq=32 Ack=2 Win=512 Len=0
43	6.504772	20.62.149.92	192.168.1.186	TCP	60	443 → 50381 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
44	6.696543	192.168.1.110	192.168.1.255	UDP	82	61499 → 1947 Len=40
46	8.076776	192.168.1.186	52.113.207.2	TLSv1.2	111	Application Data
47	8.198406	52.113.207.2	192.168.1.186	TLSv1.2	100	Application Data
48	8.248520	192.168.1.186	52.113.207.2	TCP	54	50251 → 443 [ACK] Seq=58 Ack=47 Win=509 Len=0
52	11.312895	192.168.1.153	255.255.255.255	UDP	224	52711 → 10001 Len=182
55	12.469847	192.168.1.186	8.8.8.8	DNS	75	Standard query 0xc113 A www.youtube.com
56	12.470022	192.168.1.186	8.8.8.8	DNS	75	Standard query 0x5c01 HTTPS www.youtube.com
57	12.471775	192.168.1.186	8.8.8.8	DNS	71	Standard query 0x027c A i.ytimg.com
58	12.471911	192.168.1.186	8.8.8.8	DNS	71	Standard query 0xb329 HTTPS i.ytimg.com

Figura 4: Resultados del Análisis por Wireshark

Como se puede observar, la dirección pertenece a Microsoft, específicamente a uno de sus Datacenters ubicado en Estados Unidos. Siendo que esta dirección está siendo reconocida por la

corporación Microsoft misma, el intercambio solo ha sido de un paquete, y se ha observado intercambios parecidos en el log de Wireshark con otras empresas de tecnología como Google, podemos deducir que el riesgo que supone esta comunicación es bastante mínimo.

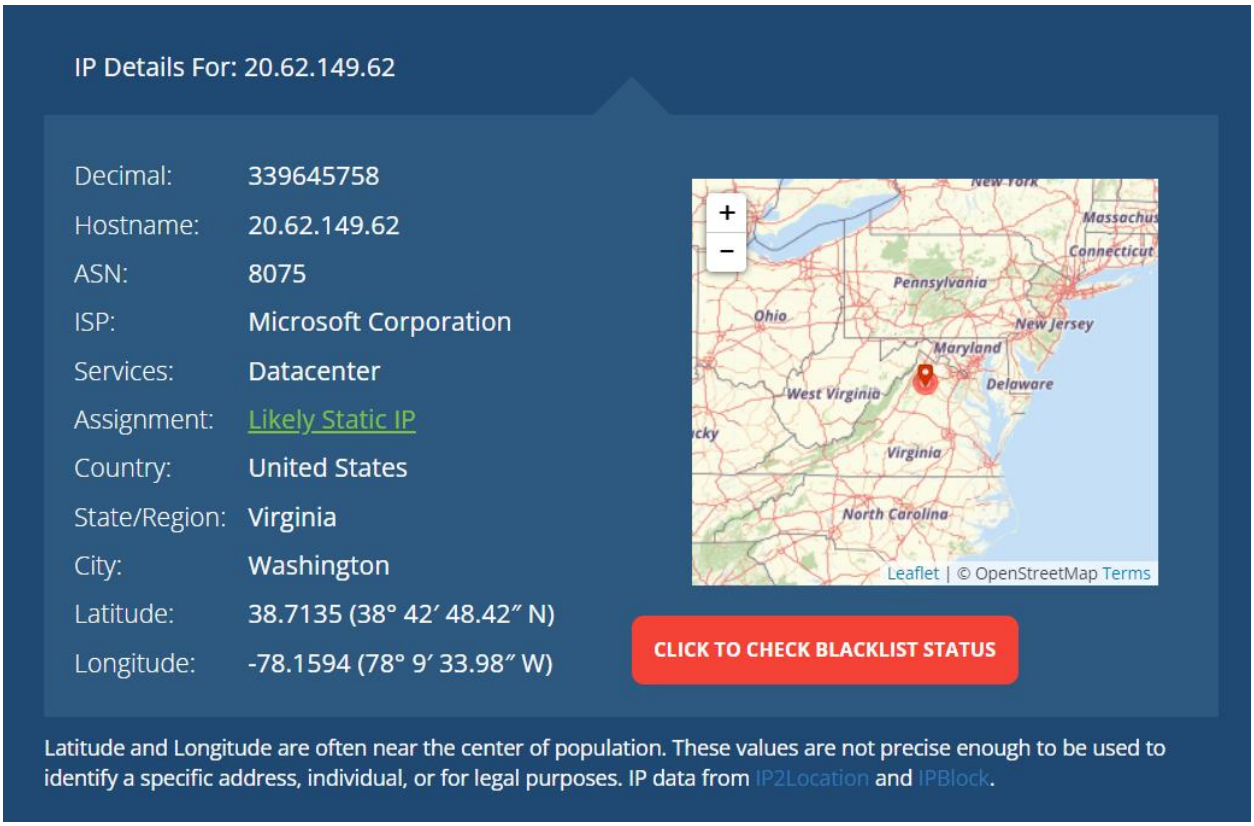


Figura 5: Resultado del Análisis de Dirección IP

Aplicación de BED:

En el caso de BED la utilización es bastante simple, requerimos darle al programa cuatro argumentos: Primero especificamos el protocolo que vamos a escanear agregando -s, después con el argumento -t dirigimos el programa hacia la dirección IP de nuestro objetivo, y por último especificamos el puerto de evaluación con -p y un tiempo de finalización en caso de que la conexión sea interrumpida, con el argumento -o. En este caso, vamos a evaluar el puerto 80 para HTTP con el fin de encontrar vulnerabilidades en el servidor web de la red del Hotel. Los resultados los podemos observar a continuación en las Figuras 6, 7 y 8:

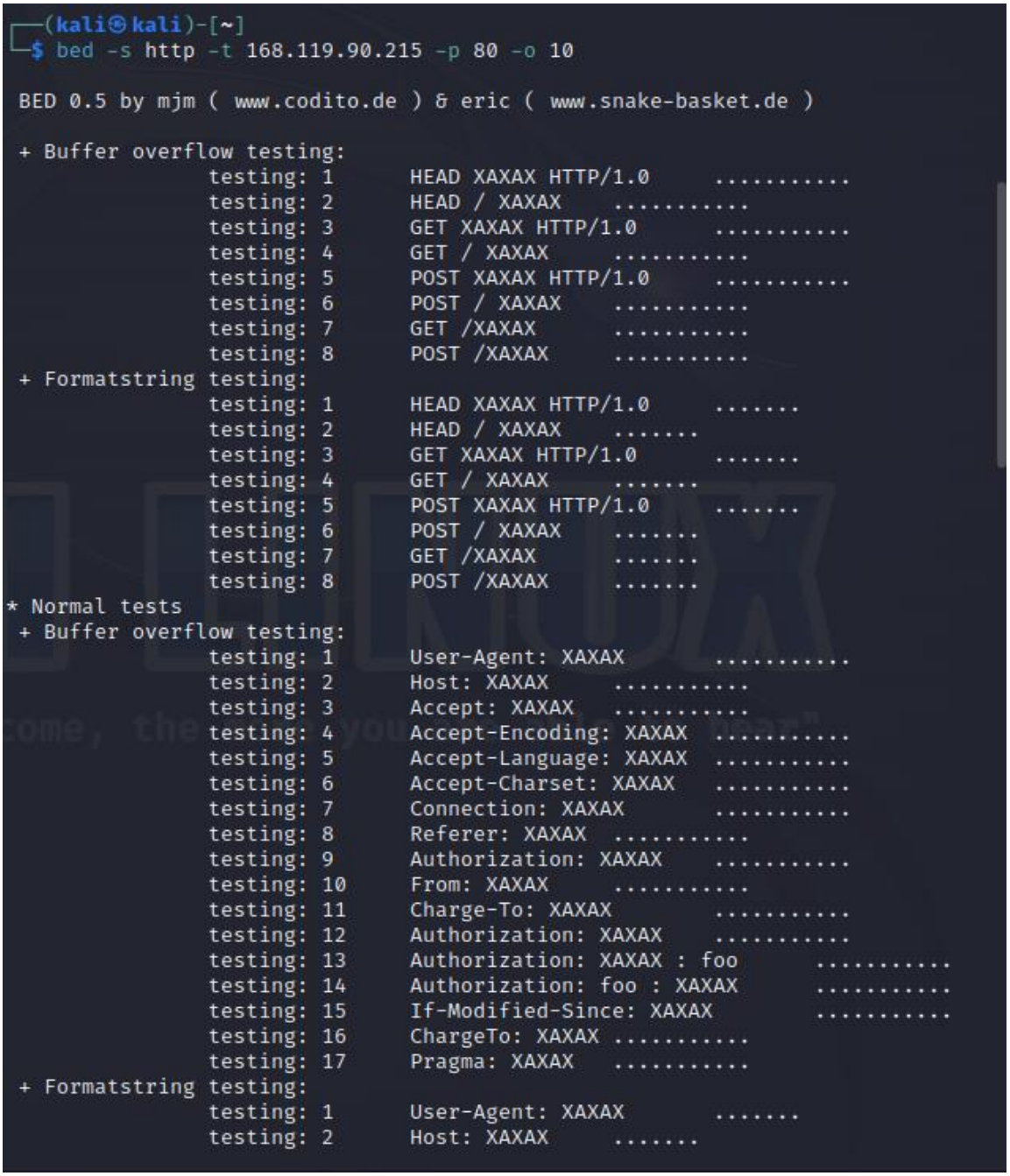


Figura 6: Resultados del Análisis por BED Parte 1

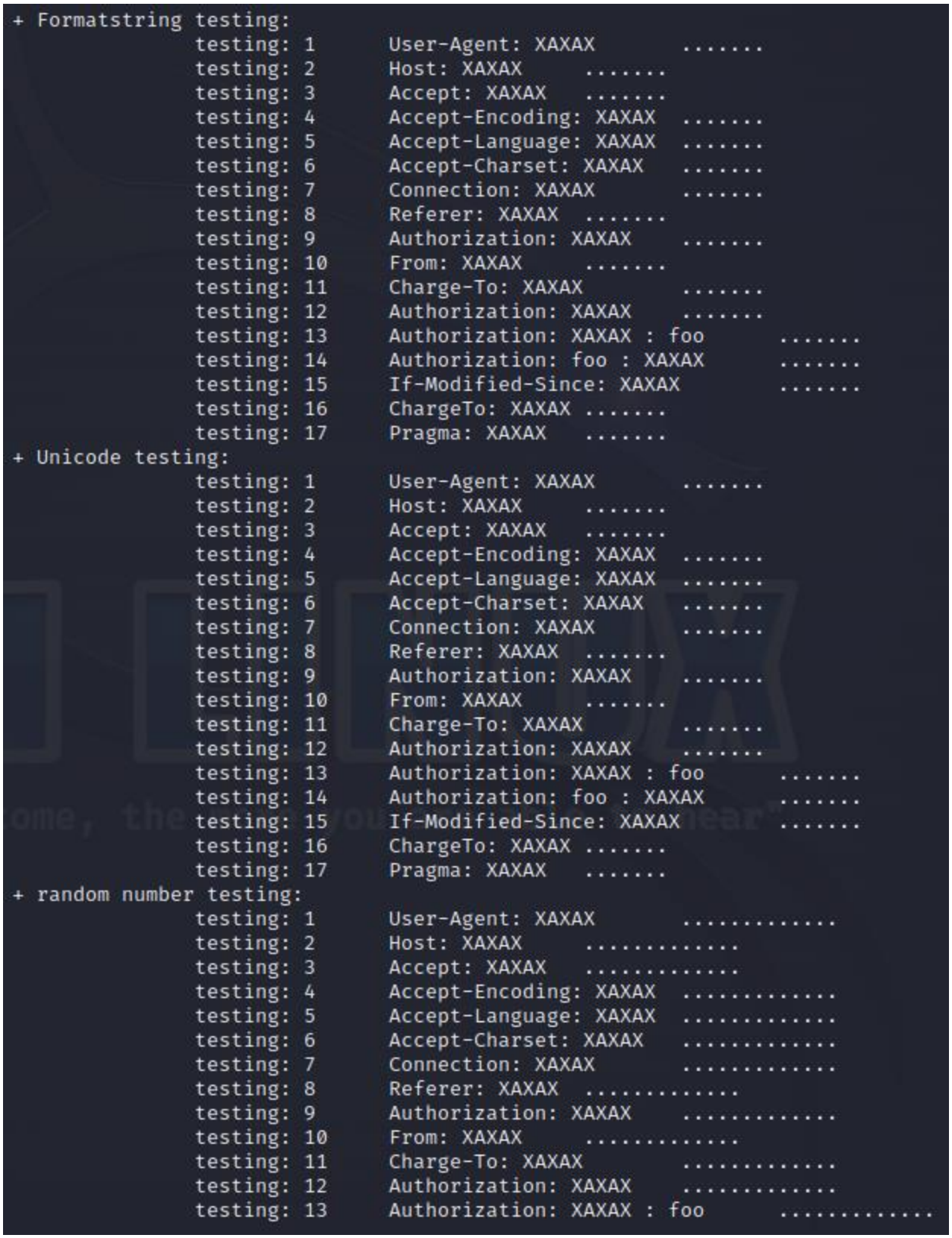


Figura 7: Resultados del Análisis por BED Parte 2

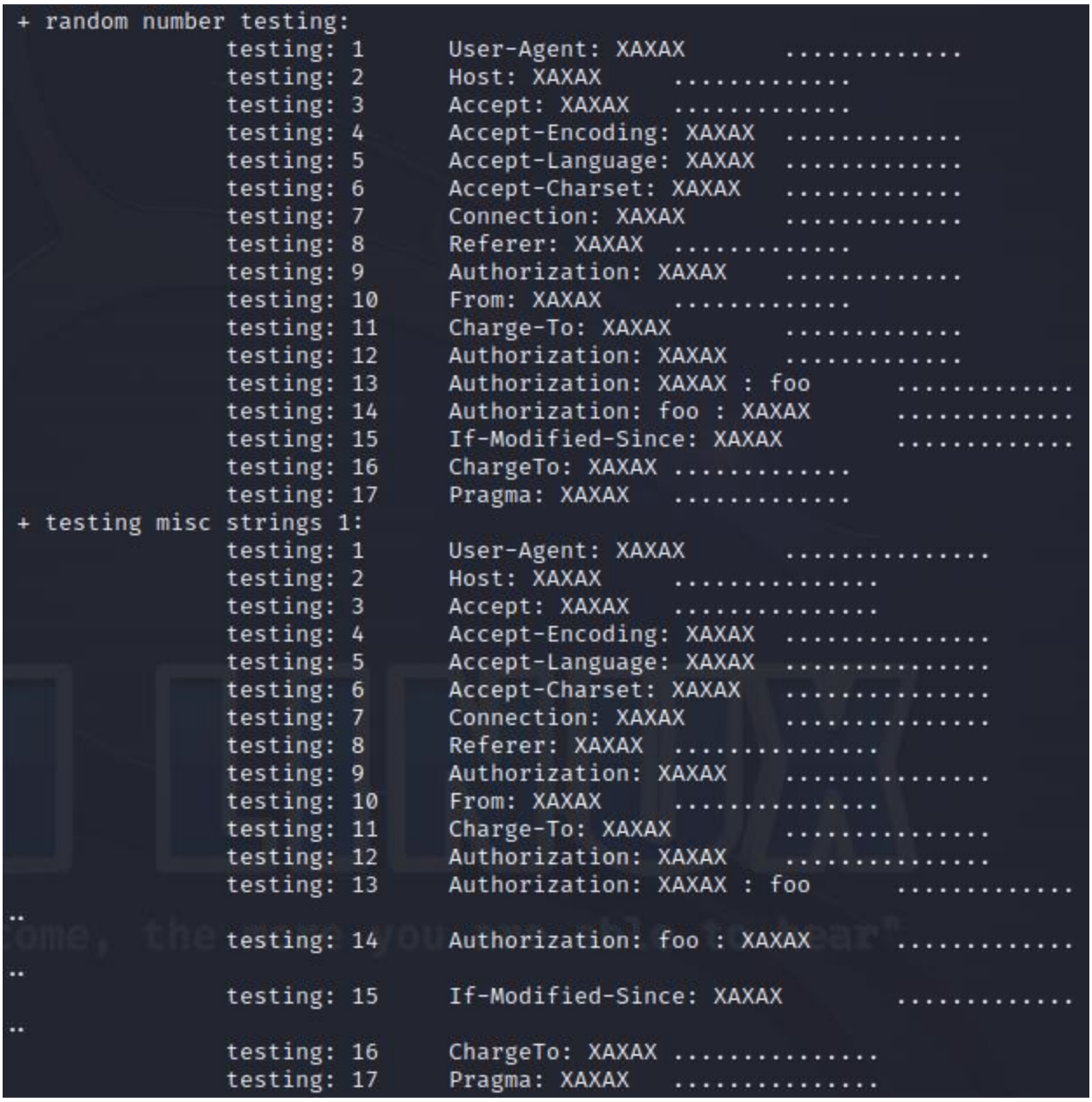


Figura 8: Resultados del Análisis por BED Parte 3

Después del laborioso análisis, BED afortunadamente no encontró ninguna vulnerabilidad dentro de nuestro objetivo, por lo que podemos descartar la posibilidad de encontrar un punto de entrada para un ciberataque por esta ruta.

Aplicación de Nmap:

Dentro de Nmap existe una variedad grande de comandos y pruebas que podemos implementar para realizar un análisis de vulnerabilidades, pero Nmap nos ofrece una alternativa más cómoda en la forma de scripts, los cuales permiten correr varios comandos de análisis similares simultáneamente, simplificando así el proceso de análisis. Para el propósito de este trabajo, se ha designado un script para cumplir con el objetivo de la evaluación para este caso. El script en cuestión se denomina safe, debido a que utiliza métodos que son menos probables que sean detectados como una amenaza por un servidor. Esto nos permite realizar una prueba con un costo de banda ancha mínimo, pero manteniendo la misma cualidad de análisis de vulnerabilidades en una red (Lyon, s.f.). A continuación, se presentará los resultados del análisis en las Figuras 9, 10, 11 y 12:

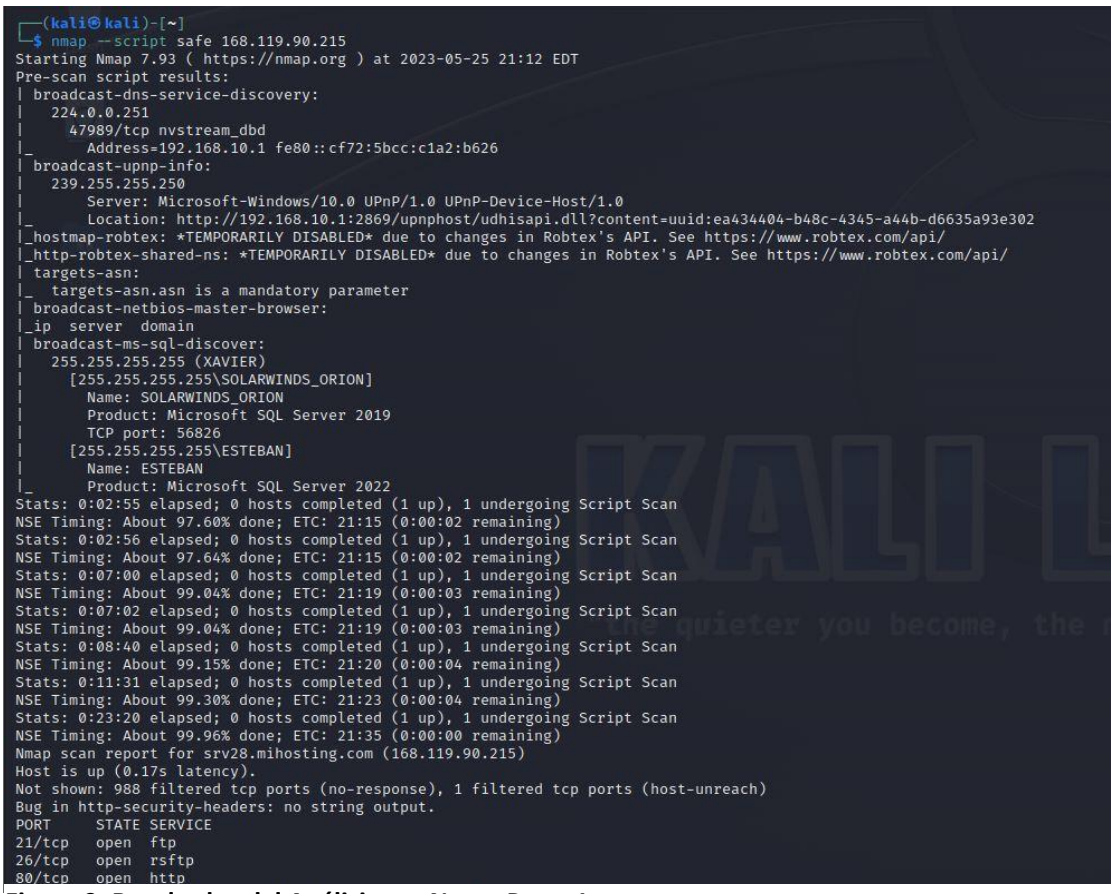


Figura 9: Resultados del Análisis por Nmap Parte 1

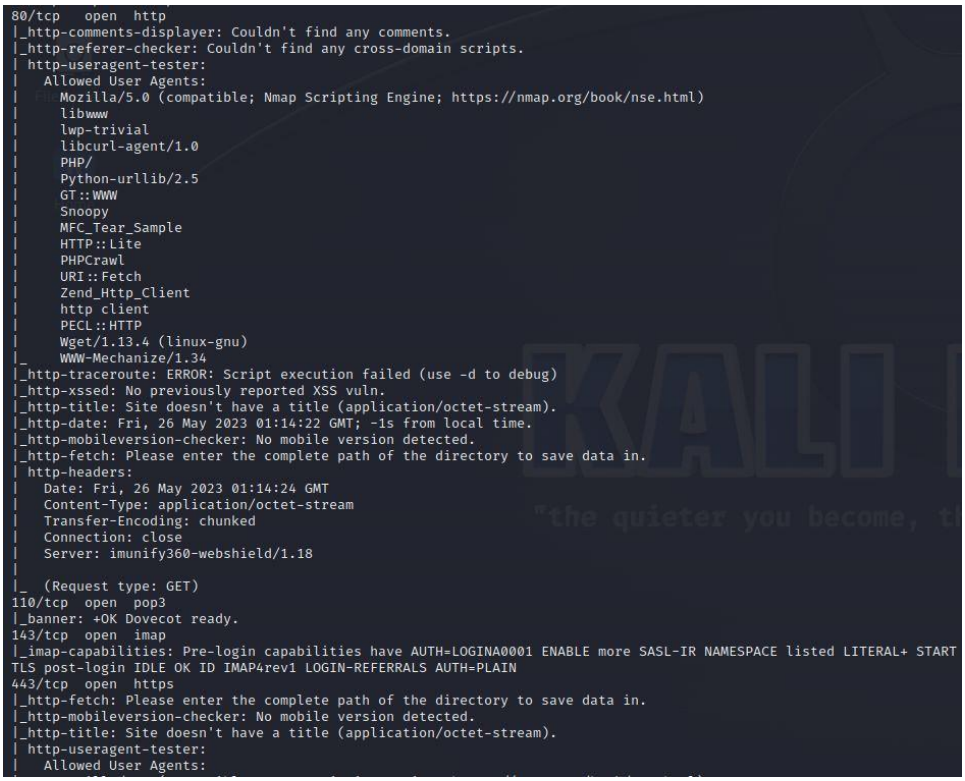


Figura 10: Resultados del Análisis por Nmap Parte 2

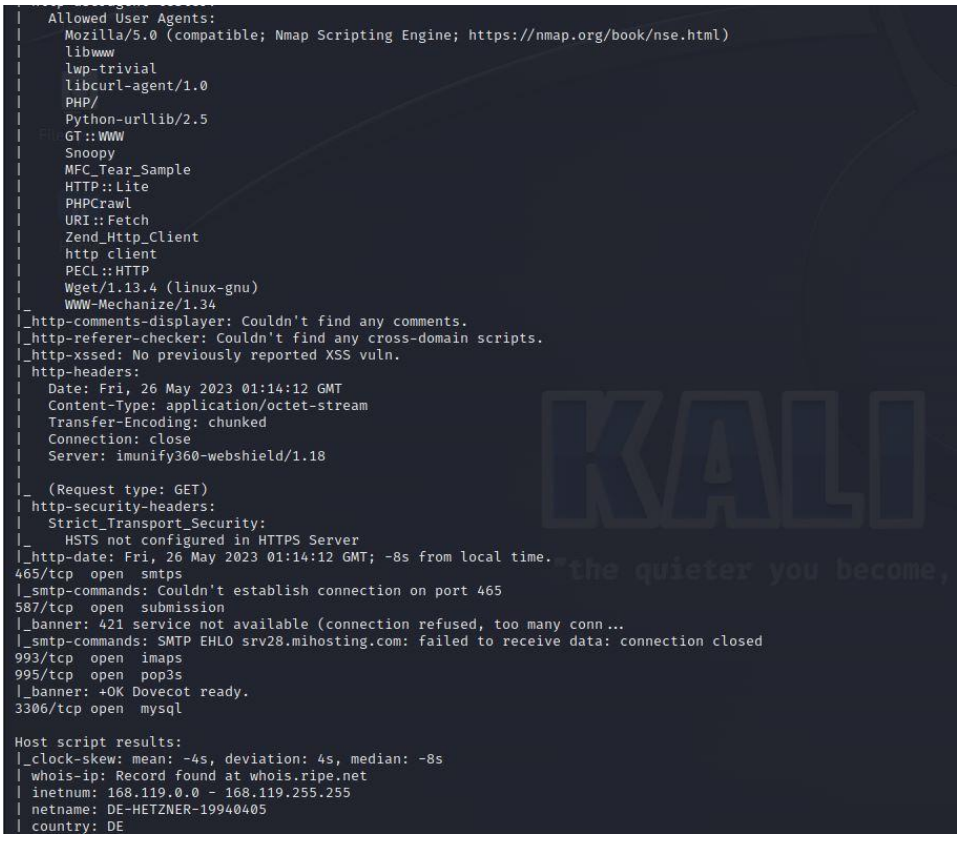


Figura 11: Resultados del Análisis por Nmap Parte 3

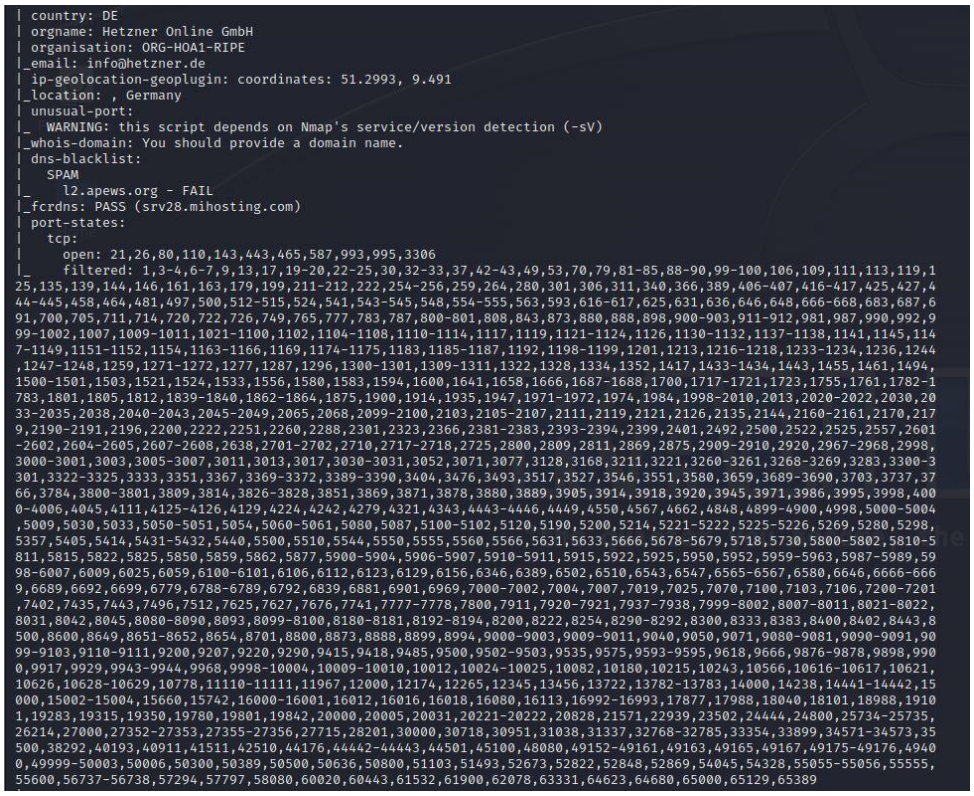


Figura 12: Resultados del Análisis por Nmap Parte 3



Figura 13: Resultados del Análisis por Nmap Parte 4

Terminada la ejecución podemos concluir que Nmap no ha encontrado mayores vulnerabilidades, y podemos determinar unos cuantos elementos donde podemos enfocarnos para encontrar posibles mejoras. En particular, en la Figura 11 podemos observar la siguiente línea: “HSTS not configured in HTTPS Server”, el cual hace alusión a HTTP Strict Transport Security, una política que establece regulaciones para una conexión entre usuario y servidor por HTTPS. La falta de este protocolo se

considera una vulnerabilidad media, ya que puede poner a los usuarios de una página web en riesgo si la página utiliza enlaces de redirección, para poder prevenir ciertos ataques contra las cookies de navegador y algunos protocolos. (Hodges, 2012)

Capítulo 4: Análisis de Resultados

Aplicación de la Metodología

En este capítulo se procederá con el ingreso de la información previamente obtenida con las herramientas tecnológicas a la matriz de análisis de errores creada para este proyecto, con el fin de determinar su nivel de riesgo hacia la empresa, y próximamente analizar ciertas soluciones posibles que puede implementarse para resolver las cuestiones de más alto riesgo.

Presentación de Matrices de Trabajo

A continuación, se presentarán varias tablas dedicadas al análisis individual por cada vulnerabilidad encontrada, ya sea por medio de observación en persona o hecha notar por un miembro del Hotel, o encontrada gracias al uso de las herramientas de software anteriormente presentadas.

Vulnerabilidades Descubiertas Sin Herramientas

Proceso Por Evaluarse	Modos de Fallo Potenciales	Consecuencias Potenciales	Nivel de Severidad	Causas Potenciales	Nivel de Ocurrencia	Controles Existentes	Probabilidad de Detección	Numero de Prioridad de Riesgo	Acción Recomendada
Equipos de Computación del Hotel	Un pendrive infectado con malware puede llegar hacia uno de los equipos.	Los equipos del Hotel pueden estar comprometidos, y los sistemas pueden dejar de funcionar adecuadamente.	5	Malware proveniente de un dispositivo externo, ciberataque por una vulnerabilidad resultante.	4	Consulta interna con una persona a cargo (Gerente, Dueño del Hotel, etc.).	7	140	Capacitar al personal para reducir incidencias de este tipo.
Equipos de Computación del Hotel	Correos potencialmente peligrosos (phishing, estafas, etc.)	Posible pérdida de información vulnerable.	5	Falta de capacitación frente a situaciones similares.	5	Consulta interna a una persona a cargo (Gerente, Dueño del Hotel, etc.)	6	150	Informar a todo el personal del Hotel sobre este tema, dando advertencias y ejemplos concisos.
Equipos de Computación del Hotel	Dispositivos personales infectados con malware	Infección de dispositivos propios de la empresa.	6	Conexión a una red inalámbrica insegura, falta de protección contra ataques en dispositivos personales.	3	Consulta con un Agente Externo de Sistemas para análisis personalizado.	7	126	Consultando frecuentemente con el Agente Externo para realizar análisis periódicos.

Tabla 3: Vulnerabilidades Descubiertas Sin Herramientas

Vulnerabilidades Descubiertas por Herramientas

Proceso Por Evaluarse	Modos de Fallo Potenciales	Consecuencias Potenciales	Nivel de Severidad	Causas Potenciales	Nivel de Ocurrencia	Controles Existentes	Probabilidad de Detección	Numero de Prioridad de Riesgo	Acción Recomendada
Servidor Web	Ciberataque mediante vulnerabilidad criptográfica	Caída del sistema mientras ocurre el percance. Potencial pérdida o robo de información	8	Versión de protocolo TLS desactualizada.	4	Ninguno	3	96	Contactar con el servicio de hosting para que ellos puedan implementar una versión de TLS más avanzada.
Servidor Web	Posible tráfico de red no deseado y peligroso (Intervención Maliciosa de Red	Inyección de malware, robo o perdida de información	8	Posible backdoor causado por malware que ha atacado previamente.	4	Ninguno	5	160	Realizar un análisis de tráfico periódicamente. Implementar un sniffer de tráfico para analizar el tráfico más pendiente.
Página Web	Ataques de robo de información sobre la página web y sus usuarios	Robo o pérdida de información	8	Falta de uso de protocolos de seguridad en la página.	5	Ninguno	3	120	Contactar al hosting para que implementen protocolos web más seguros

Tabla 4: Vulnerabilidades Descubiertas por Herramientas

Clasificación de Posibles Problemas según Nivel de Riesgo

Una vez concluida la tabulación de resultados de los diversos análisis, podemos determinar el orden en el que deberían resolverse estos problemas según la metodología escogida. Cabe aclarar que los resultados de este análisis son bastante bajos en la escala de riesgo total posible, que puede llegar hasta el número 1000. Sin embargo, los problemas en sí deberían ser resueltos a la medida de lo posible.

i. Intervención Maliciosa de la Red del Hotel – 160 puntos
ii. Correos Potencialmente Peligrosos (Phishing o Estafas) – 150 puntos
iii. Pendrives o Dispositivos Externos Infectados – 140 puntos
iv. Dispositivos Personales Infectados con Malware – 126 puntos
v. Ataques de Robo de Información sobre la Página Web – 120 puntos
vi. Ciberataque por Vulnerabilidad Criptográfica – 96 puntos

Posibles Soluciones

A pesar de que se ha previsto una serie de soluciones preliminares en las Tablas 3 y 4, podemos definir un plan de trabajo preliminar, para que el Hotel pueda evaluar estas soluciones de acuerdo con su capacidad adquisitiva y nivel de entendimiento de los problemas encontrados.

Problemas Físicos:

Para solventar los problemas físicos, los cuales son los que acabaron con mayor nivel de riesgo en promedio, el Hotel debería implementar una serie de pautas a seguir para sus empleados y

líderes. Tener una guía que detalle protocolos a seguir ayudaría no solo a prevenir una situación adversa, pero saber cómo manejarla de mejor manera si algo fuese a pasar.

Según la guía de NIST de Small Business Information Security: The Fundamentals Podemos observar los siguientes consejos:

- Prestar atención a la gente en tu entorno de trabajo - Realizar chequeos de background para una persona que recién va a entrar a la empresa puede ayudar a reducir el riesgo que esa persona signifique para la empresa.
- Tener cuidado de emails con archivos adjuntos y links – Revisar bien los emisores de correos, y tratar de no ingresar a links y descargar archivos si no es estrictamente necesario.
- Usar distintos dispositivos para el trabajo y para uso personal – Esto permitirá minimizar a ambos lados en caso de sufrir cualquier infección por malware o cualquier brecha de información que ocurra en un lado de nuestra vida, para que no pase al otro.
- No conectar dispositivos o hardware desconocidos a nuestra red o a computadores personales o de trabajo – Esto evitará el riesgo de contraer un virus o instalar malware en un lugar o dispositivo sensible.
- Tener cuidado al descargar software – Descargar aplicaciones solo de fuentes confiables y verificables.
- No divulgar información personal sensible – Esta información puede ser usada contra nosotros o contra nuestra empresa para comprometer nuestros datos.
- Usar contraseñas seguras – Se recomienda el uso de contraseñas fuertes para prevenir ataques de fuerza bruta contra ellas y, de ser posible, implementar una política de cambio de contraseñas periódicamente.

  (Paulsen & Toth, 2016)

Problemas Internos (Encontrados por Herramientas)

Debido a que la parte informática del Hotel ha sido manejada por un proveedor de hosting tercero, no existen varios cambios que se puedan implementar realísticamente, ya que bastantes aspectos del servicio los proveen ellos. Una alternativa podría ser que el Hotel empiece a alojar sus propios recursos tecnológicos, como la página web y el servidor de correo internamente, pero esto supondría un costo adicional, además de dificultades que vendrían con el manejo manual de estos recursos, como el mantenimiento, la instalación y los procesos de troubleshooting.

Personalmente, creo que es más conveniente que el Hotel busque otro proveedor de Hosting que pueda proveerle con mejores características de seguridad, como protocolos de comunicación más nuevos ya implementados en el caso de TLS, o un manejo más seguro y confiable de la página web y el servidor de correo.

Conclusiones

- De acuerdo con las investigaciones realizadas con el personal del Hotel, se ha determinado que la falta de conocimiento acerca de los problemas tecnológicos que puedan surgir es uno de los problemas más urgentes que enfrentan.
- Una solución asequible que se puede implementar en una Pyme en Ecuador puede ser la de protocolos de seguridad informática, ya que solo supondría un costo de capacitación y puede ser aplicado en varias situaciones generales.
- Varias de las vulnerabilidades encontradas durante la investigación para este proyecto pueden ser implementadas e identificadas fácilmente y con costos bajos, por lo que se podría también recomendar la contratación de una persona que pueda encargarse de estas tareas dentro del Hotel.

Recomendaciones

- Debido al constante avance de la tecnología, es recomendable realizar este tipo de análisis de manera periódica, para evitar inconvenientes causados por sistemas que súbitamente no están a la par de estándares de seguridad actuales.
- Se recomienda capacitar al personal y a uno mismo, aunque sea en un nivel básico, sobre temas de seguridad informática, para evitar la mayor cantidad de incidentes contra nuestra persona, nuestro grupo cercano o nuestro lugar de trabajo.
- Es recomendable crear un ambiente de conciencia alrededor de la seguridad informática. Es un tema bastante fácil de ignorar, incluso cuando se aplica, ya que no expresa resultados inmediatamente, pero es un tema importante para personas que usan dispositivos tecnológicos diariamente en su vida.

Bibliografía

Ajie, I. (2019). A Review of Trends and Issues of Cybersecurity in Academic Libraries. *Library Philosophy and Practice*, 2523.

Avila Pesantez, D. F. (2021). Ciberseguridad en los sistemas de gestión de aprendizaje (LMS). *Ecuadorian Science Journal*, 46-54.

Brown, M., Townsend, J., & Baird, L. (22 de Mayo de 2023). *TheHarvester*. Obtenido de TheHarvester: https://github.com/laramies/theHarvester

Combs, G. (s.f.). *Wireshark*. Obtenido de Wireshark: https://www.wireshark.org

Francisco, E. B. (21 de Abril de 2023). *SafetyCulture*. Obtenido de FMEA: Definition, Steps, Types & Tools: https://safetyculture.com/topics/fmea/

g0tmi1k. (20 de Enero de 2023). *Kali Linux*. Obtenido de What is Kali Linux?: https://www.kali.org/docs/introduction/what-is-kali-linux/#about-kali-linux

Gayoso Martínez, V., Hernández Encinas, L., & Arroyo Guardeño, D. (2020). *¿Qué sabemos de Ciberseguridad?* Madrid: CSIC.

Hodges, J. (Noviembre de 2012). *Internet Engineering Task Force*. Obtenido de HTTP Strict Transport Security (HSTS): https://www.rfc-editor.org/rfc/rfc6797.html

Hollenbeck, S. (Mayo de 2004). *Network Working Group*. Obtenido de Transport Layer Security Protocol Compression Methods: https://www.ietf.org/rfc/rfc3749.txt

IBM. (31 de Agosto de 2021). *IBM Documentation*. Obtenido de Renegotiation: https://www.ibm.com/docs/en/i/7.1?topic=properties-renegotiation

ISO. (Junio de 2005). *Information Technology - Security Techniques - Code of practice for information security management.* Obtenido de https://www.iso.org/standard/39612.html

ISO. (Julio de 2012). *Information Technology - Security Techniques - Guidelines for Cybersecurity.* Obtenido de https://www.iso.org/standard/44375.html

Jove, E., Calvo-Rolle, J.-L., Urda, D., Herrero, Á., Zurutuza, U., & Casola, V. (2021). Avances recientes en la aplicación de la ciencia de datos a la ciberseguridad industrial. *Revista DYNA*, 231-231.

Kiprin, B. (10 de Enero de 2022). *Crashtest Security*. Obtenido de What are TLS/SSL Cipher Suites and how to order them: https://crashtest-security.com/configure-ssl-cipher-order/

Klimaszewski, S. (8 de Febrero de 2023). *BED*. Obtenido de BED: https://gitlab.com/kalilinux/packages/bed

Linkedin Collaborative Articles. (27 de Abril de 2023). *Linkedin*. Obtenido de How do you test and measure the impact of TLS compression on your application?: https://www.linkedin.com/advice/0/how-do-you-test-measure-impact-tls-compression#:~:text=TLS%20compression%20is%20a%20feature,with%20large%20or%20repetitive%20data.

Lord, N. (6 de Mayo de 2023). *Digital Guardian*. Obtenido de What is NIST Compliance? (Checklist, Definition & More): https://www.digitalguardian.com/blog/what-nist-compliance

Lyon, G. (s.f.). *Insecure.org*. Obtenido de NMap.org: https://nmap.org

Melon, E., & Hernandez, W. (2020). Cybersecurity in the Dental Healthcare Sector: The Need of Knowledge for Small Practitioners. *Issues in Information Systems*, 118-124.

Moeller, B., & Langley, A. (Abril de 2015). *RFC Editor*. Obtenido de TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks: https://www.rfc-editor.org/rfc/rfc7507

Morales Paredes, P. I., & Medina Chicaiza, P. (2021). Ciberseguridad en Plataformas Educativas Institucionales de Educación Superior de la Provincia de Tungurahua - Ecuador. *Cuadernos de desarrollo aplicados a las TIC*, 49-75.

Offsec Services Limited. (2023). *Kali Linux*. Obtenido de https://www.kali.org

Olivares Rojas, J. C., Archundia, E. R., Gutiérrez Gnecchi, J. A., Molina Moreno, I., & Cerda Jacobo, J. (2020). Una revisión a la ciber seguridad en redes elécticas inteligentes. *Pistas Educativas*, 195-207.

Paulsen, C., & Toth, P. (Noviembre de 2016). *National Institute of Standards and Technology*. Obtenido de Small Business Information Security: The Fundamentals: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Quito, C. d. (s.f.). *Clasificación de las Pymes, Pequeña y Mediana Empresa*. Obtenido de Boletin Jurídico: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiA37XgueX2AhUqSTABHfMLAsYQFnoECAQQAQ&url=http%3A%2F%2Fwww.ccq.ec%2Fwp-

content%2Fuploads%2F2017%2F06%2FConsulta_Societaria_Junio_2017.pdf&usg=AOvVaw19FJ_2fz1uTBqs6EUnNOUS

Radware. (s.f.). *Radware Cyberpedia*. Obtenido de IP Address: https://www.radware.com/security/ddos-knowledge-center/ddospedia/ip-address/#:~:text=i.e.%20any%20connection-,255.255.,network%20it%20is%20connected%20to

Souppaya, M., & Scarfone, K. (Febrero de 2012). *National Institute of Standards and Technology.* Obtenido de Guidelines for Securing Wireless Local Area Networks (WLANs): https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

Tague, N. (2005). *The Quality Toolbox, Second Edition.* Milwaukee: ASQ Quality Press.

Testa, J. (17 de Abril de 2023). *SSLScan*. Obtenido de SSLScan: https://github.com/rbsec/sslscan

The OWASP Foundation Inc. (2023). *About the OWASP Foundation*. Obtenido de https://owasp.org/about/

The OWASP Foundation. (s.f.). *OWASP*. Obtenido de About the OWASP Foundation: https://owasp.org/about/

The SSL Store. (30 de Enero de 2020). *Comodo SSL Store*. Obtenido de SHA2 SSL/TLS Certificates: All You Need to Know: https://comodosslstore.com/resources/sha2-ssl-tls-certificates-all-you-need-to-know/