EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN GYG INGENIERÍA S.A.S. BASADO EN EL MODELO CYBER KILL CHAIN

CARLOS MAURICIO RAMIREZ ORDOÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA-CAQUETÁ
2024

EVALUACIÓN DE LOS MECANISMOS DE SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN GYG INGENIERÍA S.A.S. BASADO EN EL MODELO CYBER KILL CHAIN

CARLOS MAURICIO RAMIREZ ORDOÑEZ

Proyecto de Grado – Proyecto aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

JOEL CARROLL VARGAS
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA-CAQUETÁ
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Florencia Caquetá, 26 de Marzo de 2024.

DEDICATORIA

Le dedico este proyecto al acompañamiento de mis padres en esta nueva meta académica, le doy gracias por fundamentar el carácter que hay en mi para resistir a las dificultades que se han manifestado para la ejecución de este trabajo, Además también está dedicado al grande y majestuoso Dios que nos da el don de la vida para poder luchar por nuestros sueños.

AGRADECIMIENTOS

Al todo poderoso Jehová por darme el don de vida para lograr mis sueños, fortaleciendo mi espíritu en cada amanecer, renovando mis fuerzas, además, guiándome con su infinita sabiduría para alcanzar la meta propuesta en este proyecto.
A mi tutor de proyecto, por compartir su conocimiento para el desarrollo del proceso propuesto.
A mis padres, por sus sabios consejos y apoyo en este proceso de superación personal, ya que son participes de este gran logro en mi vida.

CONTENIDO

Pág.

TABLA DE TABLAS

TABLA DE IMÁGENES

GLOSARIO

Ciberresiliencia

Es la capacidad de una organización para minimizar el nivel de impacto ante un ataque informático.

CVE

Es la estandarización establecida para la lista de vulnerabilidades registradas.

Firewall

Es la primera barrera para defender a una red de los accesos no autorizados.

Ingeniería social

Son el conjunto de metodologías que utilizan los hackers para obtener datos confidenciales desde el ámbito social.

Kali Linux

Es un sistema operativo diseñado para la parte de seguridad informática.

Metasploit

Contiene una base de datos de las vulnerabilidades registradas y sus respectivos métodos para vulnerarlos.

Nmap

Es un programa para detectar puertos abiertos mediante el escaneo de una red.

Openvas

Software especializado en el escaneo de redes.

Payload

Es la carga que se implementa para aprovechar las vulnerabilidades.

Vector de ataque

Es una brecha de seguridad en la infraestructura tecnológica y organizacional.

Virtualbox

Es un software para montar máquinas virtuales.

Wireshark

Es un software que se encarga de analizar por medio de la interceptación de paquetes en una red.

RESUMEN

La presente propuesta fue elaborada con el fin de satisfacer las necesidades detectadas en temas de seguridad informática en la empresa GYG INGENIERIA S.A.S., pues la misma en el año 2020 fue víctima de diversos intentos de ataque distribuido de denegación de servicio DDOS y donde uno de ellos fue efectivo, el cual impidió estar en línea a la plataforma empresarial dedicada a la gestión del área PQR, cuya medida tomada por el profesional encargado fue recuperarse de la situación usando una copia de seguridad, la cual, su última actualización era de una semana anterior generando retroceso al personal de esta área.

De acuerdo a una entrevista realizada a expertos de Kaspersky afirman que la educación de los usuarios medios y profesionales del sector es el pilar para salvaguardar los países y los organismos gubernamentales, pero es un desafío engorroso para algunas regiones del planeta como América Latina, donde según los expertos del tema, aún no hay ciudadanos suficientemente capacitados como para desarrollar esta tarea, y el problema reside en que ningún estado pretende contratar a extranjeros para diseñar sus planes de seguridad informática, así que cada país debe encargarse de capacitar a los suyos para ejecutar estas infraestructuras.

Teniendo en cuenta el potencial de las nuevas tecnologías y el riesgo a las que están expuestas las mismas, se pretende desarrollar un diagnóstico de la seguridad informática en la organización mediante la implementación del modelo Cyber Kill Chain, el cual consta de siete etapas: reconocimiento, preparación, distribución, explotación, instalación, comando y control, acciones sobre los objetivos. Se implementará este modelo ya que permite actuar de la forma que ejecutaría el ataque el ciberdelincuente.

Palabras clave: Cyber Kill Chain-Nmap-Kali Linux- wireshark- OpenVas- firewall.

ABSTRACT

This proposal was prepared in order to satisfy the needs detected in computer security issues in the company GYG INGENIERIA S.A.S., since the same in 2020 was the victim of various DDOS denial of service attack attempts and where one of them was cash, which prevented the business platform dedicated to the management of the PQR area from being online, whose measure taken by the professional in charge was to recover from the situation using a backup, which, its last update was from a previous week generating pushback to staff in this area.

According to an interview with Kaspersky experts, they affirm that the education of average users and professionals in the sector is the pillar to safeguard countries and government agencies, but it is a cumbersome challenge for some regions of the planet such as Latin America. , where according to experts on the subject, there are still not enough trained citizens to carry out this task, and the problem is that no state intends to hire foreigners to design its computer security plans, so each country must be responsible for training the theirs to run these infrastructures.

Taking into account the potential of new technologies and the risk to which they are exposed, it is intended to develop a diagnosis of computer security in the organization through the implementation of the Cyber Kill Chain model, which consists of seven stages: recognition, preparation, distribution, exploitation, installation, command and control, actions on the targets. This model will be implemented since it allows acting in the way that the cybercriminal would execute the attack.

Palabras clave: Cyber Kill Chain-Nmap-Kali Linux- wireshark- OpenVas- firewall.

INTRODUCCIÓN

En diversos protocolos o marcos de buenas prácticas, la estructura es solo eso: una secuencia a llevar a cabo. La aplicación satisfactoria que produce los resultados comerciales requeridos para la organización se obtiene de una estructura basada en la conformación de análisis basados en datos, adopción interna generalizada y la ejecución correcta de cultura y personas. Las transformaciones debido a su naturaleza de cambio no es un tema fácil de aplicar y requiere tiempo.

InterLan[1] público que, en Colombia, lastimosamente el panorama no es nada alentador. Sola el 50% de las empresas colombianas destinan entre 1 a 5% del presupuesto de TI para invertir en temas de ciberseguridad. Actualmente la empresa GYG INGENIERÍA S.A.S. no ha realizado pruebas de intrusión a su infraestructura tecnológica, además, no cuenta con planes de acción ya que no cuenta con personal dedicado específicamente a esa área, lo anterior es preocupante ya que su infraestructura critica es susceptible a un ataque DOS.

Teniendo en cuenta lo anterior y analizando el impacto negativo de esta clase de ataques, surge la necesidad de implementar unas pruebas de pentesting para defender la infraestructura critica de la empresa, además, se realizará una capacitación al personal para evitar que sean víctimas de ingeniería social.

[1] INTERLAN. Las empresas colombianas invierten menos del 5% en ciberseguridad. [Sitio web]. [Consultado el 29 de octubre de 2022]. Disponible en: https://www.interlan.com.co/2019/08/28/las-empresas-colombianas-invierten-menos-del-5-en-ciberseguridad/

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Pstyga, N.[2] informa que años atrás se tenía la mentalidad que la seguridad informática era un lujo que solo organizaciones internacionales y grandes bancos podían darse, y si bien los expertos en el área afirmaban que no era así y soportaban con hechos la necesidad de diseñar políticas de seguridad informática eficientes, lastimosamente los líderes de estas organizaciones no necesariamente daban atención al tema.

Bodnar, D. [3]expresa que, en toda cadena de seguridad los humanos casi siempre representan el eslabón más débil, ya que suelen ser susceptibles a gran variedad de tácticas de manipulación. Las técnicas de ingeniería social se valen de esta vulnerabilidad humana para engañar a las víctimas y lograr que compartan información privada. Además, según Kaspersky[4] informa que los hackers pueden tratar de aprovecharse de la falta de conocimiento de un usuario; como consecuencia de la velocidad a la que avanza la tecnología, numerosos trabajadores y consumidores no son conscientes del valor real de los datos

[2] Pstyga, N. Ciberseguridad: todos podemos ser víctimas. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en: https://iqlatino.org/ciberseguridad-todos-podemos-ser-victimas/?gclid=CjwKCAjw7eSZBhB8EiwA60kCW0OT9qvwbuhUdvf6qV3COhPJLu-h87H6SHNIAvo2fD4Msk1prXw_4xoCzhkQAvD_BwE

[3] Bodnar, D. Ingeniería social. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en: https://www.avast.com/es-es/c-social-engineering#:~:text=En%20cualquier%20cadena%20de%20seguridad,conseguir%20que%20divulguen%20informaci%C3%B3n%20privada.

[4] Kaspersky. Ingeniería social: definición. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

personales, y no saben con exactitud cuál es la mejor forma de proteger esta información.

La organización GYG INGENIERÍA S.A.S. no es ajeno a esta realidad, ya que, al realizar procesos de soporte de manera remota, se ha encontrado software instalado de ámbito no empresarial y de origen desconocido, además la empresa ya ha sufrido intentos de vulneración de las contraseñas de los correos de diferentes áreas por medio de ataque de fuerza bruta, e incluso ataques efectivos de denegación de servicios DOS, lo cual paralizo las actividades de PQR de la empresa evidenciándose una afectación a la infraestructura crítica y al tratar de recuperarse de la situación se optó por implementar una copia de seguridad, pero se encontraba desactualizada, generando que el personal tuviese que cargar procesos de 7 días anteriores hasta la fecha actual del incidente, donde en un primer análisis arrojo la vulnerabilidad CVE-2011-1002.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo se puede evaluar los mecanismos de seguridad de la infraestructura tecnológica de la organización GYG INGENIERÍA S.A.S. de la ciudad de Florencia Caquetá?

2. JUSTIFICACIÓN

De acuerdo con una publicación de Global Technology[5] informa que los ciberataques han mantenido un crecimiento exponencial en los últimos años, guardando relación con el incremento de la incorporación de la tecnología en las organizaciones. Esto es un caso que se ve reflejado a nivel mundial, en mayor o menor medida, pero en gran parte de los casos se infravalora el daño causado.

Los activos más valiosos para los hackers son los datos personales que están bajo la supervisión de las compañías, independientemente de su actividad y tamaño. Por eso es uno de los elementos que más peligro corren en un ciberataque. Según Global Technology[7] expresa que "dadas las graves consecuencias que implican los ciberataques es vital para cualquier organización prepararse para ellos. Y, mejor aún, implementar sistemas de protección que eviten cualquier posible ataque a cualquier nivel".

Portafolio[6] menciona que "el costo promedio de una filtración de datos en servicios financieros a nivel mundial ascendió a US$5,97 millones y se constituyó en la segunda industria luego de la de servicios de salud, con US$10,1 millones".

De acuerdo con la publicación de Portafolio[8] menciona que en América Latina el tiempo promedio para detectar y reprimir una filtración de datos se minimizo a 25 días aproximadamente (331,5 días) pero sigue por encima del promedio global de

---

[5] Global Technology. Consecuencias de un ciberataque. [Sitio web]. [Consultado el 31 de septiembre de 2022]. Disponible en: https://globalt4e.com/consecuencias-de-un-ciberataque/

[6] Portafolio. El 73% de las empresas en el mundo han sufrido de ciberataques. [Sitio web] [Consultado el 31 de septiembre de 2022]. Disponible en: https://www.portafolio.co/economia/finanzas/ciberseguridad-el-73-de-las-empresas-en-el-mundo-ha-sufrido-ciberataques-570387

277. En Colombia, más del 40% de las firmas informa que el responsable de la ciberseguridad es el área de Tecnología de Información.

La empresa GYG INGENIERIA S.A.S. a pesar de ser víctima de un ataque de DOS en el año 2020 y generar retroceso en el área de PQR, hasta la fecha no cuenta con un diagnóstico para mejorar sus defensas en el campo de la seguridad informática, además, ha de tenerse en cuenta la siguiente premisa (un ciberdelincuente prepara mejor sus procesos para atacar con mayor fuerza. Teniendo en cuenta lo anterior y analizando el impacto negativo de esta clase de ataques, surge la necesidad de implementar unas pruebas de pentesting para defender la infraestructura critica de la empresa, además, se realizará una capacitación al personal para evitar que sean víctimas de ingeniería social. Trayendo beneficios de gran importancia para mejorar la lealtad e imagen de la empresa, brinda las estrategias necesarias para actuar en caso de un ciberataque, entrenar al personal y obtener las vulnerabilidades presentes de la infraestructura tecnológica, además, evitara perdidas de información y recursos económicos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Evaluar los mecanismos de seguridad de la infraestructura tecnológica de la organización GYG INGENIERÍA S.A.S., mediante el modelo Cyber Kill Chain con la finalidad de establecer estrategias que permitan salvaguardar la información.

3.2. OBJETIVOS ESPECÍFICOS

- Establecer el alcance de la evaluación de seguridad en la infraestructura tecnológica de la organización GYG INGENIERÍA S.A.S. mediante entrevistas que permitan determinar los activos críticos que requieran ser examinados con el fin de detectar vectores de ataques asociados a éstos.

- Aplicar la metodología Cyber Kill Chain a partir del alcance determinado para la evaluación de seguridad en la infraestructura tecnológica con el fin de establecer las herramientas necesarias a emplear durante cada etapa.

- Analizar los resultados obtenidos de la metodología implementada, generando una lista de vulnerabilidades dependiendo de su nivel de impacto, para finalmente entregar el informe con los hallazgos encontrados.

- Proponer un plan de acción empleando algunos controles de ISO/IEC 27002:2013, donde se establecerán estrategias para prevenir ataques informáticos, y procesos a seguir con el fin de mitigar el nivel de impacto frente a los incidentes detectados.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

4.1.1 Importancia de los Test de Penetración. Según Dragonjar[7] lo define como un proceso sistemático y metodológico en el que se simula un ataque real a sistema o red, con el objetivo de detectar y arreglar los vectores de seguridad.

De acuerdo con Prenafeta, J.[8] detalla que existen herramientas para analizar la gravedad de las amenazas a las que una organización se enfrenta en su cotidianidad. Esto les facilita encontrar los vectores de seguridad existentes en la organización y así estar preparados por medio de protocolos estandarizados.

El pentesting es una manera de hacking, solo que esta práctica es totalmente legal, ya que tiene el consentimiento de los propietarios de los equipos en los que se van a ejecutar las pruebas, además se ataca con la intención de causar un daño real.

4.1.2 Tipos de Pentesting. Según Prenafeta, J. [10] indica que el tipo de datos a obtener sobre el sistema para su testeo de pende del tipo de pentesting a ejecutar, los cuales son:

4.1.3 Pentesting de caja blanca: en este tipo de prueba se sabe todo a cerca de la aplicación, sistemas o la arquitectura. Es el Pentest más completo. Esta

---

[7] Dragonjar. Pentest. [Sitio Web]. [Consultado el 02 de octubre de 2022] Disponible en: https://www.dragonjar.org/como-realizar-un-pentest.xhtml

Disponible en: https://ciberseguridad.com/guias/cyber-kill-chain/

[8] Prenafeta, J. Pentesting. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/#:~:text=El%20%E2%80%9Cpentesting%E2%80%9D%20o%20%E2%80%9Ctest,pueden%20afectar%20a%20su%20sistema.

metodología parte de un análisis integral, que analiza toda la infraestructura de red. Al tener un alto volumen de información, suele ejecutarse por miembros del propio equipo de TI de la Organización.

4.1.4 Pentesting de caja negra**:** En esta clase no se cuenta con ningún tipo de dato sobre el objetivo y es de recalcar que su costo a contratar es alto. Comúnmente se conoce como prueba a ciegas y el más similar a simular las particularidades de un ataque externo. Su secuencia de ataque tiene la mayor paridad a la de los cibercriminales.

4.1.5 Pentesting de caja gris**:** este se compone de los dos anteriores, en otras palabras, se tiene ya cierta información a disposición, pero no la suficiente, por lo que se requiere invertir tiempo y recursos para detectar amenazas y las vulnerabilidades en base a la cantidad de información que se tenga. Es el pentest más recomendado.

4.2 MARCO CONCEPTUAL

Las pruebas de penetración son relevantes en una organización ya que permiten conocer el estado actual de la ciberresiliencia, de acuerdo con Itera[9], dicho proceso permite realizar un diagnóstico integral de las aplicaciones e infraestructura que componen a la empresa para su optimo funcionamiento, cuyos datos obtenidos se utilizaran para incorporar estrategias para mitigar el nivel de impacto de un ataque informático a través de manuales y planes de acción. La prueba de penetración implementa diferentes herramientas para evaluar el estado de la seguridad digital de determina organización. Se implementan pruebas de hackeo para detectar el mayor número posible de brechas de seguridad para posteriormente mitigarlas. A

[9] Itera. ¿qué es una prueba de penetración? [sitio web]. (). [Consultado el 09 de diciembre de 2022]. Disponible en https://iteraprocess.com/2021/04/05/para-que-sirven-las-pruebas-de-penetracion/#:~:text=Las%20pruebas%20de%20penetraci%C3%B3n%20adem%C3%A1s,que%20genera%20en%20la%20organizaci%C3%B3n.

continuación, se procederá a mencionar herramientas útiles para este campo de acción:

4.2.1 Kali Linux**:** es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa.

4.2.2 Nmap**:** es una herramienta de sondeo de seguridad y exploración de redes.

Wireshark: es una herramienta para monitorear el tráfico de red, permitiendo evaluar paquetes caídos, actividad maliciosa en su red y problemas de latencia.

4.2.3 Openvas**:** De acuerdo con Vera, R.[10] afirma que "es un completo scanner de vulnerabilidades que puede detectar problemas de diferentes calibres, tanto de bajo riesgo para usuarios, como vulnerabilidades más graves en equipos en dispositivos en red".

4.2.4 Firewall**:** Traducido al español **(**cortafuegos) es un dispositivo cuya finalidad es brindar seguridad en la red permitiendo supervisar el tráfico de red entrante y saliente, lo anterior, a privilegios de decidir si permite o no tráfico específico en función de un grupo de reglas de seguridad establecidas.

4.2.5 Metasploit**:** Es una de las herramientas más completas enfocada para auditores de seguridad, contiene una gran base de datos con más de 3000 esploit.

[10] Vera, R. OpenVas. [Sitio web]. [Consultado el 01 de octubre de 2022] Disponible en: https://openwebinars.net/blog/que-es-openvas/

4.3 MARCO CONTEXTUAL

4.3.1 Razón Social De La Empresa. La actividad a la que se dedica la empresa Gyg Ingenieria S A S es Construcción de proyectos de servicio público. "Comprometidos y Mejorando la Calidad del servicio Eléctrico".

4.3.2 MISIÓN. GYG INGENIERÍA S.A.S. se dedica al desarrollo de proyectos eléctricos para el sector residencial, comercial, rural e industrial, aplicando prácticas y elementos que garanticen el cumplimiento de la normatividad vigente para la seguridad de nuestros clientes; además contamos con profesionales integrales capaces de llevar a cabo los proyectos más exigentes y ambiciosos del mercado.

4.3.3 VISIÓN. Para el año 2027 GYG INGENIERÍA S.A.S. será reconocida a nivel mundial como líder en el desarrollo de proyectos eléctricos, siendo una empresa multiservicios capaz de dar soluciones integrales a las diversas necesidades del sector eléctrico y la ingeniería.

4.4 ANTECEDENTES O ESTADO ACTUAL

InterLan[11] público que, en Colombia, lastimosamente el panorama no es nada alentador. Sola el 50% de las empresas colombianas destinan entre 1 a 5% del presupuesto de TI para invertir en temas de ciberseguridad.

De acuerdo con lo publicado por Elempleo[12] informa que el cambio digital en las organizaciones es uno de los factores que ha ocasionado un creciente interés, ya que se ha transformado en una necesidad para los procesos estratégicos, logrando mantener sus modelos de negocio y generar una mayor competitividad.

[11] InterLan. Las empresas colombianas invierten menos del 5% en ciberseguridad. [Sitio web]. [Consultado el 29 de octubre de 2022]. Disponible en: https://www.interlan.com.co/2019/08/28/las-empresas-colombianas-invierten-menos-del-5-en-ciberseguridad/

[12] Elempleo. ¿Cómo combatir los ciberataques en empresas colombianas? [Sitio Web]. 2022. [Consultado el 29 de Octubre de 2022]. Disponible en https://www.elempleo.com/co/noticias/mundo-empresarial/como-combatir-los-ciberataques-en-companias-colombianas-6925

Imparto TIC[13] afirma que recientemente en Colombia, se halló que más del 53% de las organizaciones fueron víctimas de ataques informáticos en el 2021.

Teniendo en cuenta lo anterior, Vanegas, R. & Alfonso, Y.[14] en su trabajo Pentesting, ¿Porque es importante para las empresas?, resaltan la importancia de las pruebas de pentesting en las organizaciones que están expuestas a riesgos que generan un menor cumplimiento de los tres pilares de la seguridad informática. Proteger los datos debe ser de vital importancia para las organizaciones, pues deben saber el impacto económico y daño de imagen generaría una brecha de seguridad que posibilite la perdida de ellos.

Vanegas, R. & Alfonso, Y. [14] recomiendan llevar a cabo unas serie de pruebas que cubrirán todo el entorno de TI, a este procedimiento se le conoce bajo el nombre de pruebas de penetración o pentesting, cuyo objetivo es dejar en claro a las organizaciones las brechas de seguridad existente y las consecuencias de las mismas, además, al implementar el pentesting en las organizaciones se podrá establecer el plan de acción para mitigar las vulnerabilidades, analizando el nivel de priorización necesario y establecer los controles ideales para cada situación.

Para ejecutar las pruebas de pentesting se requiere implementar alguna metodología diseñada para esa tarea, por ende, Saltos, B. & Campoverde, C.[15] en su trabajo de titulación sugieren el marco metodológico Cyber Kill Chain, el cual se define como una estrategia de gestión de vulnerabilidades para la detección y prevención de ciberataques, basándose en una secuencia de pasos de como lo ejecutarían los crackers para llevar a cabo un ataque exitoso.

---

[13] Impacto TIC. Mas de la mitad de las empresas colombianas sufrió ataques en este ultimo año, [En linea]. 2022. Consultado el 29 de Octubre de 2022]. Disponible en: https://impactotic.co/mas-de-la-mitad-de-las-empresas-colombianas-sufrio-ataques-el-ultimo-ano/

[14] Vanegas, R. & Alfonso, Y. Pentesting ¿por kue es tan importante para las empresas?. [en línea]. 2021. [Consultado el 10 de diciembre de 2022]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1

[15] Saltos, B. & Campoverde, C. Diseño e implementación de un framework para la evaluación periódica de la seguridad usando pruebas de penetración en la red interna de la Universidad de Cuenca. [en línea]. 2021. [consultado el 10 de diciembre de 2022]. Disponible en https://dspace.ucuenca.edu.ec/bitstream/123456789/37143/1/Trabajo%20de%20Titulaci%C3%B3n.pdf

4.5 MARCO LEGAL

RESOLUCIÓN 500 DE 2021, la cual permitirá tener en cuenta los estándares y lineamientos para la seguridad digital.

ARTÍCULO 10. OBJETO. Contribuye en el proyecto, ya que informa los lineamientos principales para la incorporación del Modelo de Seguridad y Privacidad de la Información (MSPI), además, comparte información respecto al proceso para la gestión de los incidentes de seguridad digital y el manual de gestión de riesgos de seguridad de la Información, y, de acuerdo con lineamientos estandarizados.

ARTÍCULO 50. LA ESTRATEGIA DE SEGURIDAD DIGITAL. Se integra con este proceso ya que permite construir estrategias de seguridad digital, generando guías, políticas, formatos, manuales y lineamientos para la administración de la seguridad de la información.

ARTÍCULO 60. LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y LA GESTIÓN DE RIESGOS DE LA ENTIDAD. Teniendo en cuenta la problemática presentada en la empresa y las vulnerabilidades que hasta el momento se desconocen, Se debe establecer e incorporar sistemas de control para minimizar los riesgos que puedan perjudicar la seguridad física y digital de acuerdo con los datos obtenidos del estudio y valoración de riesgos, se aspira cumplir con los siguientes aspectos:

- Establecer sistemas de control teniendo en cuenta factores propios de GYG INGENIERIA S.A.S.
- Ejecutar una gestión que contribuya la seguridad de la información en la organización.
- Comunicar los resultados del estudio de riesgos y gestión de incidentes al comité encargado.
- Llevar a cabo capacitaciones al personal de la organización en temas enlazados a la seguridad digital y amenazas cibernéticas.
- Ejecutar el monitoreo del nivel cumplimiento de los procesos y políticas establecidos en materia de seguridad de la información.

Ley 1581 DE 2012

Artículo 4. Principios para el Tratamiento de datos personales.

Artículo 5. Datos sensibles. Para los propósitos del presente proyecto, debido a la información que estará expuesta ante la investigación, se debe dar fiel cumplimiento a los acuerdos de confidencialidad.

LEY 1273 DE 2009

ARTÍCULO 269

El articulo 269 este compuesto por tres literales A-B-C, en este proyecto se abordaron los siguientes:

A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

5. DISEÑO METODOLÓGICO

Se llevará a cabo una investigación aplicada, de acuerdo con la publicación de significados[16] En este caso, el objetivo es encontrar estrategias que puedan ser empleadas en el abordaje de un problema específico. La investigación aplicada se nutre de la teoría para generar conocimiento práctico, y su uso es muy común en ramas del conocimiento como la ingeniería o la medicina.

Teniendo en cuenta lo anterior, para el presente proyecto se hará uso de la investigación aplicada tecnológica, ya que es fundamental para generar conocimientos que se puedan llevar a la práctica en el sector productivo, con el propósito de generar un impacto positivo en la vida cotidiana.

Este tipo de diseño es útil en el proyecto que se va a llevar a cabo, pues se adapta al objetivo a lograr, además se obtiene información necesaria para tener bases para realizar la metodología CYBER BILL CHAIN para el desarrollo de este trabajo.

6. DESARROLLO DE LOS OBJETIVOS

6.1. ESTABLECER EL ALCANCE DE LA EVALUACIÓN DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA ORGANIZACIÓN GYG INGENIERÍA S.A.S. MEDIANTE ENTREVISTAS QUE PERMITAN DETERMINAR LOS ACTIVOS CRÍTICOS QUE REQUIERAN SER EXAMINADOS CON EL FIN DE DETECTAR VECTORES DE ATAQUES ASOCIADOS A ÉSTOS.

Para determinar el alcance para la evaluación de seguridad en la infraestructura tecnológica de la organización GYG INGENIERÍA S.A.S., se hizo necesario llevar a cabo una entrevista para obtener datos relevantes que permitieran determinar el alcance del análisis a realizar, además, se logró establecer las herramientas

[16] Significados. Tipos de investigación. [Sitio web]. [Consultado el 14 de noviembre de 2022]. Disponible en: https://www.significados.com/tipos-de-investigacion/#:~:text=Investigaci%C3%B3n%20aplicada,la%20ingenier%C3%ADa%20o%20la%20medicina.

adecuadas para esta tarea, tomando como base los datos recopilados de la entrevistada expuestos en el punto 6.1.1.

6.1.1 Datos de entrevista

Entrevistado: director de proyectos, ya que es el encargado de supervisar la puesta en marcha de los proyectos y procesos de la empresa, además, se encarga se monitorear el nivel de cumplimiento es cuanto a los tiempos establecidos y por supuesto la calidad de lo entregado.
Motivo: Es el profesional encargo de supervisar los proyectos de la empresa, por lo tanto, vigila también los impactos negativos que puedan ocurrir en su ejecución.
Estructura Encuesta:

1. ¿conoce las vulnerabilidades existentes en la infraestructura tecnológica de la empresa?

   Respuesta: Al ser un ingeniero eléctrico desconozco los temas relacionados con vulnerabilidades en los sistemas que se manejan en la empresa, solo se hacen visibles ya cuando la infraestructura tecnológica es afectada y como resultado reacciona evidentemente, además, la empresa no cuenta con personal de sistemas directamente vinculado a la empresa, por lo que siempre se requiere contratar ayuda externa para tratar estos inconvenientes y esperar lo tiempos de asignación de ellos.

2. Después de presentarse el ataque exitoso de DOS, ¿Han realizado pruebas de intrusión para mejorar la ciberresiliencia?

   Respuesta: Inicialmente al desconocer del tema se pensó que se había caído el internet como se suele decir o sencillamente la plataforma por temas de mantenimiento estaba fallando. El problema se profundizo cuando ya el ataque era inminente y nuestro proveedor nos informó que éramos víctimas de un ataque DOS, bueno, después de esta breve introducción en cuanto a la pregunta como tal, después de restablecer la plataforma y perder una semana de registros, fue el punto final para ese incidente, además, de lo que

me comento de que la vulnerabilidad sigue existiendo y no se han aplicado procesos para mitigarlo es preocupante, ya que ese tipo de ataques genera retrocesos en el cargue de la información representando que no cumplamos con los niveles de calidad exigidos por el cliente.

3. ¿El personal ha sido capacitado para evitar ser víctimas de ataques de ingeniería social?

Respuesta: Como ya se había comentado con anterioridad, la empresa no cuenta con personal de sistemas contratado directamente y que sean aptos para dar este tipo de charla, inclusive se requirió de una breve explicación sobre ese término, ya que hasta el momento me era desconocido, e incluso en días anteriores habían llegado correos de esa índole, los cuales me generaban incertidumbre al no saber cómo proceder.

4. ¿Cuentan con un inventario actualizado de la infraestructura tecnológica?

Respuesta: No se cuenta con inventario actualizado de la infraestructura tecnológica, incluso, para saber las características técnicas de algún dispositivo de las oficinas toca hacer la consulta con el auxiliar a cargo, pues no se cuenta con una base de datos que tenga registrada dicha información, en algunas ocasiones al movilizar las impresoras, no se sabe ni cual tiene determinado municipio, como consecuencia, siempre se debe preguntar al auxiliar por el número de activo y sus referencias para el tema de soporte técnico, algo que no ejecuta la empresa son los mantenimientos preventivos, ya que todos son de carácter correctivo.

Como se puede observar la empresa tiene varios factores a mejorar, y que desde la profesión de ingeniería de sistemas y aún más en la especialización que se está llevando a cabo, se puede aportar de manera significativa ante los inconvenientes

mencionados por parte del ingeniero entrevistado. Por tal motivo se establecen los siguientes alcances que se van a ejecutar en el proyecto:

- Ejecutar un ataque para vulnerar la seguridad de la contraseña de la red.
- Detectar los activos tecnológicos conectados a la red.
- Buscar puertos abiertos que pudiesen ser aprovechados por los ciberdelincuentes.
- Realizar un análisis de vulnerabilidades que se puedan aprovechar para la intrusión.
- Llevar a cabo un ataque de hombre en el medio, para validar la seguridad de los datos en transferencia.
- Elaborar un plan de acción para mitigar la vulneración de la seguridad informática de la empresa.

Consecuencias

Las vulnerabilidades desconocidas hasta el momento pueden afectar tanto a nivel económico como a nivel operativo a GYG INGENIERÍA S.A.S., además, sin contar el daño a la buena imagen consecuencia de un ataque informático efectivo. Es importante saber que al ser comprometido con un ataque de denegación de servicios y comprobar su efectividad, los ciberdelincuentes podrían nuevamente ejecutar nuevos procedimientos, en el peor de los casos exigir una remuneración económica a cambio del restablecimiento del sistema.

6.1.3 HERRAMIENTAS

Estas herramientas pertenecen al a fase de preparación, donde se seleccionan las aplicaciones necesarias para llevar a cabo una prueba de pentesting exitosa.

- NMAP, permitirá conocer los dispositivos conectados a la red y los puertos abiertos, además se podrá investigar las vulnerabilidades expuestas en cada puerto encontrado.

- METASPLOIT: Una vez obtenidas las brechas de seguridad, se procede a buscar los exploit disponibles para aprovechar la vulnerabilidad.
- WIRESHARK, Permite la captura de paquetes en la red, esto es importante en el proyecto ya que se pretende también realizar un ataque del hombre en el medio para conocer la ciberresiliencia de los datos en tráfico,
- KALI LINUX, es el sistema operativo que proveerá las herramientas necesarias para hacer la prueba de penetración.
- Herramientas ofimáticas, para realizar el informe de los hallazgos encontrados.

6.1.4. IDENTIFICACIÓN DE ACTIVOS

Se recolecta información respecto a los activos a evaluar con el objetivo de obtener una mayor claridad para el siguiente objetivo.

Tabla 1.Listado de activos

ÁREA	TIPO ACTIVO	MODELO	SISTEMA OPERATIVO	IP
Recepción	Computador todo en uno	HP 24-cb1005la	Windows 10 PRO	192.168.1.2
PQR	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.16
PQR	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.20
PQR	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.29
PQR	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.38
PQR	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.46
PQR	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.54
Talento humano	Computador todo en uno	HP 24-cb1005la	Windows 10 PRO	192.168.1.62
Talento humano	Computador todo en uno	HP 24-cb1005la	Windows 10 PRO	192.168.1.71
Almacén & dirección PQR	Computador todo en uno	HP Pavilion 27-ca0000la	Windows 10 PRO	192.168.1.85
Contabilidad	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.115

Contabilidad	Computador todo en uno	HP 24-df0006la	Windows 10 PRO	192.168.1.125
Proyectos	Computador todo en uno	HP Pavilion 27-ca0000la	Windows 10 PRO	192.168.1.156
Proyectos	Computador todo en uno	HP Pavilion 27-ca0000la	Windows 10 PRO	192.168.1.208
Proyectos	Fotocopiadora	RICOH C2000	No aplica	192.168.1.155
Gerencia	Computador todo en uno	HP Pro 240 G9	Windows 10 PRO	192.168.1.213

Fuente. Autoría propia.

6.2. APLICAR LA METODOLOGÍA CYBER KILL CHAIN A PARTIR DEL ALCANCE DETERMINADO PARA LA EVALUACIÓN DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA CON EL FIN DE ESTABLECER LAS HERRAMIENTAS NECESARIAS A EMPLEAR DURANTE CADA ETAPA.

Los ataques cibernéticos han evolucionado drásticamente con el transcurrir del tiempo. La tecnología en la nube, la ingeniería social y las amenazas internas han transformado la manera en que se percibe el perímetro de seguridad, pero lastimosamente a pesar de la relevancia del tema, en la mente de muchas personas tienen el concepto de que la seguridad informática es irrelevante para sus empresas.

Para lograr el cumplimiento de este objetivo, se deberá abordar a gran profundidad la metodología Cyber Kill Chain o cadena de asesinato cibernético, es de aclarar que se llevara a cabo también bajo el método de caja gris. En la empresa GYG INGENIERIA S.A.S. se ejecutará esta metodología que está diseñada para realizar una prueba de pentesting con altos estándares de calidad, procediendo de la forma como procedería a ejecutar el proceso un ciberdelincuente, este modelo está compuesto por 7 niveles, teniendo en cuenta los alcances del proyecto, se ejecutará hasta el 4 nivel, ya que un proyecto de prueba utilizando la metodología Cyber Kill Chain, se recomienda ejecutar hasta el cuarto paso, la etapa de "Instalación", por varias razones:

Identificación de vulnerabilidades tempranas: Al detener el proceso en la etapa de instalación, se puede identificar y corregir las vulnerabilidades del sistema que

permitieron que el artefacto malicioso se instalara en primer lugar. Esto ayuda a fortalecer la seguridad del sistema y a prevenir futuros ataques.

Control del acceso no autorizado: Al detener el proceso en la etapa de instalación, se puede evitar que el atacante establezca un control completo sobre el sistema comprometido. Esto limita el daño potencial y reduce la exposición de datos sensibles.

Minimización del impacto: Al interrumpir el proceso antes de que el atacante pueda ejecutar plenamente sus objetivos, se minimiza el impacto del ataque en la organización. Esto puede ayudar a evitar la pérdida de datos críticos, interrupciones en los servicios, o daños a la reputación de la empresa.

Optimización de recursos: Enfocarse en las primeras etapas de la Cyber Kill Chain permite a las organizaciones optimizar sus recursos y esfuerzos en la detección y prevención temprana de ataques. Esto puede ser más eficiente y efectivo que intentar abordar todas las etapas del ciclo de ataque de una vez.

A continuación, se procede a abordar las cuatro etapas de la metodología Ciber Kill Chain:

1. Reconocimiento

En esta etapa, se establecerá los alcances de la prueba de penetración, ya que se disponen de los datos de contacto del objetivo, como la dirección de correo electrónico, la información de las redes sociales, y otros datos de la empresa o los empleados. Pues esto es una ventaja de trabajar en simultáneo con la metodología de caja gris, la cual facilita ciertos datos de la empresa.

Se permitió escanear todos los Dispositivos conectados a la Red haciendo uso de NMAP, además se implementará METAEXPLOIT en caso de encontrar vulnerabilidades.

El área de PQR entregó el listado de correos electrónicos de las sedes para el ataque simulado de ingeniería social.

Imagen 1. Listado de correos electrónicos

PQR SOLANO <solanopqrgyg@gmail.com>,
PQR VALPARAISO <valparaisopqrgyg@gmail.com>,
PQR SAN VICENTE <svpqr2021@gmail.com>,
PQR PUERTO RICO <puertoricopqrgyg@gmail.com>,
PQR LA MONTAÑITA
<lamontanitamilanpqrgyg.2022@gmail.com>,
PQR ALBANIA <albaniapqrgyg@gmail.com>,
PQR LA MACARENA <macarenapqrgyg@gmail.com>,
PQR PAUJIL <elpaujilpqrgyg@gmail.com>,
PQR SOLITA <solitapqrgyg2022@gmail.com>,
PQR DONCELLO <doncellopqrgyg@gmail.com>,
PQR SAN ANTONIO <sanantoniopqr@gmail.com>,
PQR SAN JOSÉ <sanjosegyg2022@gmail.com>,
PQR BELEN <oficinabelen2019@gmail.com>,
PQR CURILLO <pqrcurillo@gmail.com>

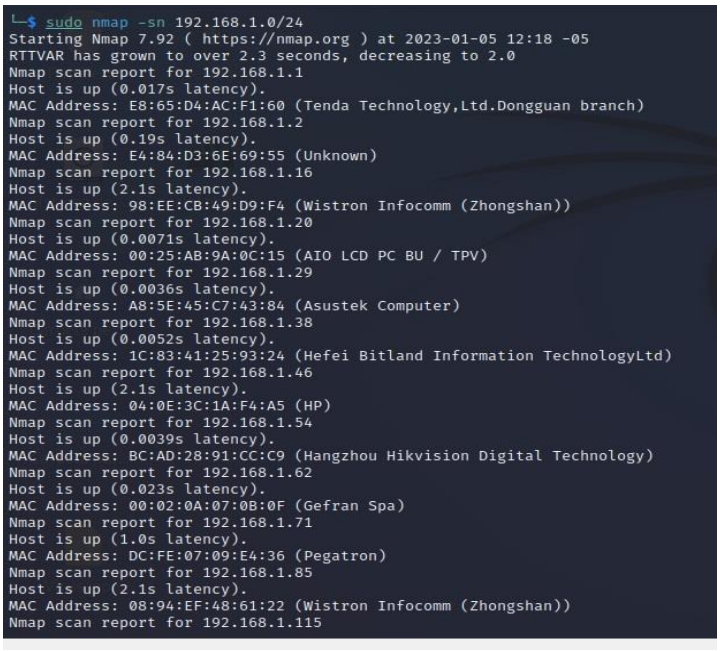
Nota. El área de PQR entrego el listado de los correos con el objetivo de llevar a cabo el ataque simulado de ingeniera social.

2. Preparación del ataque

En este apartado, se procederá a utilizar NMAP, METAEXPLOIT y suplantación de identidad para proceder a ejecutar el ataque cibernético, entre los cuales se encuentra el Phishing y escaneo de red con su respectivo método de explotación de vulnerabilidades.

Conociendo la puerta de enlace de la red, la cual fue entregada por parte del personal, se ejecuta el comando que se puede visualizar la imagen 2, el cual permite escanear la red de la empresa, dando como resultado la IP de todos los equipos conectados.

Imagen 2. Comando Sudo nmap -sn ejecutado en la red de la empresa GYG



Nota. Lista todos los dispositivos conectados a la red, permitiendo obtener las respectivas IP.

En la imagen 3 se muestra la continuidad del listado generado del comando ejecutado en la imagen 2.

Imagen 3. Listado IP de dispositivos conectados a la red de la empresa

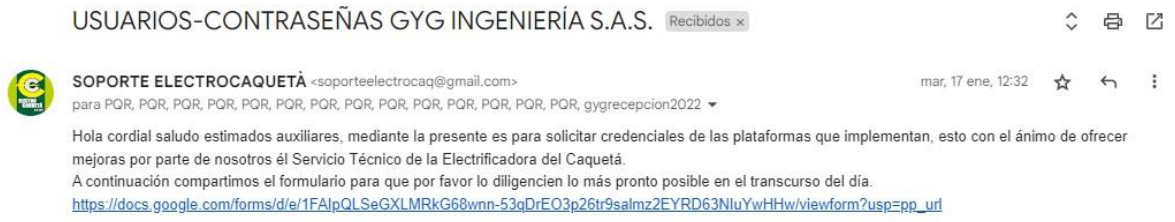
Nota. Segunda parte del listado de las IP escaneadas.

3. Entrega

La empresa GYG INGENIERA S.A.S entre sus contratos con la Electrificadora del Caquetá, tiene el de PQR (PETICIÍON, QUEJAS Y RECLAMOS), debido a lo anterior, cuenta con 12 oficinas en el departamento del Caquetá, cada una en un municipio diferente, aclarando lo anterior, se procede a llevar a cabo el ciberataque a la infraestructura tecnológica de GYG INGENIERA S.A.S, cabe declarar que se llega hasta cierto punto para no afectar la operatividad de la empresa. Es de vital importancia informar que las redes sociales son con mayor frecuencia la fuente con mayor relevancia para espiar datos personales. Los ciberataques de phishing por medio de sitios web maliciosos también son imaginables.

Para el tema de la suplantación de identidad se descargo una imagen de la electrificado del Caquetá y se asigno al perfil del correo soporteelectrocaqueta@gmail.com, con el cual se procedió a enviar una solicito de diligenciar un formulario requiriendo información de credenciales como se puede observar en la imagen 4.

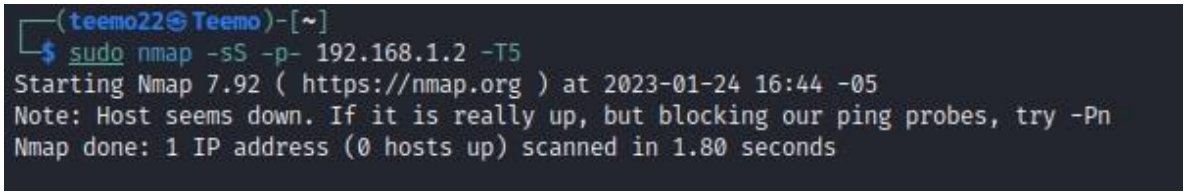
Imagen 4. Correo enviado suplantando la identidad de la empresa contratante.



Nota. Se solicitan determinados datos, los cuales se deben diligenciar en un formulario de Windows.

El primer activo tecnológico escaneado fue el del área de recepción con IP 192.168.1.2, el cual indico que tenía tanto servicios como los puertos cerrados como se puede apreciar en la imagen 5.

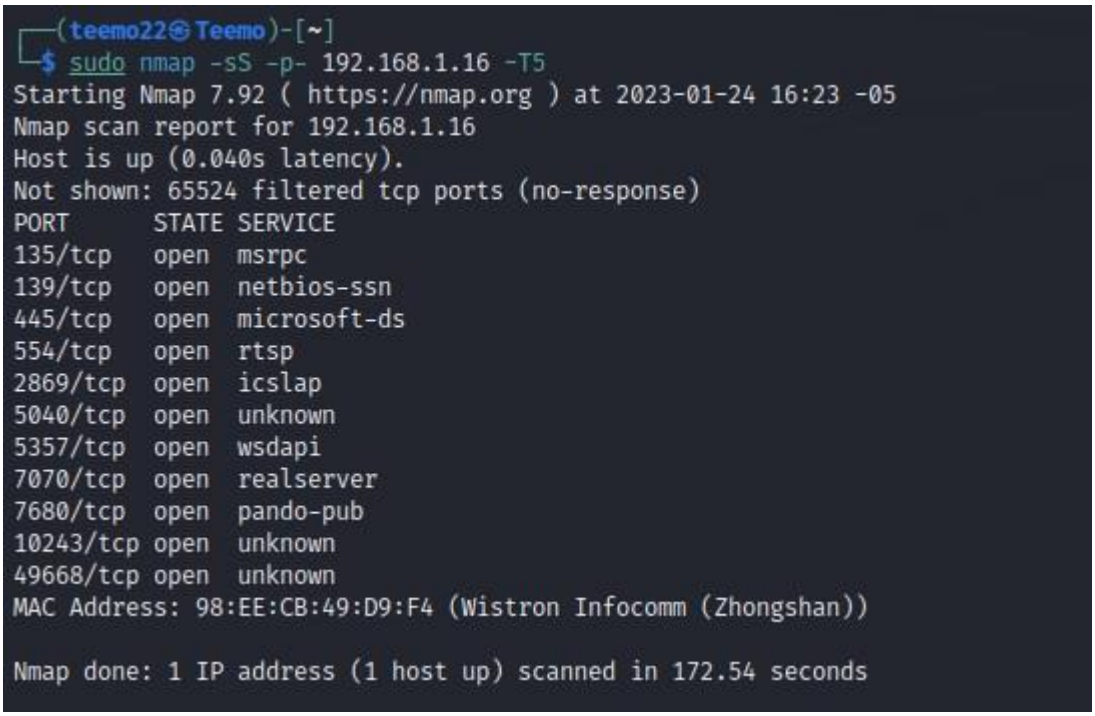
Imagen 5. Escaneo de puertos y servicios del computador del área de recepción con IP 192.168.1.2



Nota. De acuerdo al resultado, el activo tecnológico del área de recepción tiene los puertos y servicios cerrados.

El activo tecnológico escaneado con IP 192.168.1.16 pertenece al área de PQR de la oficina central, como se puede apreciar en la imagen 6, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

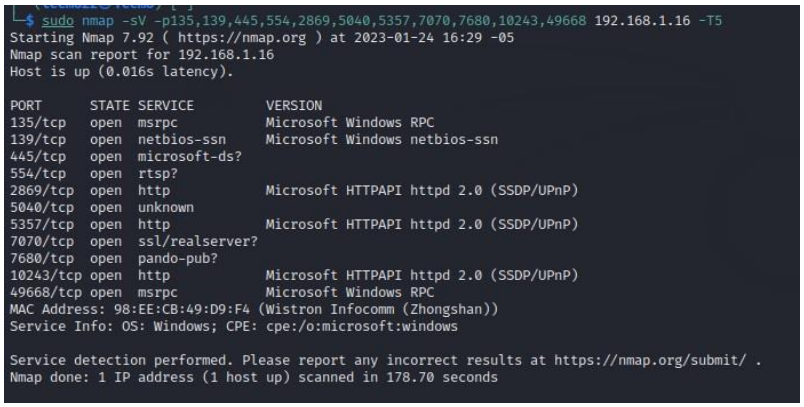
Imagen 6. Escaneo de puertos y servicios del computador del área de PQR con IP 192.168.1.16



Nota. Listado de puertos y servicios abiertos del computador del área de PQR con IP 192.168.1.16

Como se puede observar en la imagen 7, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.16 perteneciente al área de PQR, se lista información más precisa acerca de cada puerto y servicio abierto.

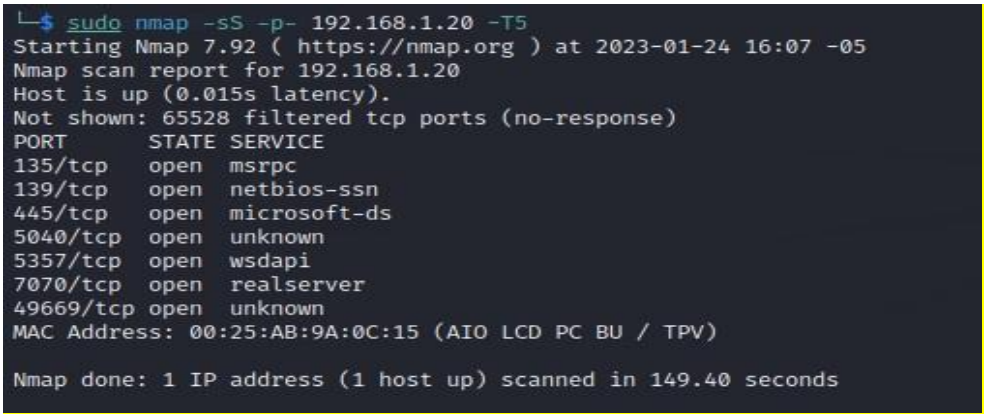
Imagen 7. Datos de los puertos del computador del área de PQR con IP 192.168.1.16



Nota. Información de la versión de los servicios de los puertos del computador del con IP 192.168.1.16.

El activo tecnológico escaneado con IP 192.168.1.20 pertenece al área de PQR de la oficina central, como se puede apreciar en la imagen 8, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

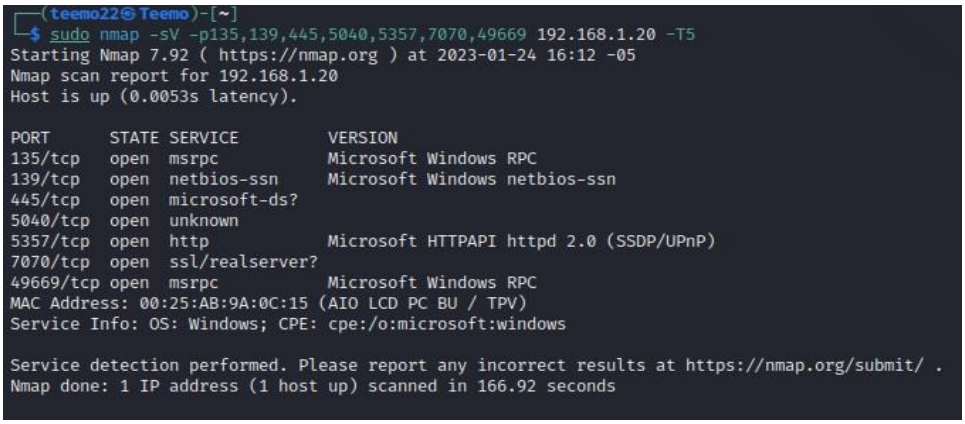
Imagen 8. Escaneo de puertos y servicios del computador del área de PQR con IP 192.168.1.20



Nota. Listado de puertos y servicios abiertos, lo que significa que el sistema está aceptando conexiones entrantes.

Como se puede observar en la imagen 9, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.20 perteneciente al área de PQR, se lista información más precisa acerca de cada puerto y servicio abierto.

Imagen 9. Datos de los puertos del computador del área de PQR con IP 192.168.1.20

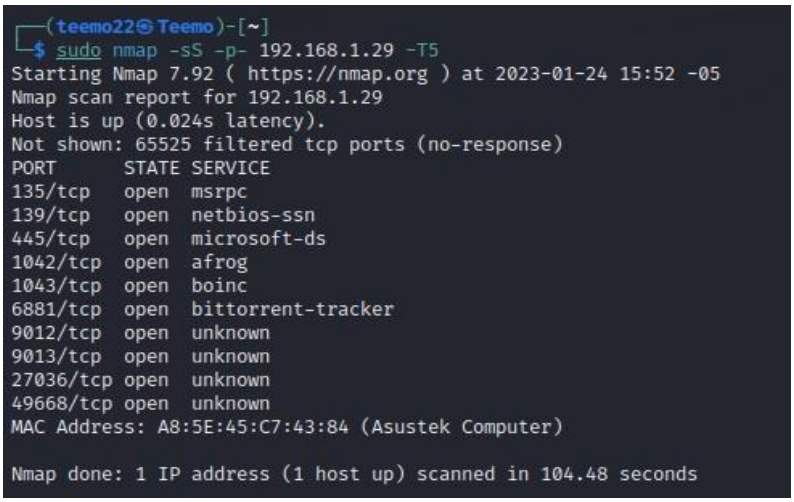


Nota. Información de la versión de los servicios de los puertos.

El activo tecnológico escaneado con IP 192.168.1.29 pertenece al área de PQR de la oficina central, como se puede apreciar en la imagen 10, tiene varios puertos

abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

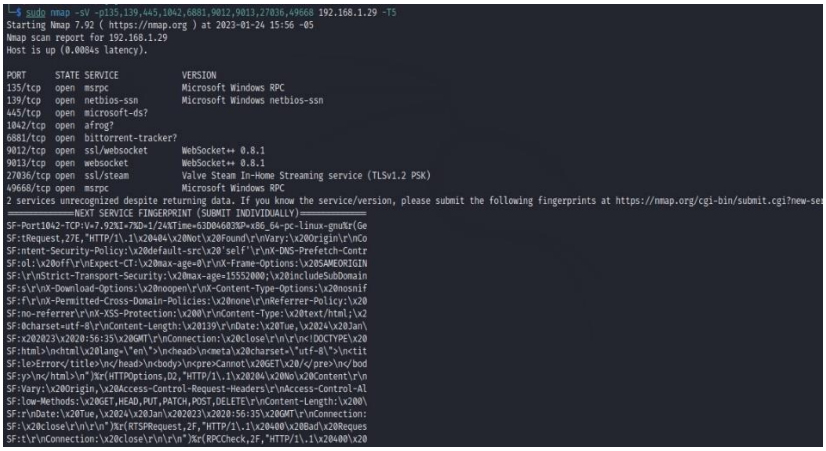
Imagen 10. Escaneo de puertos y servicios del computador del área de PQR con IP 192.168.1.29



Nota. Listado de puertos y servicios abiertos, lo que significa que el sistema está aceptando conexiones entrantes.

Como se puede observar en la imagen 11, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.29 perteneciente al área de PQR, se lista información más precisa acerca de cada puerto y servicio abierto.

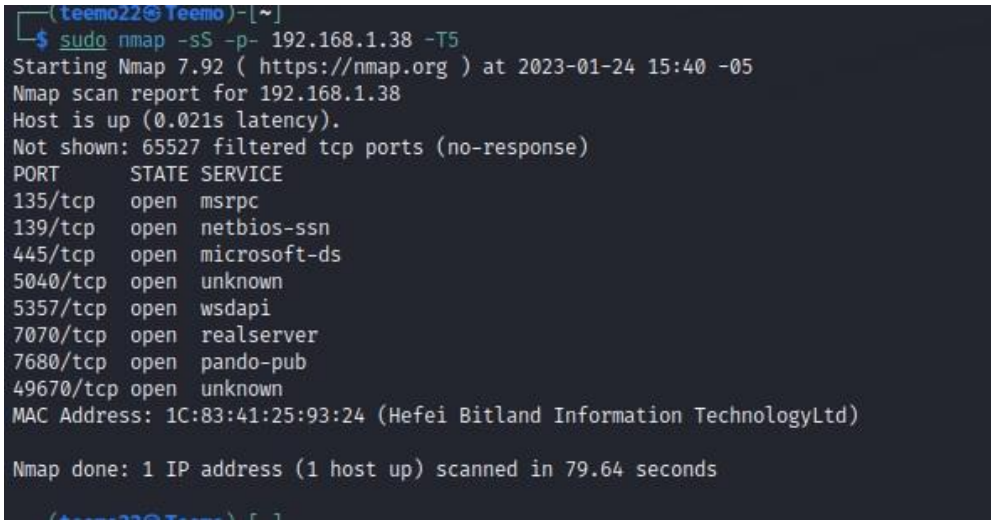
Imagen 11. Datos de los puertos del computador del área de PQR con IP 192.168.1.29



Nota. Información de la versión de los servidos de puertos.

El activo tecnológico escaneado con IP 192.168.1.38 pertenece al área de PQR de la oficina central, como se puede apreciar en la imagen 12, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

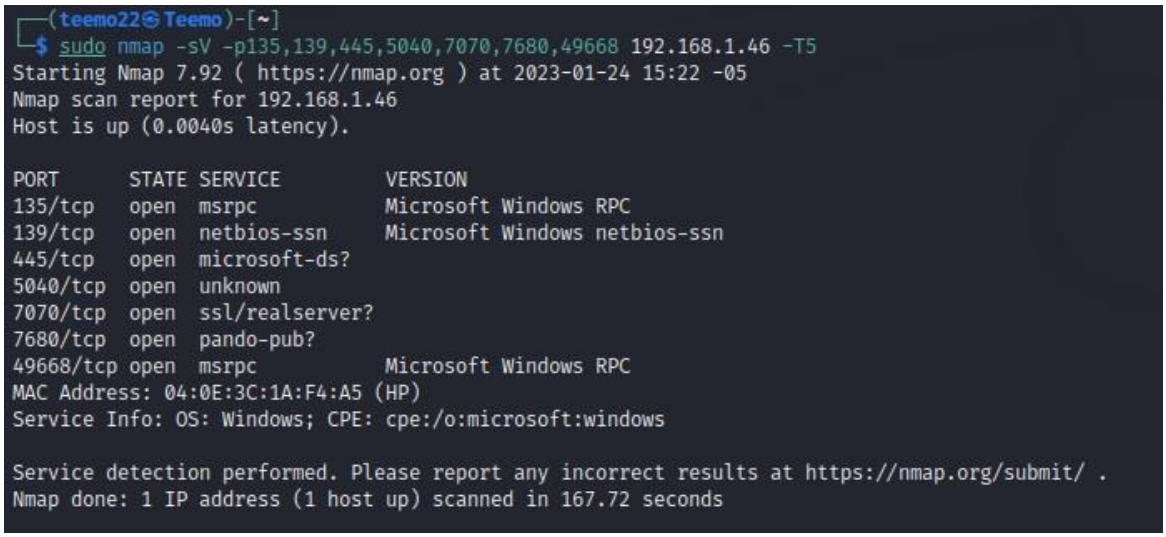
Imagen 12. Escaneo de puertos y servicios del computador del área de PQR con IP 192.168.1.38



Nota. Listado de puertos y servicios abiertos, lo que significa que el sistema está aceptando conexiones entrantes.

Como se puede observar en la imagen 13, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.38 perteneciente al área de PQR, se lista información más precisa acerca de cada puerto y servicio abierto.

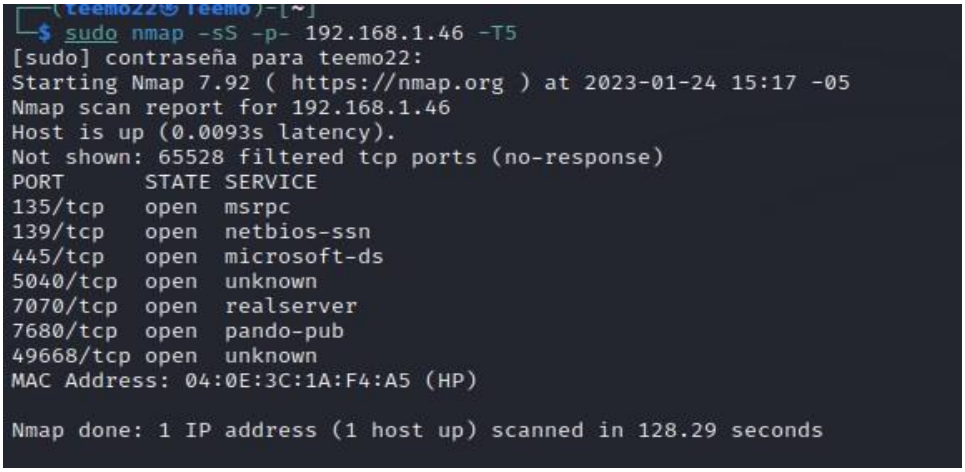
Imagen 13. Datos de los puertos del computador del área de PQR con IP 192.168.1.38



Nota. Información de la versión de los servicios de los puertos.

El activo tecnológico escaneado con IP 192.168.1.46 pertenece al área de PQR de la oficina central, como se puede apreciar en la imagen 14, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

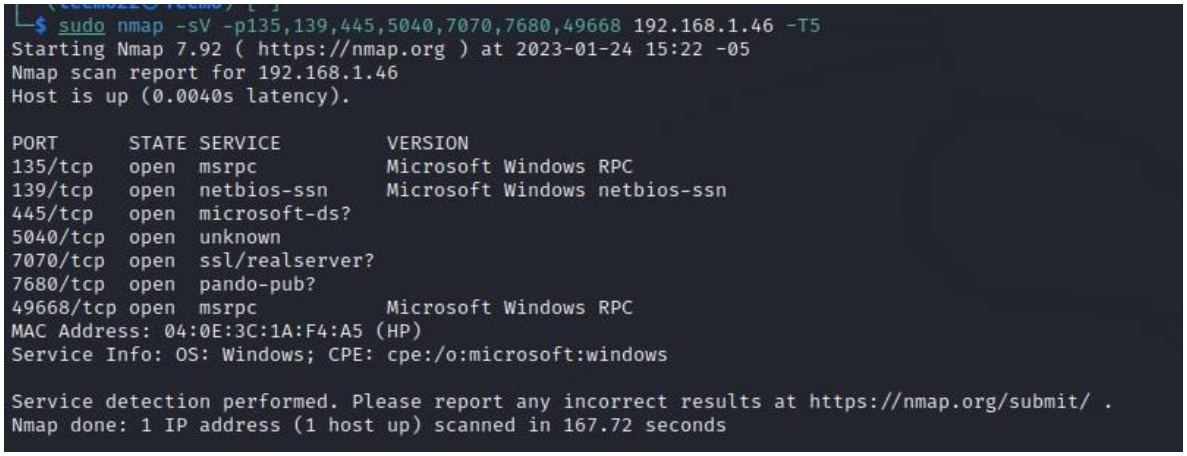
Imagen 14. Escaneo de puertos y servicios del computador del área de PQR con IP 192.168.1.46



Nota. Listado de puertos y servicios abiertos, lo que significa que el sistema está aceptando conexiones entrantes.

Como se puede observar en la imagen 15, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.46 perteneciente al área de PQR, se lista información más precisa acerca de cada puerto y servicio abierto.

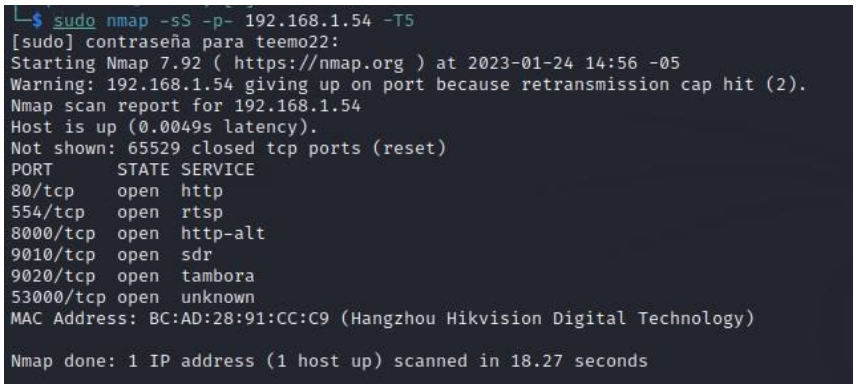
Imagen 15. Datos de los puertos del computador del área de PQR con IP 192.168.1.46



Nota. Información de la versión de los servicios de puertos.

El activo tecnológico escaneado con IP 192.168.1.54 pertenece al área de PQR de la oficina central, como se puede apreciar en la imagen 16, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

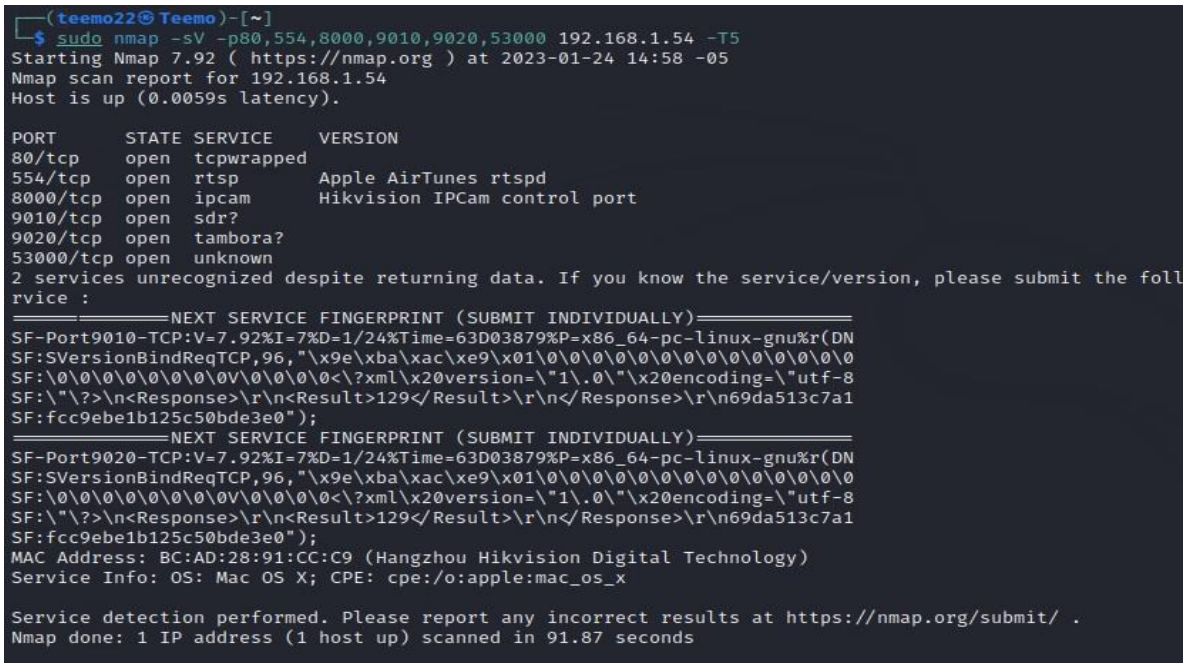
Imagen 16. Escaneo de puertos y servicios del computador del área de PQR con IP 192.168.1.54



Nota. Listado de puertos y servicios abiertos, lo que significa que el sistema está aceptando conexiones entrantes.

Como se puede observar en la imagen 17, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.54 perteneciente al área de PQR, se lista información más precisa acerca de cada puerto y servicio abierto.

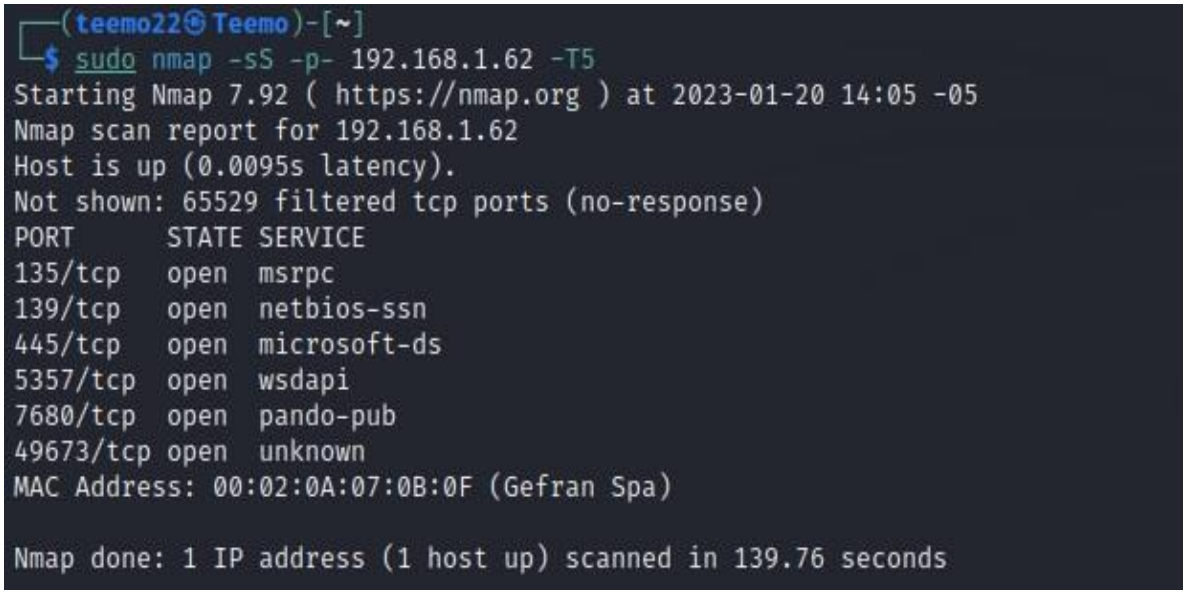
Imagen 17. Datos de los puertos del computador del área de PQR con IP 192.168.1.54



Nota. Información de la versión de los servicios de puertos.

El activo tecnológico escaneado con IP 192.168.1.62 pertenece al área de Talento Humano de la oficina central, como se puede apreciar en la imagen 18, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

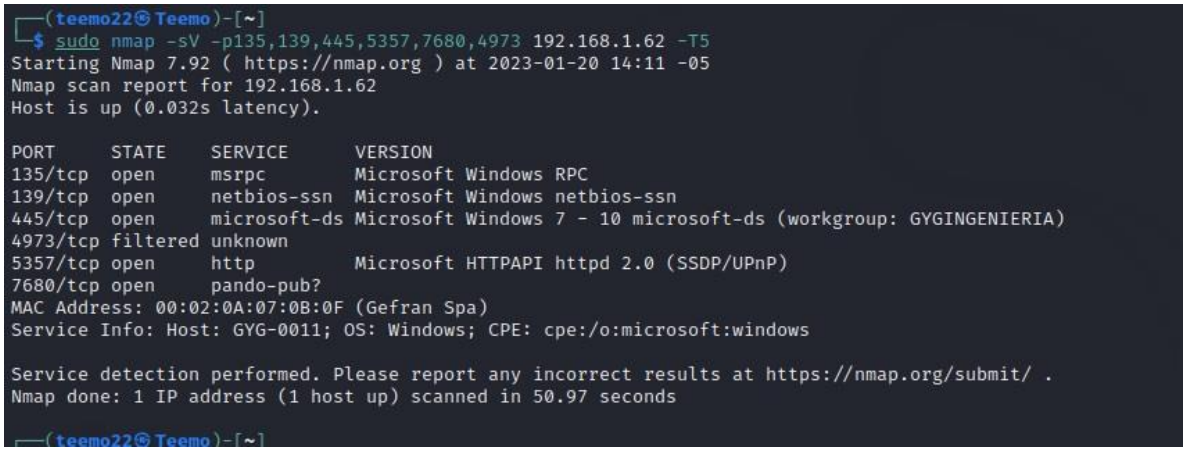
Imagen 18. Escaneo de puertos y servicios del computador del área de talento humano con IP 192.168.1.62



Nota. Listado de puertos y servicios abiertos, lo que significa que el sistema está aceptando conexiones entrantes.

Como se puede observar en la imagen 19, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.62 perteneciente al área de Talento Humano, se lista información más precisa acerca de cada puerto y servicio abierto.

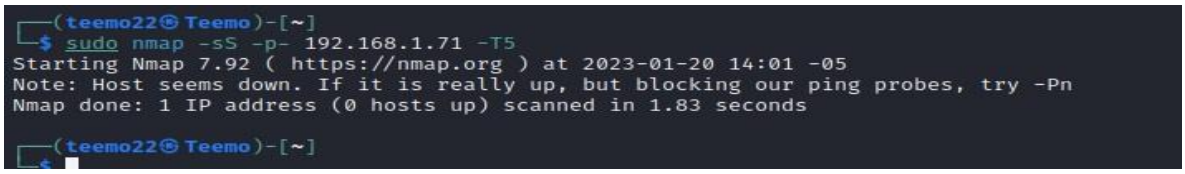
Imagen 19. Datos de los puertos del computador del área de talento humano con IP 192.168.1.62



Nota. Información de la versión de los servicios de puertos.

El activo tecnológico escaneado con IP 192.168.1.71 pertenece al área de Talento Humano de la oficina central, como se puede apreciar en la imagen 20, los servicios y puertos se encuentran cerrados, lo cual indica un mayor nivel de seguridad.

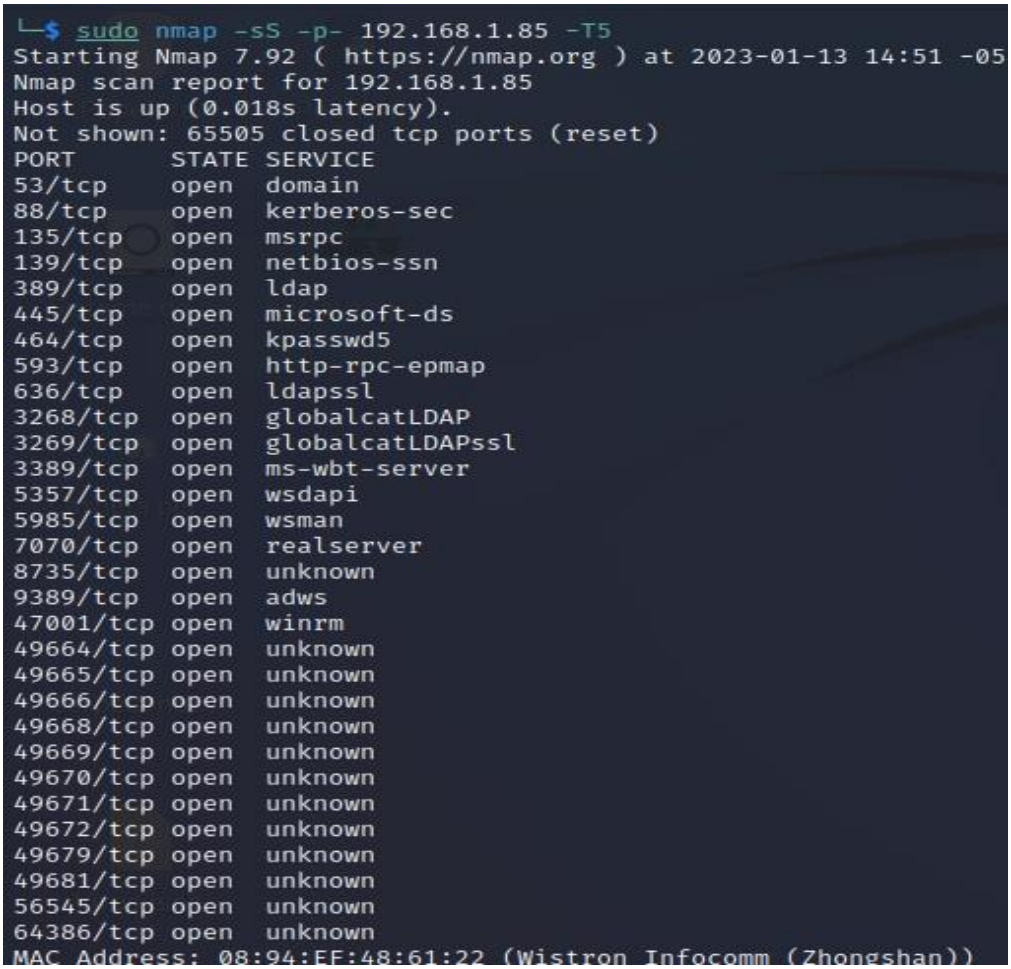
Imagen 20. Escaneo de puertos y servicios del computador del área de PQR con IP 192.168.1.71



Nota. No vulnerable debido a que tiene los puertos y servicios cerrados

El activo tecnológico escaneado con IP 192.168.1.85 pertenece al área de Almacén & dirección PQR, como se puede apreciar en la imagen 21, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

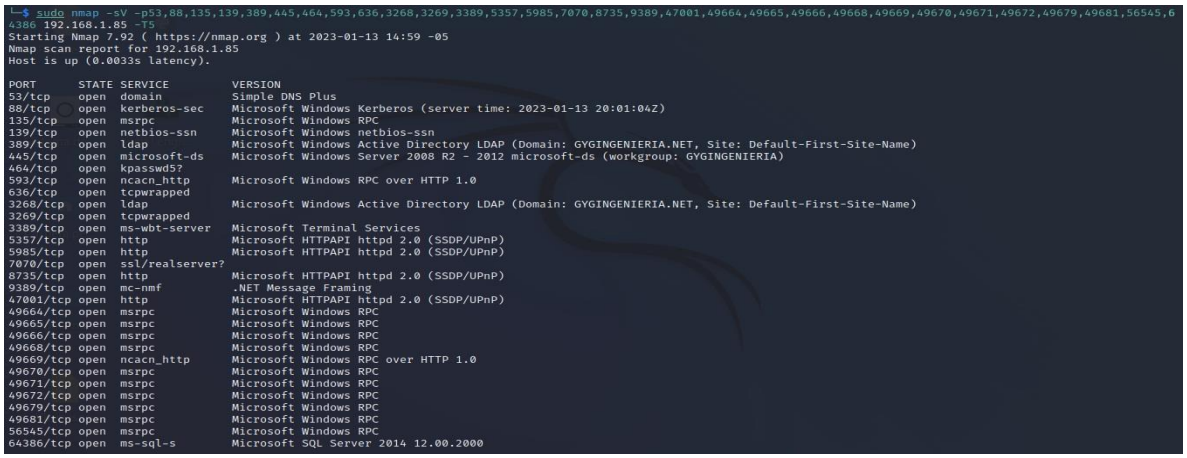
Imagen 21. Escaneo de puertos y servicios del computador del área de Almacén & dirección PQR con IP 192.168.1.85



Nota. Listado de puertos y servicios abiertos.

Como se puede observar en la imagen 22, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.85 perteneciente al área de Almacén & dirección PQR, se lista información más precisa acerca de cada puerto y servicio abierto.

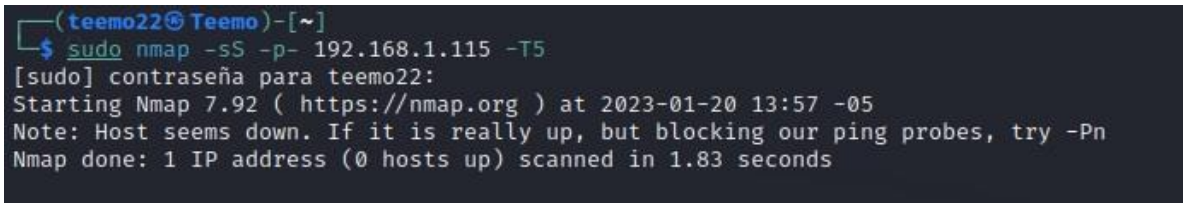
Imagen 22. Datos de los puertos del computador con IP 192.168.1.85



Nota. Información de la versión de los servicios de puertos.

El activo tecnológico escaneado con IP 192.168.1.115 pertenece al área de contabilidad, como se puede apreciar en la imagen 23, tiene cerrados los puertos y servicios representando un mayor nivel de seguridad.

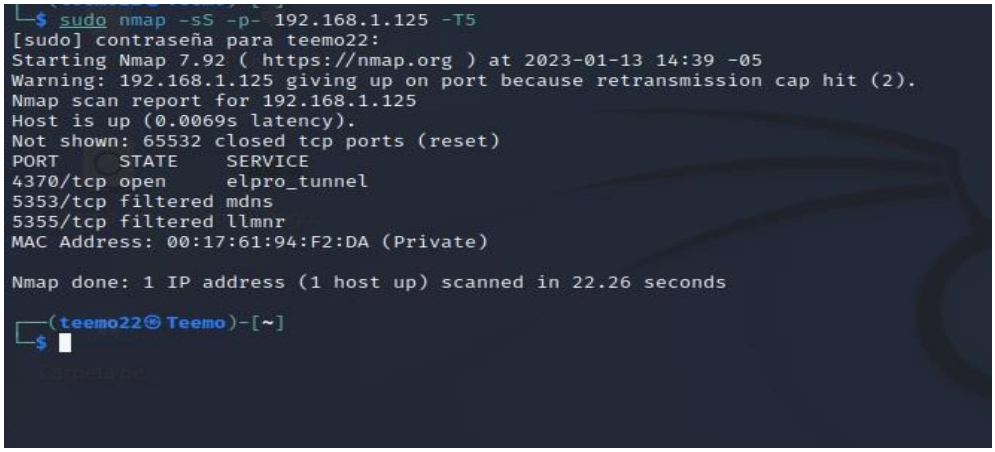
Imagen 23.Escaneo de puertos y servicios del computador del área de contabilidad con IP 192.168.1.115



Nota. No vulnerable debido a que tiene los puertos y servicios cerrados

El activo tecnológico escaneado con IP 192.168.1.125 pertenece al área de contabilidad, como se puede apreciar en la imagen 24, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

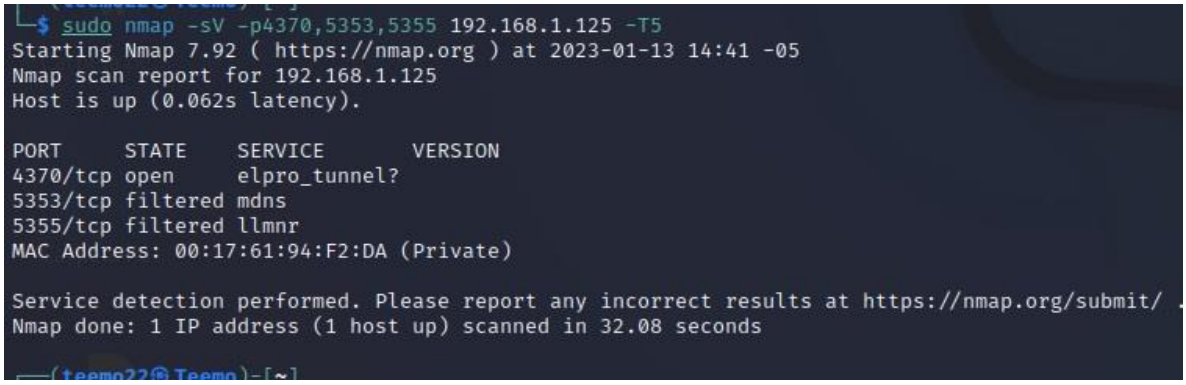
Imagen 24. Escaneo de puertos y servicios del computador del área de contabilidad con IP 192.168.1.125



Nota. Listado de puertos y servicios abiertos

Como se puede observar en la imagen 25, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.125 perteneciente al área de contabilidad, se lista información más precisa acerca de cada puerto y servicio abierto.

Imagen 25. Datos de los puertos del computador con IP 192.168.1.125

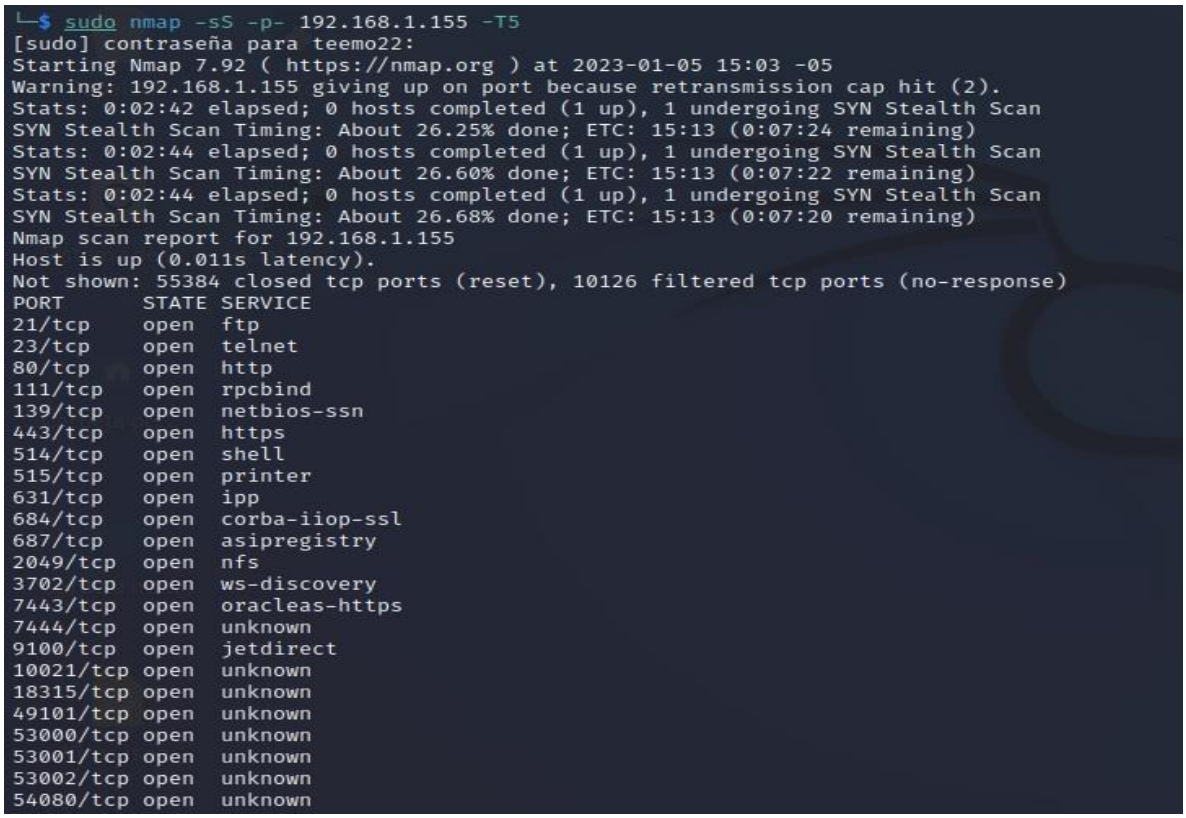


Nota. Información de la versión de los servicios de puertos.

El activo tecnológico escaneado con IP 192.168.1.155 pertenece al área de proyectos, como se puede apreciar en la imagen 26, tiene varios puertos abiertos

indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

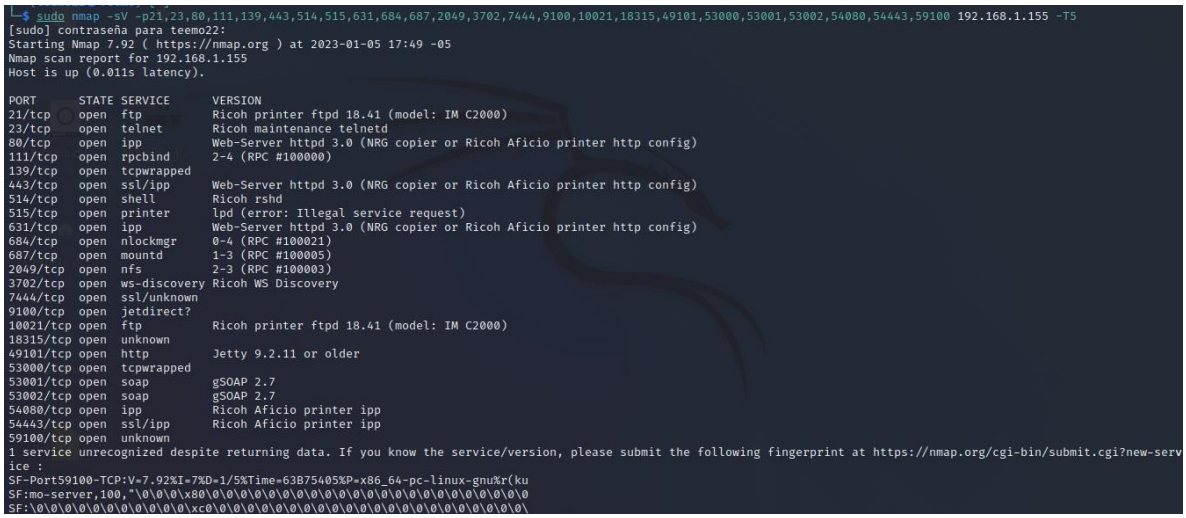
Imagen 26. Escaneo de puertos y servicios de la fotocopiadora del área de proyectos con IP 192.168.1.155



Nota. Listado de puertos y servicios abiertos

Como se puede observar en la imagen 27, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.155 perteneciente al área de proyectos, se lista información más precisa acerca de cada puerto y servicio abierto.

Imagen 27.Datos de los puertos de la fotocopiadora con IP 192.168.1.155



Nota. Información de la versión de los servicios de puertos.

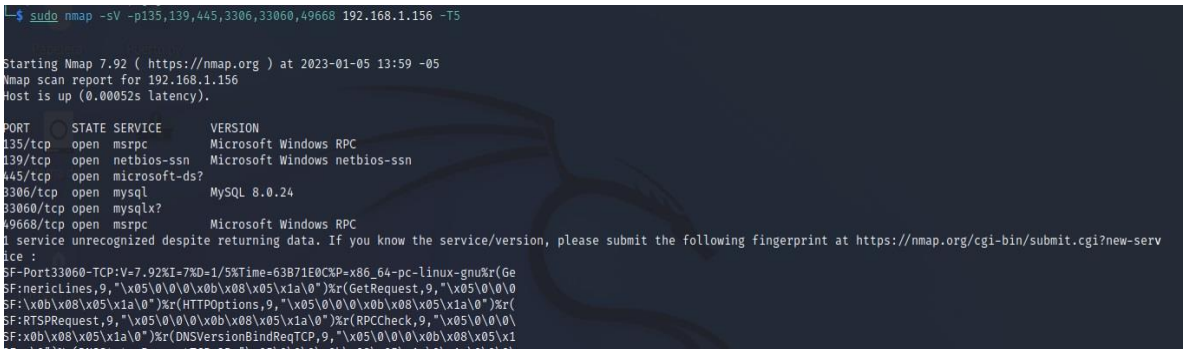
El activo tecnológico escaneado con IP 192.168.1.156 pertenece al área de proyectos, como se puede apreciar en la imagen 28, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

Imagen 28. Escaneo de puertos y servicios del computador del área de proyectos con IP 192.168.1.156

Nota. Listado de puertos y servicios abiertos

Como se puede observar en la imagen 29, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.156 perteneciente al área de proyectos, se lista información más precisa acerca de cada puerto y servicio abierto.

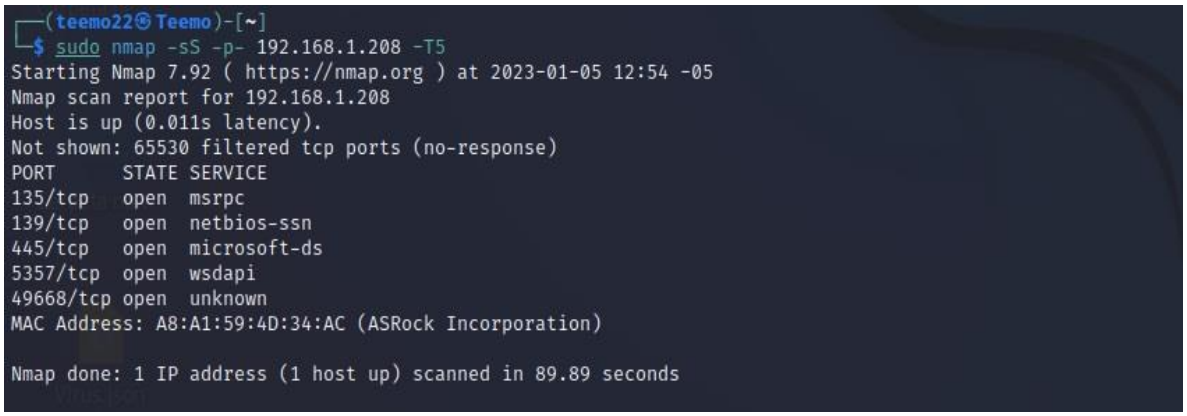
Imagen 29. Datos de los puertos del computador con IP 192.168.1.156



Nota. Información de la versión de los servicios de puertos.

El activo tecnológico escaneado con IP 192.168.1.208 pertenece al área de proyectos, como se puede apreciar en la imagen 30, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

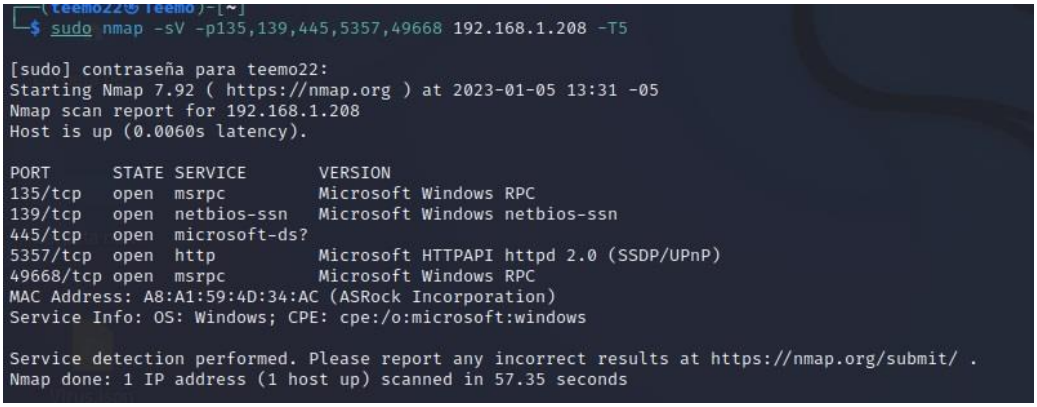
Imagen 30. Escaneo de puertos y servicios del computador del área de proyectos con IP 192.168.1.208



Nota. Listado de puertos y servicios abiertos.

Como se puede observar en la imagen 31, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.208 perteneciente al área de proyectos, se lista información más precisa acerca de cada puerto y servicio abierto.

Imagen 31.Datos de los puertos del computador del área de proyectos con IP 192.168.1.208



Nota. Información de la versión de los servicios de puertos.

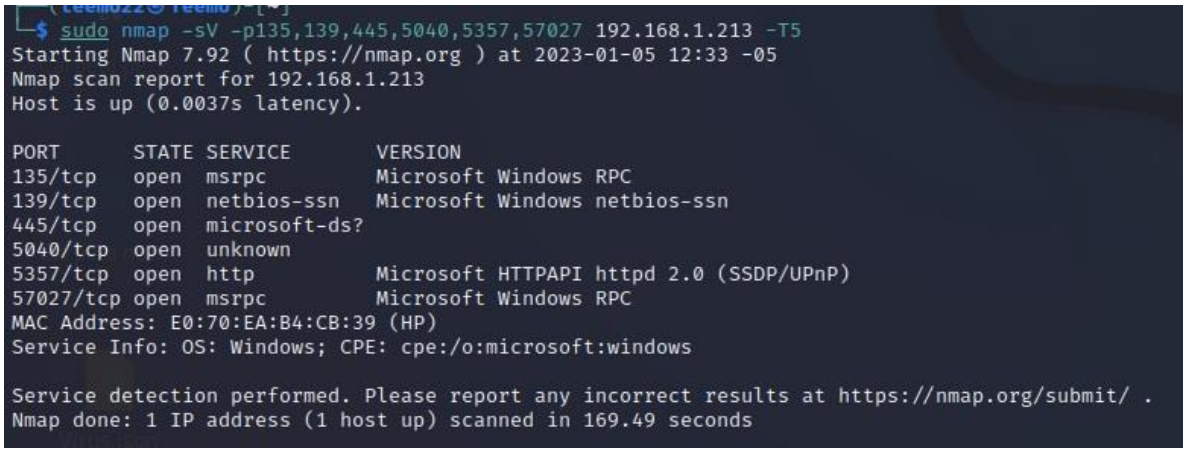
El activo tecnológico escaneado con IP 192.168.1.213 pertenece al área de Gerencia, como se puede apreciar en la imagen 32, tiene varios puertos abiertos indicando que se puede realizar procesos de testing para validar si tiene brecha de seguridad.

Imagen 32. Escaneo de puertos y servicios del computador del área de gerencia con IP 192.168.1.213

Nota. Listado de puertos y servicios abiertos

Como se puede observar en la imagen 33, con el comando ejecutado sobre el activo tecnológico con IP 192.168.1.213 perteneciente al área de gerencia, se lista información más precisa acerca de cada puerto y servicio abierto.

Imagen 33. Datos de los puertos del computador del área de gerencia con IP 192.168.1.213



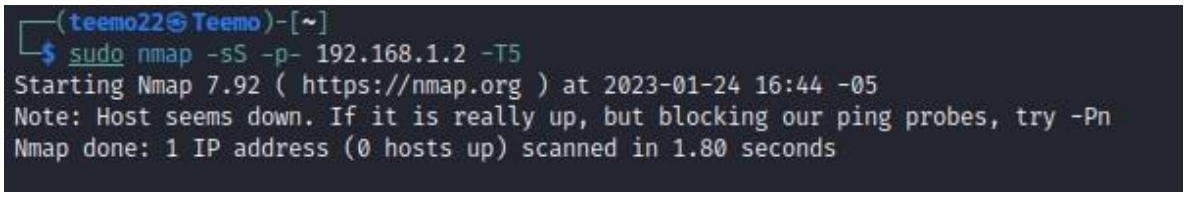
Nota. Información de la versión de los servicios de puertos.

4. Explotación

En esta fase se aprovechan las brechas de seguridad específicas en el sistema o en la red de la víctima, como consecuencia el ataque se centra a afectar el compromiso técnico. Teniendo en cuenta que hasta la fase 4 se procede debido a los límites establecidos para la prueba de pentesting.

El primer activo tecnológico escaneado fue el del área de recepción con IP 192.168.1.2, el cual indico que tenía tanto servicios como los puertos cerrados como se puede apreciar en la imagen 34, dejando en evidencia que debido a las actualizaciones del sistema operativo no es vulnerable,

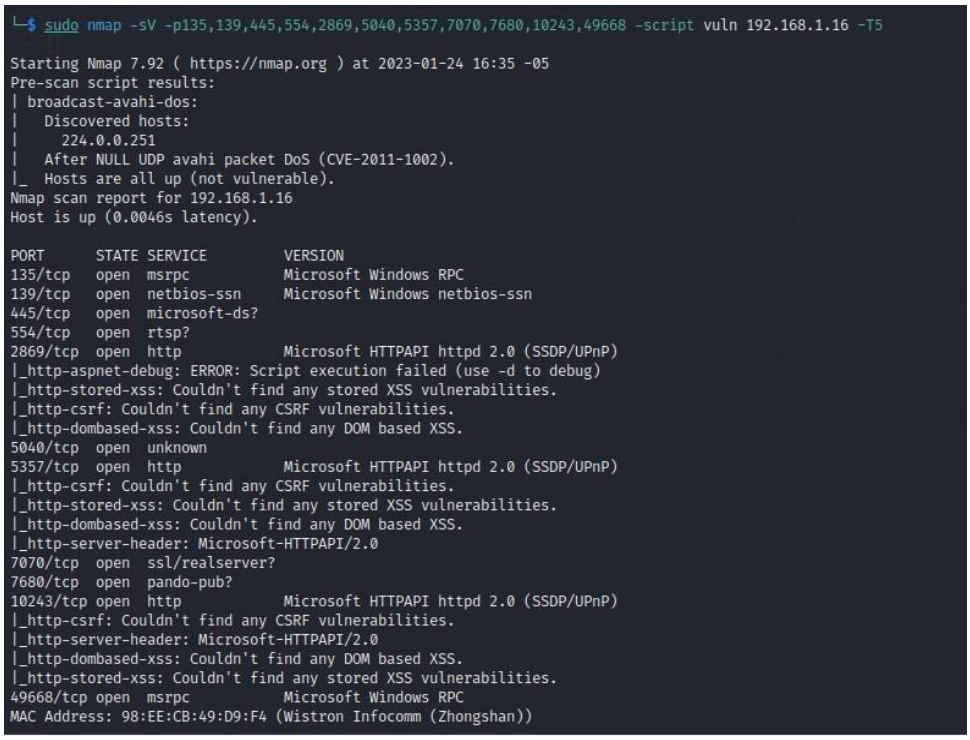
Imagen 34. Resultado de proceso de detección vulnerabilidades 192.168.1.2



Nota. El dispositivo no está escuchando ni aceptando conexiones entrantes en esos puertos específicos.

Como se puede observar en la imagen 35, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de PQR con IP 192.168.1.16, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

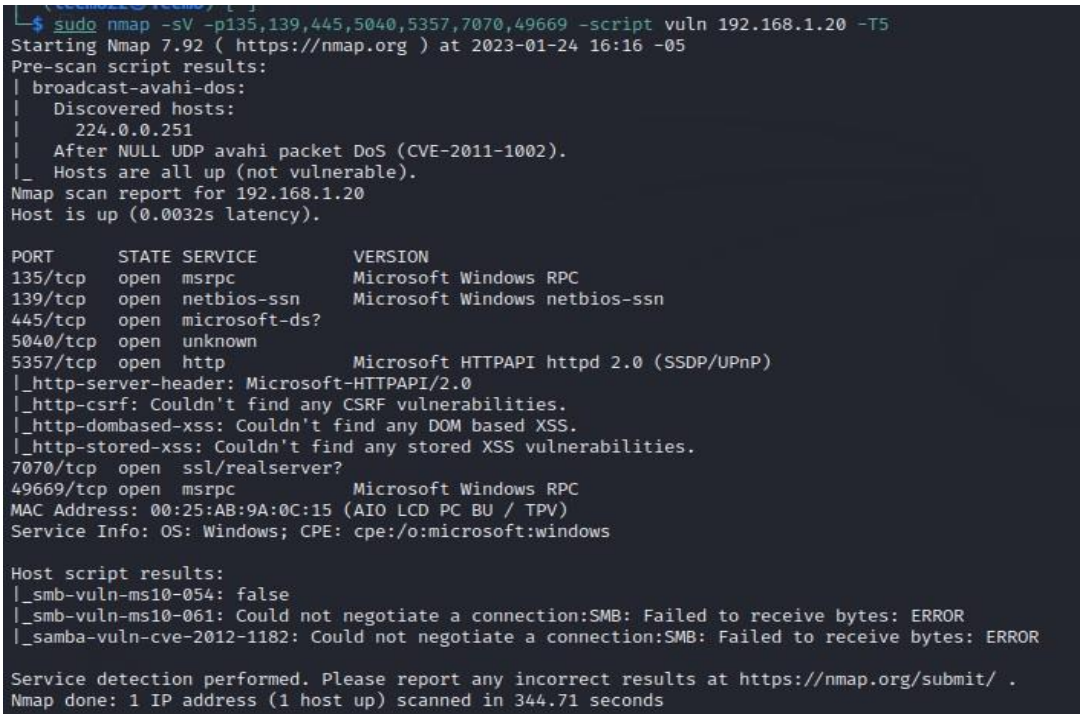
Imagen 35. Resultado de proceso de detección vulnerabilidades 192.168.1.16



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 36, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de PQR con IP 192.168.1.20, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

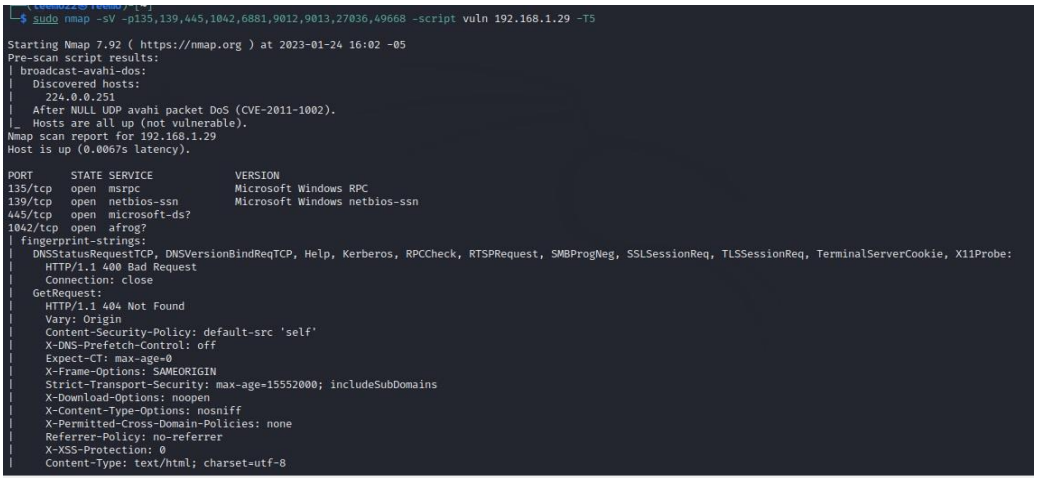
Imagen 36. Resultado de proceso de detección vulnerabilidades 192.168.1.20



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 37, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de PQR con IP 192.168.1.29, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

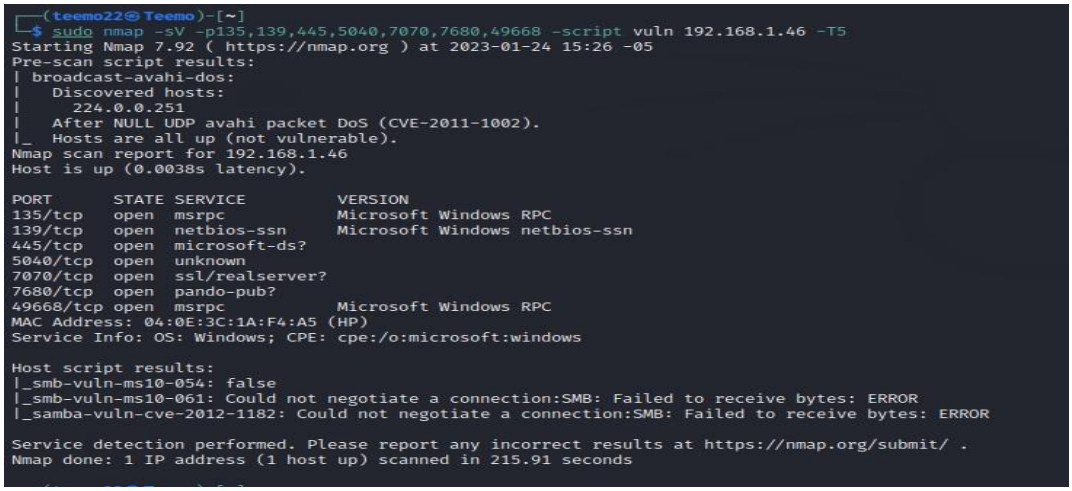
Imagen 37. Resultado de proceso de detección vulnerabilidades 192.168.1.29



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 38, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de PQR con IP 192.168.1.38, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

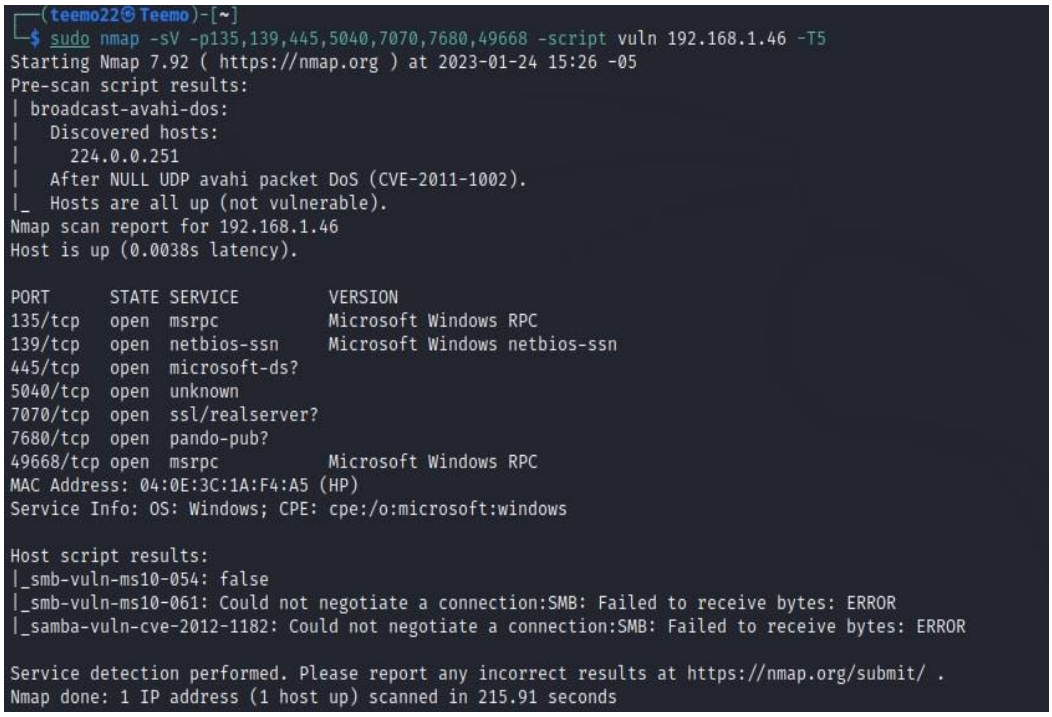
Imagen 38. Resultado de proceso de detección vulnerabilidades 192.168.1.38



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 39, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de PQR con IP 192.168.1.46, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

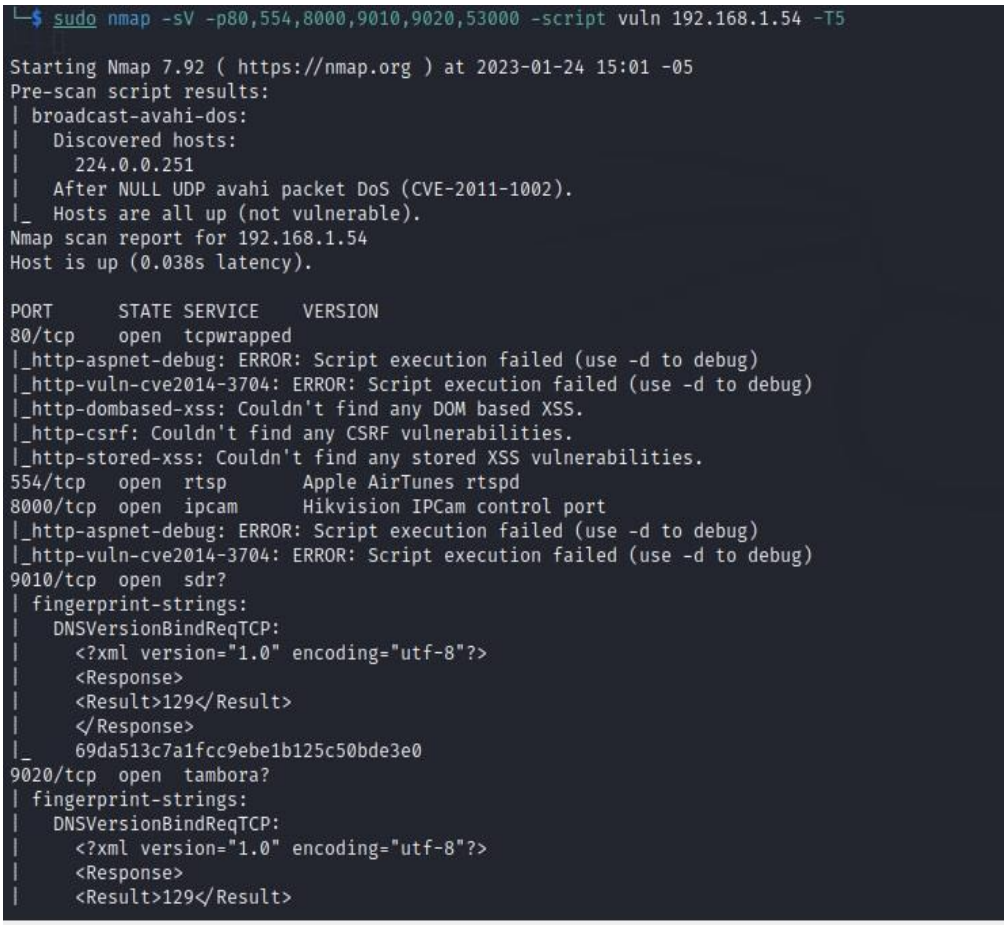
Imagen 39. Resultado de proceso de detección vulnerabilidades 192.168.1.46



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 40, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de PQR con IP 192.168.1.54, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

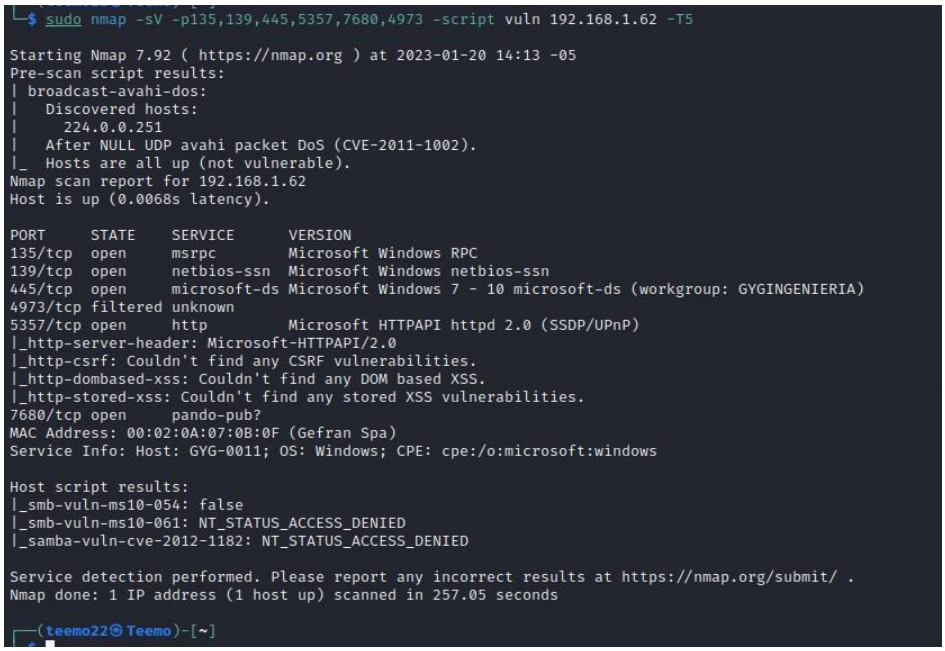
Imagen 40. Resultado de proceso de detección vulnerabilidades 192.168.1.54



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 41, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de Talento Humano con IP 192.168.1.62, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

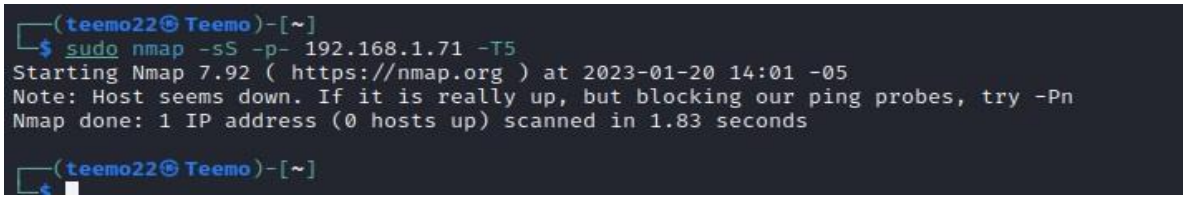
Imagen 41. Resultado de proceso de detección vulnerabilidades 192.168.1.62



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 42, se realiza el proceso de detección de vulnerabilidades con la herramienta Nmap al activo tecnológico del área de Talento Humano con IP 192.168.1.71, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar tiene los puertos y servicios cerrados, indicando un mayor nivel de seguridad debido a que se encuentra actualizado.

Imagen 42. Resultado de proceso de detección vulnerabilidades 192.168.1.71



Nota. El dispositivo no está escuchando ni aceptando conexiones entrantes en esos puertos específicos.

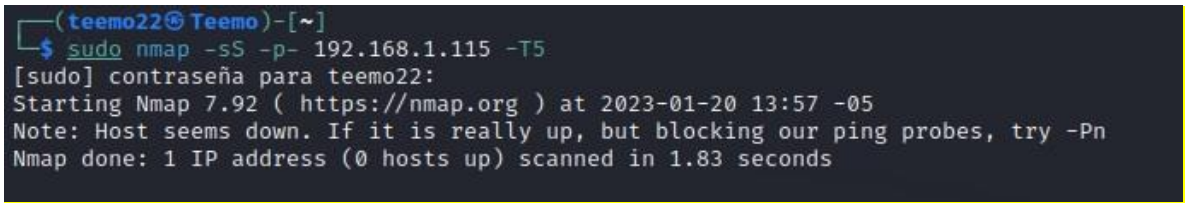
Como se puede observar en la imagen 43, se realiza el proceso de detección de vulnerabilidades con la herramienta Nmap al activo tecnológico del área de Almacén & dirección PQR con IP 192.168.1.71, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar tiene los puertos y servicios cerrados, indicando un mayor nivel de seguridad debido a que se encuentra actualizado.

Imagen 43. Resultado de proceso de detección vulnerabilidades 192.168.1.85

Nota. El dispositivo no está escuchando ni aceptando conexiones entrantes en esos puertos específicos.

Como se puede observar en la imagen 44, se realiza el proceso de detección de vulnerabilidades con la herramienta Nmap al activo tecnológico del área de contabilidad con IP 192.168.1.115, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar tiene los puertos y servicios cerrados, indicando un mayor nivel de seguridad debido a que se encuentra actualizado.

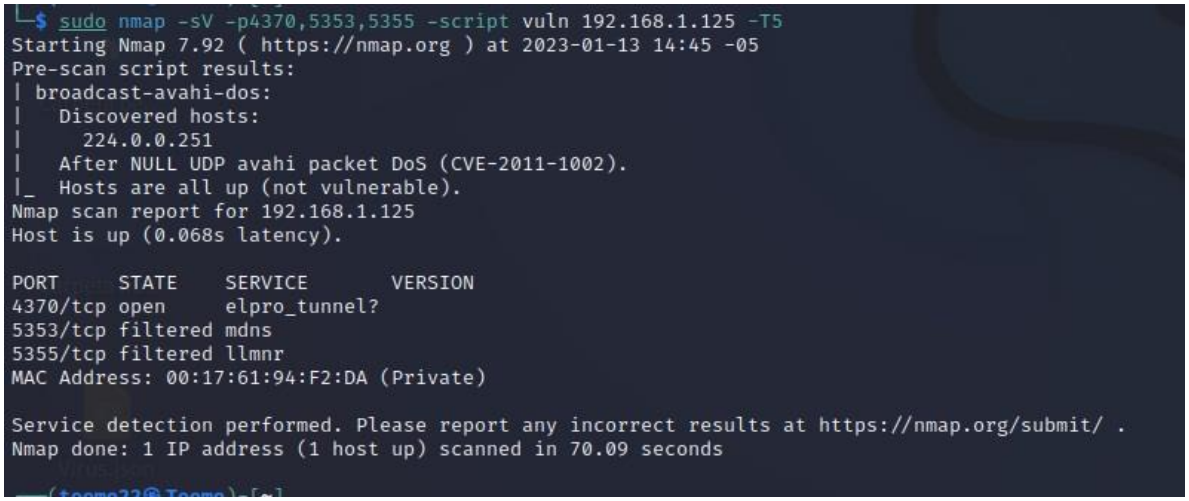
Imagen 44. Resultado del proceso de detección de vulnerabilidades del computador del área de contabilidad con IP 192.168.1.115



Nota. El dispositivo no está escuchando ni aceptando conexiones entrantes en esos puertos específicos.

Como se puede observar en la imagen 45, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de contabilidad con IP 192.168.1.125, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

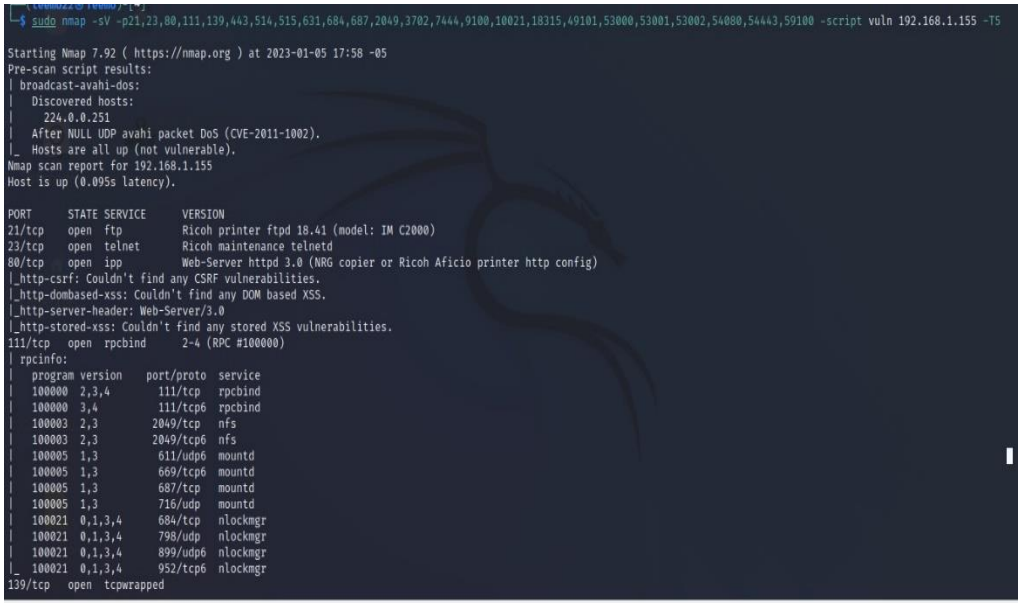
Imagen 45. Resultado de proceso de detección vulnerabilidades del computador del área de contabilidad con IP 192.168.1.125



Nota. El dispositivo no es vulnerable debido a que las versiones de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 46, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de proyectos con IP 192.168.1.155, dicho proceso busca en la base de datos del software las brechas conocidas, se puede apreciar que genero un reporte el cual indica una mayor información sobre los puertos y servicios, listando las vulnerabilidades conocidas.

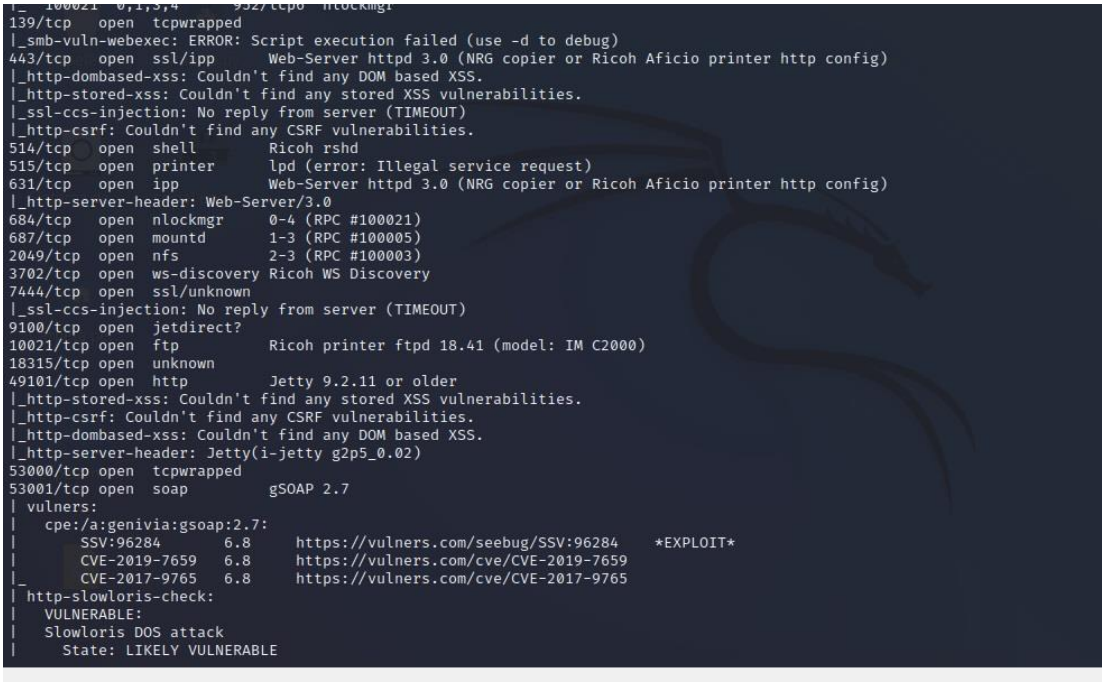
Imagen 46. Resultado del proceso de detección de vulnerabilidades de la fotocopiadora del área de proyectos con IP 192.168.1.155



Nota. Ejecución del comando – script vuln

Como se puede observar en la imagen 47, se realizó el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de proyectos con IP 192.168.1.155, se puede apreciar la primera parte del reporte el cual muestra dos vulnerabilidades conocidas la CVE-2019-7659 y CVE -2017-9765 en el servicio TCP soap versión gsoap 2.7, dicho protocolo es el encargado de la comunicación que permite la interacción entre la fotocopiadora y otros dispositivos o sistemas a través de la red.

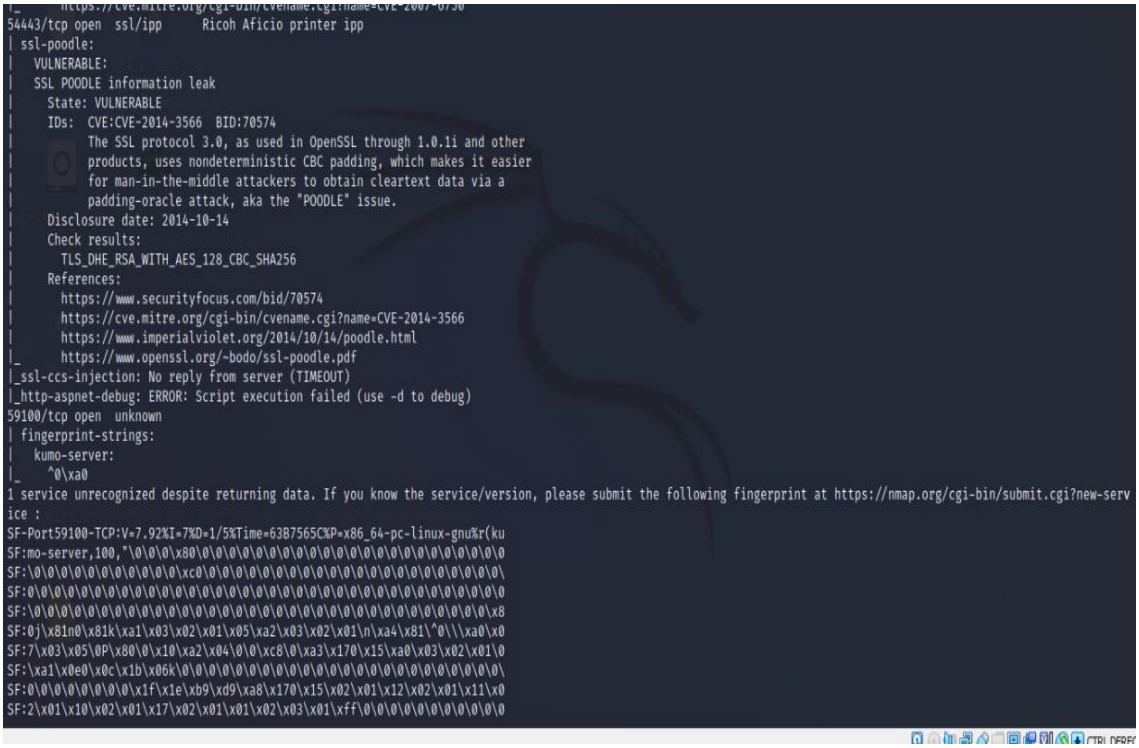
Imagen 47. Parte 1 del Reporte de vulnerabilidades de la fotocopiadora con IP 192.168.1.155



Nota. Reporte de vulnerabilidades en el dispositivo.

Como se puede observar en la imagen 48, se realizó el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de proyectos con IP 192.168.1.155, se puede apreciar la segunda parte del reporte el cual muestra una vulnerabilidad conocida la CVE-2014-3566 en el servicio TCP SSL POODLE, es el protocolo de seguridad que proporciona comunicaciones seguras a través de Internet. POODLE es una vulnerabilidad de seguridad que afecta a ciertas implementaciones de SSL y TLS. Permite a un atacante descifrar el contenido de las cookies de sesión y otros datos confidenciales transmitidos a través de una conexión cifrada.

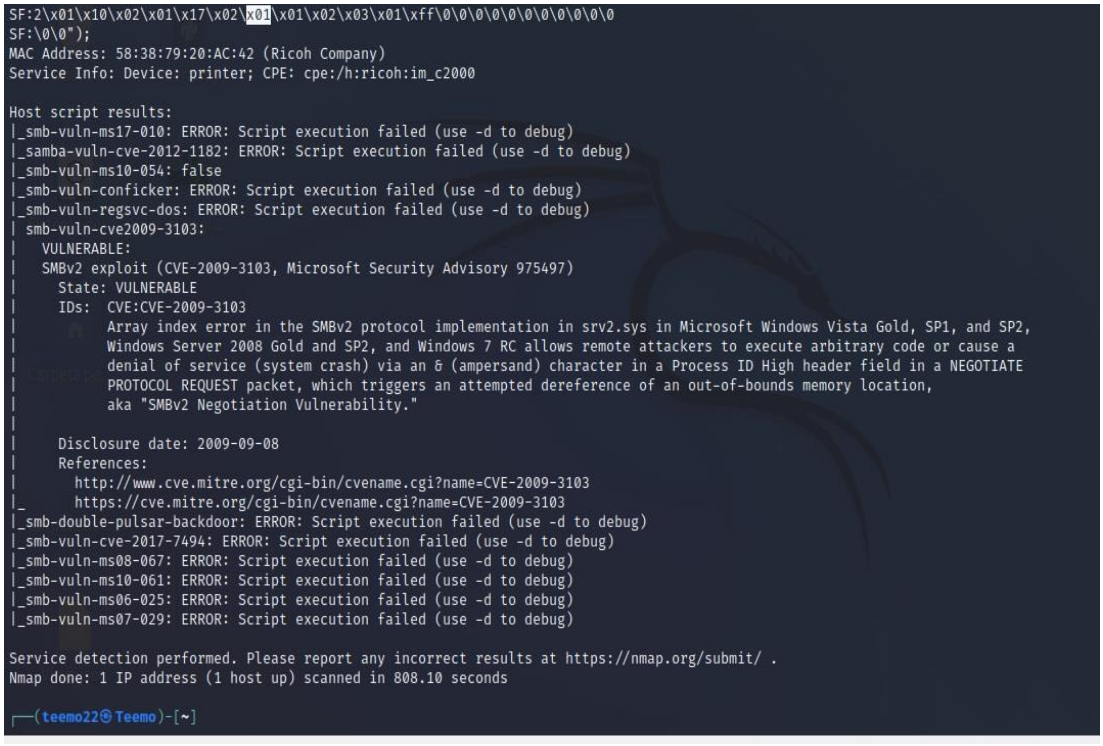
Imagen 48. Parte 2 del Reporte de vulnerabilidades de la fotocopiadora con IP 192.168.1.155



Nota. Se evidencia vulnerabilidades en el dispositivo.

Como se puede observar en la imagen 49, se realizó el proceso de detección de vulnerabilidades en el activo tecnológico del área de proyectos con IP 192.168.1.155, se puede apreciar la tercera parte del reporte el cual muestra una vulnerabilidad conocida la CVE-2009-3103, la cual está en el servicio SMB, el cual es un protocolo de red utilizado principalmente para proporcionar acceso a archivos, impresoras y otros recursos compartidos en una red local.

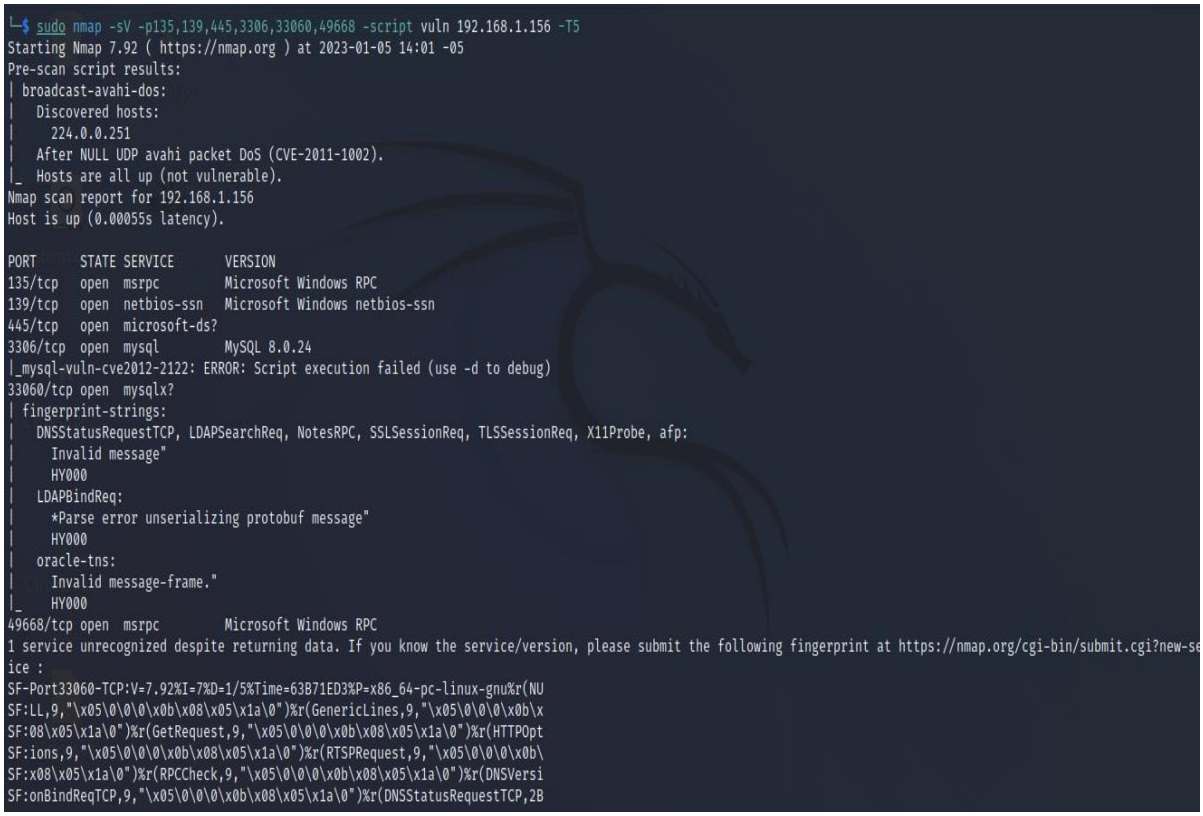
Imagen 49. Parte 3 del Reporte de vulnerabilidades de la fotocopiadora con IP 192.168.1.155



Nota. Entrega de reporte de CVE.

Como se puede observar en la imagen 50, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de proyectos con IP 192.168.1.156, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

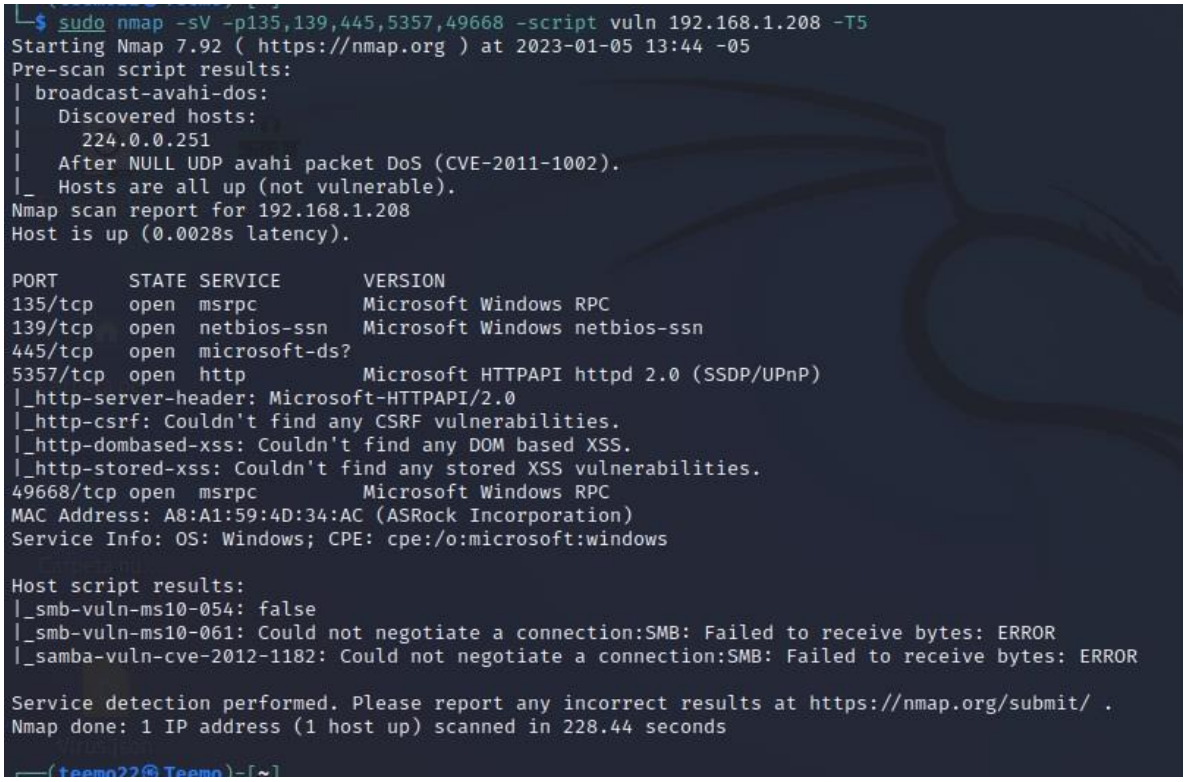
Imagen 50. Resultado de proceso de detección vulnerabilidades del computador del área de proyectos con 192.168.1.156



Nota. El dispositivo no es vulnerable debido a que la versión de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 51, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de proyectos con IP 192.168.1.208, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

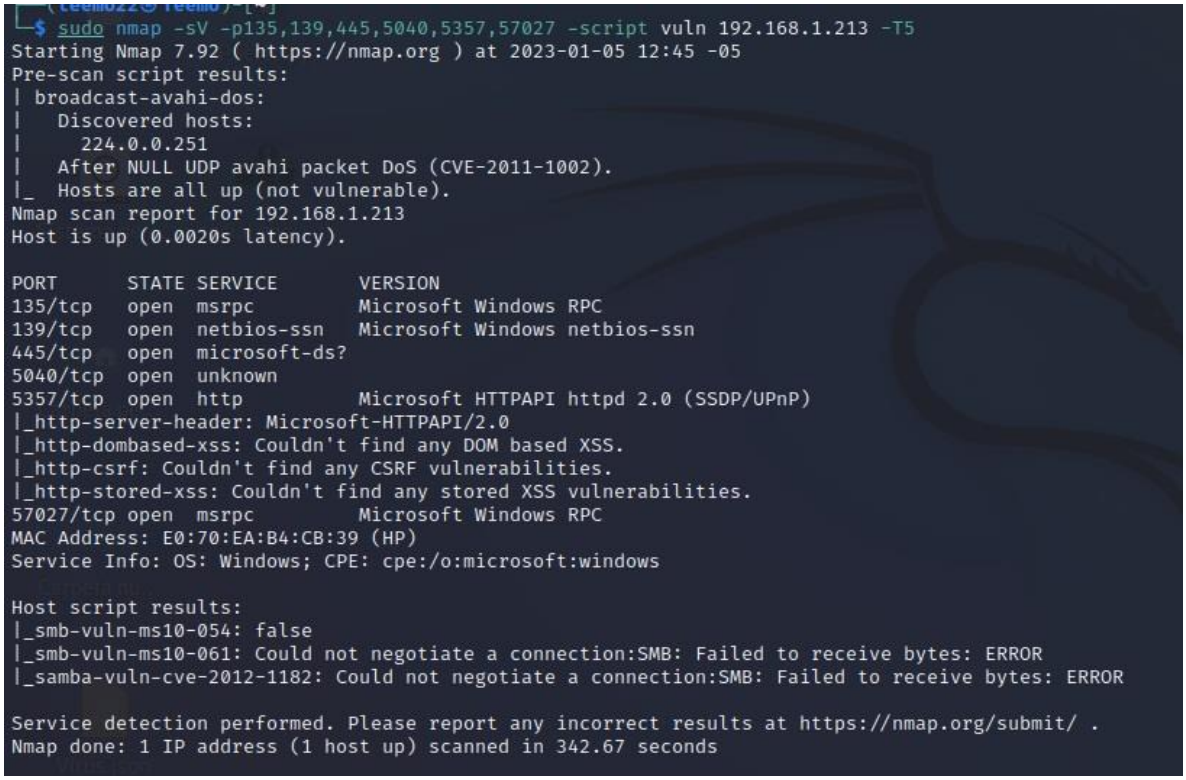
Imagen 51. Resultado del proceso de detección de vulnerabilidades del computador del área de proyectos con IP 192.168.1.208



Nota. El dispositivo no es vulnerable debido a que la versión de los puertos y servicios no tienen vulnerabilidades conocidas.

Como se puede observar en la imagen 52, se realiza el proceso de detección de vulnerabilidades con el comando -script vuln de la herramienta Nmap al activo tecnológico del área de gerencia con IP 192.168.1.213, dicho proceso busca en la base de datos del software las brechas conocidas, pero como se puede apreciar debido a que se encuentra actualizado no cuenta con vulnerabilidades aprovechables.

Imagen 52. Resultado del proceso de detección de vulnerabilidades del computador del área de gerencia con 192.168.1.213



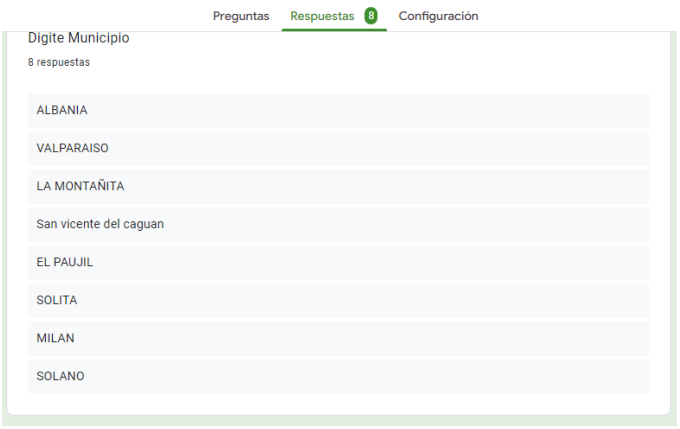
Nota. El dispositivo no es vulnerable debido a que la versión de los puertos y servicios no tienen vulnerabilidades conocidas.

Datos revelados

En este apartado se ilustran una parte de las respuestas de los auxiliares administrativos, ya que otras son de privacidad de la empresa, ya que compartieron las contraseñas de la plataforma GYG y escritorio remoto.

Como se había mencionado en anterior ocasión el proceso de ingeniería que se inició hacer por medio de los correos ver imagen 4, en la imagen 53 se puede observar que de las 12 oficinas 8 respondieron, dichas oficinas se encuentran distribuidas en varios municipios del departamento del Caquetá ver imagen 1.

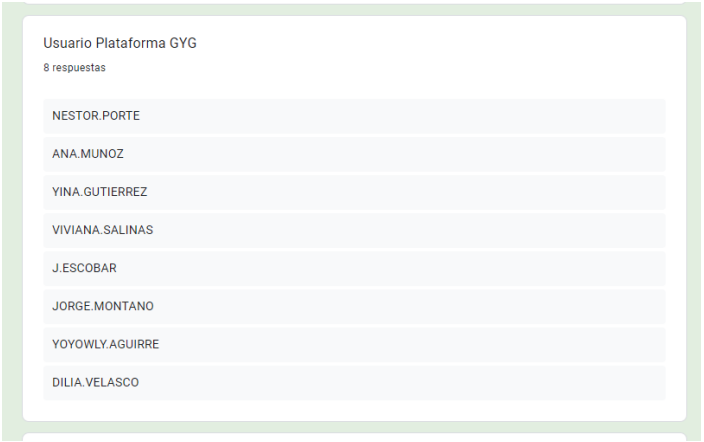
Imagen 53. Sedes Municipios



Nota. Auxiliares de los municipios que fueron susceptibles ante el ataque de la ingeniería social.

En la imagen 53 se puede apreciar como los auxiliares entregaron las credenciales de acceso de la plataforma de la empresa GYG INGENIERÍA S.A.S., cabe aclarar que, por motivos de confidencialidad con la organización, no se tomó captura de las contraseñas de acceso.

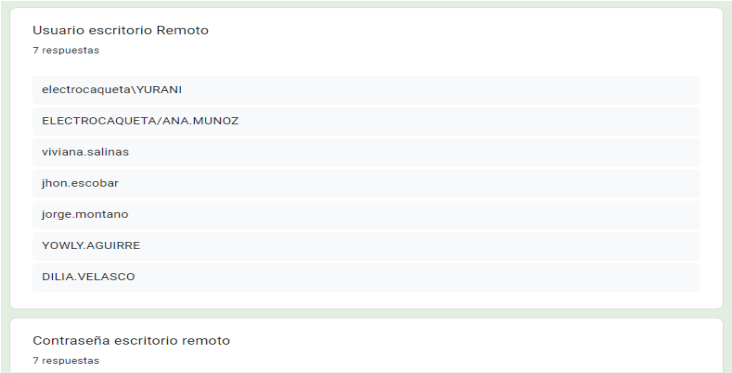
Imagen 54. Nombre de usuarios de la plataforma GYG



Nota. En este apartado se ilustra los usuarios entregados por parte del personal ante la suplantación de identidad de la empresa contratante ElectroCaquetá.

En la imagen 55 se puede apreciar como los auxiliares entregaron las credenciales de acceso del escritorio remoto de cada uno de los equipos de cómputo asignado, en este caso solo hubo 7 respuestas debido a que uno de los auxiliares llevaba poco tiempo y aun no tenía dicha información, cabe aclarar que, por motivos de confidencialidad con la organización, no se tomó captura de las contraseñas de acceso

Imagen 55. Usuario escritorio remoto



Nota. Respuestas de los usuarios escritorio remoto, cabe aclarar que también entregaron las contraseñas.

Como se puede evidenciar en las imágenes en el transcurso del desarrollo del objetivo 6.2 ejecutado, las herramientas necesarias para llevar a cabo el proceso de testeo fueron Kali Linux, NMAP, METASPLOIT. En cuanto al método de phishing llevado a cabo se uso GMAIL, permitiendo la suplantación de identidad del soporte técnico de la empresa contratante Electrificadora del Caquetá.

6.3. ANALIZAR LOS RESULTADOS OBTENIDOS DE LA METODOLOGÍA IMPLEMENTADA, GENERANDO UNA LISTA DE VULNERABILIDADES DEPENDIENDO DE SU NIVEL DE IMPACTO, PARA FINALMENTE ENTREGAR EL INFORME CON LOS HALLAZGOS ENCONTRADOS.

Ataque simulado de ingeniería social

6.3.1. Nivel de impacto

Para medir el nivel de impacto, se implementó una matriz de riesgos con las siguientes características:

La tabla 2 es una herramienta utilizada en la gestión de riesgos para evaluar y clasificar los riesgos según su probabilidad y su impacto. Por lo general, esta tabla tiene dos ejes: uno que representa la probabilidad de que ocurra un evento y otro que representa el impacto que tendría ese evento si llegara a ocurrir. A menudo se utiliza una escala numérica o de colores como se aprecia en la tabla 3 para categorizar estos niveles de probabilidad e impacto. La tabla 2 proporciona una forma visual de priorizar los riesgos y asignar recursos para gestionarlos de manera efectiva. donde la intersección entre la probabilidad y el impacto determina el nivel de riesgo.

Tabla 2. Matriz de riesgo

		MATRIZ DE RIESGO				
		IMPACTO				
		MÍNIMA	MENOR	MODERADA	MAYOR	MÁXIMA
PROBABILIDAD		1	2	4	8	16
MUY ALTA	5	5	10	20	40	80
ALTA	4	4	8	16	32	64
MEDIA	3	3	6	12	24	48
BAJA	2	2	4	8	16	32
MUY BAJA	1	1	2	4	8	16

Fuente. Autoría propia

Tabla 3. Color nivel de riesgo

NIVEL DE RIESGO	COLOR
Riesgo aceptable	
Riesgo tolerable	
Riesgo alto	
Riesgo extremo	

Fuente. Autoría propia

Teniendo en cuenta los parámetros de la tabla 2, se procede a indicar el nivel de riesgo en cada dispositivo en la tabla 4, los cuales fueron evaluados en el ITEM 6.2.

Tabla 4. Nivel de impacto

ÁREA	IP	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
Recepción	192.168.1.2	muy baja	menor	Riesgo aceptable
PQR	192.168.1.16	baja	moderada	Riesgo tolerable
PQR	192.168.1.20	baja	moderada	Riesgo tolerable
PQR	192.168.1.29	baja	moderada	Riesgo tolerable
PQR	192.168.1.38	baja	moderada	Riesgo tolerable
PQR	192.168.1.46	baja	moderada	Riesgo tolerable
PQR	192.168.1.54	baja	moderada	Riesgo tolerable
Talento humano	192.168.1.62	baja	mayor	Riesgo alto
Talento humano	192.168.1.71	muy baja	mayor	Riesgo tolerable
Almacén & dirección PQR	192.168.1.85	baja	mayor	Riesgo alto
Contabilidad	192.168.1.115	muy baja	máxima	Riesgo alto
Contabilidad	192.168.1.125	baja	máxima	Riesgo extremo
Proyectos	192.168.1.156	baja	mayor	Riesgo alto
Proyectos	192.168.1.208	baja	mayor	Riesgo alto
Proyectos	192.168.1.155	alta	menor	Riesgo tolerable
Gerencia	192.168.1.213	baja	máxima	Riesgo extremo

Fuente. Autoría propia

Hallazgos

Durante la realización de un test de intrusión utilizando la metodología Ciber Kill Chain en los activos tecnológicos de la empresa GYG INGENIERÍA S.A.S. se llevaron a cabo evaluaciones exhaustivas de los sistemas, puertos y servicios disponibles. Se observó que la gran mayoría de los activos tecnológicos, incluidos los sistemas, puertos y servicios, se encuentran actualizados y no presentan vulnerabilidades significativas que pudieran comprometer la seguridad de la red. Sin embargo, se identificó vulnerabilidades en una fotocopiadora RICOH C2000, la cual requiere atención inmediata y acciones correctivas para mitigar posibles riesgos de seguridad. Por ende, se procede a establecer el nivel de impacto en la tabla 5 dependiendo de las vulnerabilidades encontradas en la fotocopiadora RICOH C2000 con IP 192.168.1.155, ya que fue el único activo que se evidencio con brechas de seguridad. Para calcular el nivel de impacto se usó como herramienta la plataforma INCIBE, la cual ofrece dicha información.

Tabla 5. Nivel de impacto de vulnerabilidades del activo tecnológico con IP 192.168.1.155

VULNERABILIDAD	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
CVE-2019-7659	Baja	Mayor	Riesgo alto
CVE-2017-9765	Baja	Mayor	Riesgo alto
CVE-2014-3566	Media	Mayor	Riesgo alto
CVE-2012-1182	Media	Máxima	Riesgo extremo
CVE-2009-3103	Baja	Mayor	Riesgo alto

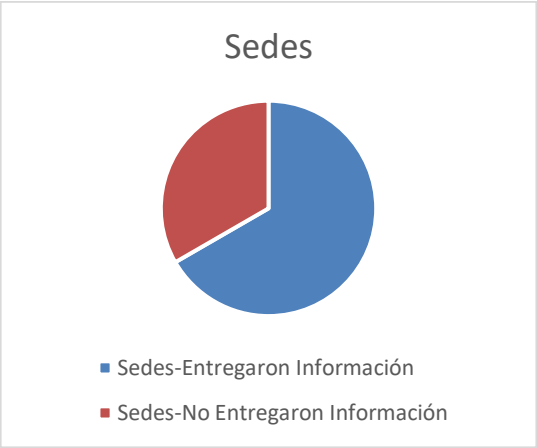
Fuente. Autoría propia.

Tras el análisis de vulnerabilidades realizado en la fotocopiadora RICOH C2000 de la empresa GYG INGENIERÍA S.A.S. se identificaron múltiples CVEs (Common Vulnerabilities and Exposures) que representan riesgos significativos para la seguridad de la red. Cuatro de estas vulnerabilidades se consideran de alto riesgo, mientras que una se considera de riesgo máximo. Es crucial abordar estas

vulnerabilidades de manera urgente para proteger los activos de la empresa contra posibles amenazas cibernéticas.

Teniendo en cuenta las pruebas de suplantación, se obtienen resultados alarmantes que se puede apreciar en la imagen 56, ya que es un factor preocupante en la empresa, que de las 12 sedes 8 entregaron información como usuario-contraseña de la plataforma de GYG y de escritorio remoto, también número de Anydesk.

Imagen 56. Sedes sometidas



Nota. Se presenta el grafico con las sedes que entregaron información.

De las 4 sedes, 2 no respondieron debido a que se encontraban ocupados con procesos administrativos y no habían revisado correo, las otras 2 reportaron a la sede principal la eventualidad, realizando la respectiva consulta si era verídico ese correo.

Test de intrusión

En este apartado se analiza los resultados de la metodología Ciber Kill Chain, como se reporta en el anterior informe, la infraestructura tecnológica debido a las actualizaciones y configuraciones de los sistemas de los diferentes dispositivos se encuentran no vulnerable, exceptuando la impresora RICOH C2000 como se

evidencia en la etapa cuatro de la metodología Ciber Kill Chain, se puede observar en las imágenes 46, 47, 48, y 49 donde se encuentra el reporte generado con las respectivas brechas dependiendo del puerto o servicio, se hallaron las siguientes vulnerabilidades:

CVE-2019-7659
Las versiones anteriores a 2.8.75 de Genivia gSOAP 2.7.x y 2.8.x posibilitan que los atacantes generen una denegación de servicio (interrupción de la aplicación) o incluso causen otro tipo de impacto no detallado si se crea una aplicación de servidor con el indicador correspondiente.

CVE-2017-9765
El desbordamiento de enteros en la función SOAP_GET en Genivia gSOAP 2.7.x y 2.8.x antes de la versión 2.8.48, que se emplea en cámaras Axis y otros dispositivos similares, posibilita que atacantes remotos lleven a cabo la ejecución de código arbitrario o causen una interrupción del servicio (mediante un desbordamiento de búfer basado en pila y la caída de la aplicación) al enviar un documento XML extenso, también conocido como Devil's Ivy.

CVE-2014-3566
El protocolo SSL 3.0, en su implementación en OpenSSL hasta la versión 1.0.1i y en otros productos similares, emplea un relleno CBC no determinista, lo que crea una vulnerabilidad que permite a los atacantes intermedios obtener datos de texto sin cifrar mediante un ataque de oráculo de relleno, conocido como "POODLE".

CVE-2012-1182
El generador de código RPC en versiones previas a 3.4.16 de Samba 3.x, versiones anteriores a 3.5.14 de 3.5.x y versiones anteriores a 3.6.4 de 3.6.x, no lleva a cabo la validación coherente de la longitud de una matriz en comparación con la asignación de memoria de dicha matriz. Esto crea una vulnerabilidad que permite a

atacantes remotos ejecutar código arbitrario mediante una llamada RPC especialmente diseñada.

CVE-2009-3103
Un error relacionado con la indexación de matrices en la implementación del protocolo SMBv2 en el archivo srv2.sys, que se encuentra en sistemas operativos como Windows Vista (versiones Gold, SP1 y SP2), Windows Server 2008 (versiones Gold y SP2) y Windows 7 RC, desarrollados por Microsoft, posibilita que atacantes remotos ejecuten código arbitrario o provoquen una interrupción del sistema (bloqueo) mediante la inserción de un carácter "&" (ampersand) en un campo denominado "Process ID High" dentro de un paquete denominado "NEGOTIATE PROTOCOL REQUEST". Este incidente desencadena un intento de acceso a una ubicación de memoria que está fuera de los límites apropiados.

6.4 PROPONER UN PLAN DE ACCIÓN EMPLEANDO ALGUNOS CONTROLES DE ISO/IEC 27002:2013, DONDE SE ESTABLECERÁN ESTRATEGIAS PARA PREVENIR ATAQUES INFORMÁTICOS, Y PROCESOS A SEGUIR CON EL FIN DE MITIGAR EL NIVEL DE IMPACTO FRENTE A LOS INCIDENTES DETECTADOS.

Plan de Acción

Fase 1: Evaluación de Riesgos

Identificación del Equipo de Trabajo: Designar un equipo responsable del proceso de inventario y protección de activos de información. Este equipo debería incluir representantes de diferentes áreas de la organización, como TI, seguridad, recursos humanos y legales.

Comunicación y Sensibilización: Comunicar a toda la organización la importancia de llevar a cabo este proceso y su contribución a la seguridad de la información.

Definición de Activos de Información: Definir una lista de categorías de activos de información, que incluya, pero no se limite a: datos, sistemas, documentos, aplicaciones, hardware y recursos humanos.

Identificación de Activos de Información: Realizar un mapeo exhaustivo de todos los activos de información en la organización, incluyendo su ubicación física y lógica, propietario, nivel de confidencialidad y valor.

Priorización de Activos Críticos: En base a la información recopilada, identificar y priorizar los activos de información críticos para la operación de la organización y su reputación.

Análisis de Riesgos: Realizar una evaluación de riesgos para identificar amenazas, vulnerabilidades y posibles impactos en los activos críticos. Además, se deberá priorizar los riesgos identificados en función de su impacto y probabilidad.

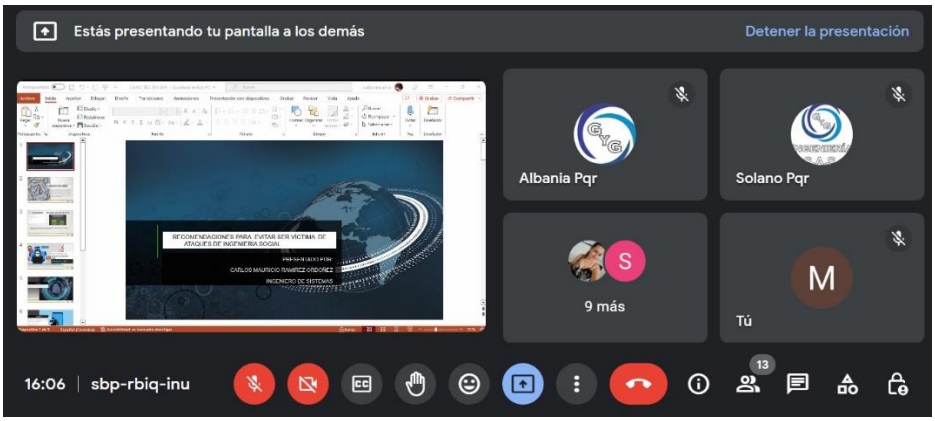
Identificación de Amenazas y Vulnerabilidades: En primer lugar, la identificación de amenazas y vulnerabilidades es fundamental para pre mitigar posibles incidentes de seguridad. Las amenazas pueden variar desde ataques cibernéticos maliciosos hasta desastres naturales que podrían afectar a los servidores locales. Las vulnerabilidades, por otro lado, pueden surgir de configuraciones incorrectas, sistemas desactualizados o prácticas de seguridad inadecuadas. Al identificar y catalogar estas amenazas, se obtiene una visión más clara de los riesgos potenciales que enfrenta la infraestructura de servidores.

Evaluación de Impacto: La evaluación de impacto permite comprender las posibles consecuencias de un incidente en los activos críticos de la empresa. Estos activos críticos pueden incluir datos confidenciales, sistemas de producción, servicios en línea y más. Al cuantificar el impacto de un incidente, se puede determinar cuán devastador sería y qué recursos se verían afectados. Esta información es crucial para la toma de decisiones informadas sobre cómo proteger estos activos en caso de un incidente.

Priorización de Riesgos: La priorización de riesgos es un paso esencial en la gestión de riesgos, ya que no todos los riesgos son iguales. Al priorizar los riesgos identificados en función de su impacto y probabilidad, la empresa puede enfocar sus recursos de manera eficiente.

Debido a que las sedes se presentaron susceptibles a ataques de ingeniería social, se llevó a cabo la respectiva capacitación con el ánimo de mitigar dicha brecha.

Imagen 57. Evidencia capacitación



Nota. Ejecución de capacitación explicando las diferentes modalidades de hacking.

De acuerdo a los resultados obtenidos en la fase 4 de la metodología Ciber kill Chain implementada en el proyecto y teniendo en cuenta el nivel de impacto, se proceden a tener en cuenta las siguientes estrategias:

Estrategias de Mitigación: Definir estrategias de mitigación para los riesgos identificados, que incluyan controles de seguridad de la información según ISO/IEC 27002.

Seguridad en la sala del servidor: Asegurar que la sala del servidor esté diseñada y equipada adecuadamente. Esto incluye sistemas de extinción de incendios, monitoreo de temperatura y humedad, sistemas de respaldo de energía (UPS) y control de inundaciones.

Protección física del servidor: Utilizar armarios o racks seguros para alojar el servidor. Además, los servidores deben estar bloqueados en su lugar y se deben utilizar sellos de seguridad para detectar cualquier manipulación no autorizada.

Respaldo de energía y suministro eléctrico ininterrumpido: Garantizar un suministro eléctrico ininterrumpido para el servidor mediante UPS y generadores de energía de respaldo, lo que ayuda a prevenir la pérdida de datos debido a apagones.

Cámaras de seguridad: Instalar cámaras de seguridad para supervisar el acceso a la sala del servidor y sus alrededores, permitiendo almacenar las grabaciones de video de acuerdo con las políticas de retención de datos.

Protección contra incendios y sistemas de extinción: Implementar sistemas de detección de incendios y extinción de incendios adecuados, como rociadores automáticos o sistemas de supresión de gases, para proteger el servidor de incendios.

Seguridad de los sistemas de almacenamiento físico: Asegurarse de que los discos duros y otros medios de almacenamiento físico estén protegidos contra robos o manipulaciones no autorizadas. Esto puede incluir la encriptación de datos en reposo.

Políticas de limpieza y desecho: Establecer procedimientos para el manejo seguro de equipos obsoletos o fuera de servicio, garantizando que los datos se borren de manera segura antes de su eliminación.

Auditoría y revisiones regulares: Realizar auditorías periódicas de los controles de seguridad física para garantizar su eficacia y cumplimiento continuo de los estándares ISO/IEC 27002.

Fase 2: Implementación de Controles

Teniendo en cuenta que la empresa no cuenta con personal de planta encargado del área de sistemas según respuesta de la entrevista por parte del ingeniero electricista Fausto franco, no se cuentan con la implementación de controles, por ende se procede a desarrollar políticas y procedimientos de seguridad de la información basados en ISO/IEC 27002 como se citan a continuación:

- Alcance de las Políticas de Seguridad de la Información.
- Política de Protección de Datos.
- Política de Seguridad Física.
- Política de Seguridad de Red.
- Política de Gestión de Incidentes.
- Política de Cumplimiento y Auditoría.

- Capacitación y Concientización.

Control de Acceso: Implementar controles de acceso adecuados, como autenticación de dos factores y gestión de contraseñas seguras.

Implementar estrictos controles de acceso físico a las instalaciones donde se encuentra el servidor. Esto incluye cerraduras, sistemas de control de acceso, tarjetas de identificación y registro de visitantes. La norma ISO/IEC 27002 recomienda establecer zonas de seguridad para limitar el acceso solo a personal autorizado.

Gestión de Vulnerabilidades: Establecer un proceso de gestión de vulnerabilidades para identificar, evaluar y remediar vulnerabilidades en sistemas y aplicaciones.

Escaneo de vulnerabilidades: Utilizar herramientas de escaneo de vulnerabilidades para identificar las debilidades en los sistemas y aplicaciones. Esto debe incluir escaneos regulares de los servidores físicos.

Clasificación de vulnerabilidades: Clasifica las vulnerabilidades identificadas según su gravedad y su impacto en los activos críticos.

Priorización de remedios: Priorizar las vulnerabilidades identificadas según su riesgo potencial que representan para los sistemas y datos.

Desarrollo de un plan de mitigación: Identificar las medidas correctivas apropiadas para cada vulnerabilidad. Esto puede incluir la aplicación de parches, actualizaciones de software, cambios en la configuración, mejoras en la infraestructura, entre otros.

Implementación de correcciones: Realizar las correcciones necesarias en los sistemas y aplicaciones afectados, siguiendo las mejores prácticas de seguridad.

Se debe de asegurar de que las actualizaciones y parches se apliquen de manera oportuna.

Concientización y Formación: Proporcionar formación y concienciación en seguridad de la información a las partes interesadas.

Evaluación de Necesidades: Realizar una evaluación de las necesidades de formación y concienciación para cada grupo de partes interesadas. Determinando

cuáles son los conocimientos necesarios para cumplir con los estándares de seguridad de la empresa.

Desarrollo de Contenido: Crear contenido de formación relevante para cada grupo de partes interesadas. Esto puede incluir presentaciones, materiales escritos, videos, tutoriales en línea y ejercicios prácticos.

Establecimiento de Objetivos de Formación: Definir objetivos de formación claros y medibles para cada grupo. Estos objetivos deben reflejar lo que se espera que los participantes aprendan en relación con la seguridad de la información.

Programación de Sesiones de Formación: Programar sesiones de formación de acuerdo con las necesidades de cada grupo de partes interesadas. Se debe asegurar que las sesiones sean accesibles y convenientes para todos.

Impartición de Formación: Impartir las sesiones de formación de manera efectiva. Se debe considerar la posibilidad de contar con expertos en seguridad de la información o instructores capacitados para garantizar la calidad de la formación.

Evaluación de la Formación: Realizar evaluaciones para medir la efectividad de la formación. Se puede utilizar cuestionarios, pruebas o ejercicios prácticos para evaluar el nivel de conocimiento adquirido.

Retroalimentación y Mejora Continua: Recopilar comentarios de los participantes y utilizar esta retroalimentación para mejorar la calidad de la formación.

Actualización Periódica: Mantener actualizados los materiales de formación para reflejar las últimas amenazas y mejores prácticas en seguridad de la información.

Cumplimiento Normativo: se debe asegurar de que la formación cumpla con los requisitos normativos y legales aplicables en materia de seguridad de la información.

Fase 3: Monitoreo y Detección

Monitoreo Continuo: Implementar sistemas de monitoreo continuo de seguridad de la información para identificar comportamientos y actividades anómalas.

Recopilación de Datos: Recopilar datos de todos los activos críticos, incluyendo el servidor físico, aplicaciones y redes. Los datos pueden incluir registros de eventos, registros de acceso, registros de aplicaciones y otros registros de seguridad.

Análisis de Comportamientos Anómalos: Implementar técnicas de análisis de comportamientos anómalos para detectar patrones inusuales o actividades sospechosas. Esto puede incluir la creación de perfiles de usuario y sistemas para identificar desviaciones de esos perfiles.

Integración de Fuentes de Datos: Asegurar que los datos de monitoreo se integren de manera efectiva desde todas las fuentes relevantes. Esto puede requerir la implementación de conectores y adaptadores para garantizar una visión completa de la seguridad.

Automatización de Respuestas: Implementar la automatización de respuestas para abordar rápidamente las actividades anómalas detectadas. Esto puede incluir la suspensión de cuentas de usuario, el bloqueo de direcciones IP o la activación de alertas para el equipo de respuesta a incidentes.

Gestión de Incidentes: Establecer un proceso de gestión de incidentes que incluya la notificación, la respuesta y la recuperación de incidentes de seguridad.

Detección del Incidente: Implementar sistemas de detección de intrusiones y monitoreo de seguridad que alerten sobre posibles incidentes.

Clasificación del Incidente: Evaluar la gravedad del incidente y clasificarlo según una escala predefinida.

Notificación: Notificar al equipo de respuesta a incidentes de seguridad (CSIRT, por sus siglas en inglés) o al personal designado responsable de la gestión de incidentes.

Evaluación y Análisis: Realizar un análisis de las causas y el alcance del incidente. Identificar la naturaleza del incidente, como un ataque cibernético, un fallo de hardware, una violación de datos, etc.

Contención: Tomar medidas inmediatas para limitar el impacto del incidente y evitar que se propague. Desconectar o aislar servidores afectados si es necesario.

Identificación de Responsabilidades: Designar un equipo de respuesta que incluya a expertos en seguridad, TI y comunicaciones.

Comunicación: Notificar a la dirección ejecutiva, las partes interesadas internas y externas, y las autoridades reguladoras, según sea necesario.

Mitigación: Implementar medidas correctivas para abordar las vulnerabilidades o debilidades que permitieron el incidente.

Restablecimiento de Servicios: Asegurar que los sistemas y servicios críticos vuelvan a funcionar normalmente.

Auditorías y Revisiones: Realizar auditorías y revisiones periódicas de la seguridad de la información para evaluar la eficacia de los controles implementados.

Fase 4: Mejora Continua

Mejora Continua: Implementar un ciclo de mejora continua basado en ISO/IEC 27001 para revisar y mejorar constantemente el sistema de gestión de seguridad de la información.

Ejecución del Plan: Llevar a cabo las acciones planificadas para abordar los objetivos de mejora. Esto puede incluir la implementación de nuevas políticas, procedimientos, tecnologías o capacitación del personal.

Monitoreo y Medición: Establecer métricas y puntos de referencia para evaluar el impacto de las mejoras implementadas. Asegurar de que los indicadores clave de rendimiento (KPI) relevantes se estén midiendo y analizando.

Evaluación de Resultados: Evaluar los resultados obtenidos con respecto a los objetivos de mejora. Compare los datos antes y después de la implementación de las mejoras para medir el impacto.

Identificación de No Conformidades: Si se identifican problemas o incumplimientos, asegúrese de documentarlos como no conformidades.

Acciones Correctivas: Tomar medidas correctivas para abordar las no conformidades y asegurar que los problemas no se repitan.

Comunicación Interna: Comunicar los resultados y el progreso a todos los empleados, asegurando de que estén al tanto de las políticas y procedimientos de seguridad de la información actualizados.

Evaluación Externa: Considerar una evaluación externa, como una auditoría de seguridad, para validar la efectividad de los controles de seguridad de la información.

Contratación de un Auditor Externo: Selección de una firma de auditoría de seguridad confiable y experimentada para llevar a cabo la auditoría. Se debe garantizar que la firma tenga experiencia en auditorías de seguridad de la información y cumpla con los estándares relevantes, como ISO 27001.

Definición del Alcance de la Auditoría: Trabajar en estrecha colaboración con el auditor para definir el alcance de la auditoría. Esto incluirá qué sistemas, aplicaciones y controles se evaluarán, así como los criterios de auditoría.

Pruebas de Penetración: En algunos casos, el auditor puede llevar a cabo pruebas de penetración para evaluar la resistencia de los sistemas y la infraestructura a posibles ataques. Esto puede incluir escaneos de vulnerabilidades, pruebas de intrusión y otros métodos de evaluación.

Identificación de Hallazgos: El auditor documentará los hallazgos, incluyendo posibles debilidades y áreas de mejora.

Informe y Comunicación

Comunicar regularmente los resultados de seguridad y las mejoras a la alta dirección y otras partes interesadas.

Este plan de acción está diseñado para abordar la seguridad de la información de manera integral, siguiendo los principios de ISO/IEC 27002:2013. Además, se recomienda contar con la participación activa de la alta dirección teniendo en cuenta el compromiso de toda la organización en la implementación y mantenimiento de las medidas de seguridad de la información.

7. RESULTADO Y DISCUSIÓN

El proyecto de evaluación de seguridad en la infraestructura tecnológica de la empresa GYG INGENIERÍA S.A.S. ha arrojado resultados significativos que proporcionan información valiosa para fortalecer la postura de seguridad de la organización. La combinación de entrevistas, instrumentos de evaluación y la aplicación de la metodología Cyber Kill Chain ha permitido un análisis exhaustivo de los sistemas de la empresa.

7.1 IDENTIFICACIÓN DETALLADA DE ACTIVOS CRÍTICOS

Durante la determinación del alcance, se llevó a cabo un proceso integral de entrevistas y encuestas, que proporcionaron una visión detallada de los activos críticos en la infraestructura. Se identificaron servidores clave, bases de datos sensibles y sistemas de gestión críticos para las operaciones de la empresa. Esta identificación precisa sienta las bases para una evaluación de seguridad enfocada.
Discusión: La identificación detallada de activos críticos es esencial para dirigir la evaluación hacia áreas específicas de riesgo. Este enfoque asegura que los recursos se utilicen de manera eficiente, centrándose en aquellos componentes que tienen un impacto significativo en la operación y la seguridad de la empresa. La inclusión de entrevistas detalladas y la incorporación de herramientas automatizadas podrían haber mejorado aún más este proceso.

7.2 APLICACIÓN EXITOSA DE LA METODOLOGÍA CYBER KILL CHAIN

La implementación de la metodología Cyber Kill Chain proporcionó una comprensión detallada de las etapas que un ciberdelincuente podría seguir para comprometer la seguridad de la infraestructura. Desde el reconocimiento hasta las acciones sobre los objetivos, cada fase fue evaluada meticulosamente utilizando herramientas especializadas como Nmap y Metasploit. La aplicación de esta metodología permitió identificar y analizar posibles vectores de ataque.
Discusión: La elección cuidadosa de herramientas y la integración de Threat Intelligence en fases tempranas fortalecieron la aplicación de la Cyber Kill Chain. Sin embargo, la inclusión de simulaciones iterativas podría haber mejorado aún más la robustez del análisis, ya que los ciberdelincuentes suelen ajustar sus tácticas en respuesta a las defensas implementadas.

7.3 ANÁLISIS DETALLADO DE RESULTADOS Y GENERACIÓN DE INFORME

El análisis detallado de los resultados obtenidos de la metodología implementada permitió la identificación y clasificación de vulnerabilidades según su nivel de

impacto. Se generó un informe exhaustivo que documenta los hallazgos, proporcionando una referencia clara y detallada de las áreas de mejora necesarias.
Discusión: El análisis meticuloso de los resultados es crucial para garantizar que las vulnerabilidades críticas no se pasen por alto. La generación de un informe detallado proporciona una base sólida para la toma de decisiones informadas y la implementación de medidas correctivas. La priorización de vulnerabilidades según la explotabilidad podría haber mejorado aún más la eficacia de este proceso.

7.4 PROPUESTA DE UN PLAN DE ACCIÓN BASADO EN ISO/IEC 27002:2013

La propuesta de un plan de acción basado en controles de ISO/IEC 27002:2013 estableció estrategias sólidas para prevenir ataques y mitigar el impacto de incidentes detectados. Se destacaron medidas como la implementación de MFA y la realización de simulacros periódicos de respuesta a incidentes.
Discusión: La elección de la norma ISO/IEC 27002:2013 proporciona un marco reconocido para la implementación de medidas de seguridad. La sugerencia de integrar MFA y conducir simulacros periódicos destaca la importancia de acciones proactivas y prácticas de seguridad continua. Se sugiere considerar la personalización del plan de acción para abordar de manera específica las vulnerabilidades identificadas en la empresa.

8. CONCLUSIONES

Durante la fase de determinación del alcance, se logró identificar de manera precisa los activos críticos en la infraestructura tecnológica de GYG INGENIERÍA S.A.S. mediante entrevistas y herramientas especializadas. La comprensión detallada de los activos críticos proporcionó una base sólida para dirigir la evaluación de seguridad hacia áreas específicas de riesgo, asegurando una evaluación más enfocada y efectiva.

La definición del alcance permitió determinar los vectores de ataque asociados a los activos críticos, brindando una visión integral de las posibles amenazas a la infraestructura. Al comprender los posibles puntos de vulnerabilidad, se estableció un marco estratégico para enfocar la evaluación y abordar los riesgos específicos que podrían afectar la seguridad de la organización.

La implementación exitosa de la metodología Cyber Kill Chain permitió analizar la infraestructura tecnológica de GYG INGENIERÍA S.A.S., esta metodología

proporcionó una comprensión detallada de cómo un ciberataque podría progresar a través de las etapas, facilitando la identificación de posibles debilidades y áreas de mejora.

La selección cuidadosa de herramientas en cada etapa de la Cyber Kill Chain garantizó una evaluación exhaustiva de la seguridad, identificando posibles brechas y vulnerabilidades. La elección adecuada de herramientas, alineada con cada fase del modelo, demostró ser esencial para obtener resultados precisos, destacando la importancia de la planificación y estrategia.

El análisis detenido de los resultados obtenidos permitió identificar una lista de vulnerabilidades clasificadas según su nivel de impacto. Este enfoque meticuloso proporcionó una visión detallada de las amenazas más críticas, permitiendo una priorización efectiva de las acciones correctivas.

La generación de un informe detallado consolidó los hallazgos de la evaluación de seguridad, proporcionando una base sólida para futuras mejoras. Un informe claro y completo no solo documenta los problemas encontrados, sino que también ofrece una guía valiosa para implementar soluciones y fortalecer la postura de seguridad.

La propuesta de un plan de acción basado en controles de ISO/IEC 27002:2013 estableció estrategias sólidas para prevenir ataques y mitigar el impacto de incidentes detectados. La alineación con estándares reconocidos proporcionó un marco robusto para la implementación de medidas de seguridad, garantizando una respuesta coherente y eficiente.

La capacitación del personal sobre modalidades de ataque, especialmente en el ámbito de la ingeniería social, fortaleció la conciencia de seguridad y redujo las posibilidades de caer en tácticas engañosas. La inversión en la formación del personal se reveló crucial para mantener una primera línea de defensa contra amenazas, subrayando la importancia de la educación continua en ciberseguridad.

9. RECOMENDACIONES

Durante la determinación del alcance, se sugiere ampliar la fase de entrevistas, asegurándose de incluir a todas las partes interesadas y realizar entrevistas más detalladas para capturar información exhaustiva sobre los activos críticos y sus interconexiones.

Para complementar la identificación de activos críticos, se recomienda incorporar herramientas de descubrimiento automático. Esto agilizará el proceso y garantizará una recopilación completa de información sobre la infraestructura.

Para mejorar la aplicación de la metodología Cyber Kill Chain, se sugiere incorporar fuentes de Threat Intelligence desde el principio. Esto permitirá una identificación más precisa de amenazas potenciales y ajustará las tácticas en consecuencia.

Después de la primera implementación de la metodología, se recomienda realizar simulaciones adicionales. Esto proporcionará una comprensión más profunda de las posibles variantes de ataques y asegurará una cobertura exhaustiva de posibles escenarios.

En el análisis de resultados, se sugiere establecer un enfoque de evaluación continua en lugar de puntuales. Esto garantizará la detección temprana de nuevas vulnerabilidades que puedan surgir con el tiempo.

Al analizar las vulnerabilidades, se recomienda refinar los criterios de priorización, considerando no solo el impacto potencial, sino también la facilidad de explotación. Esto permitirá abordar primero las vulnerabilidades más críticas y explotables.

En la propuesta del plan de acción, se sugiere implementar la autenticación multifactor en todos los sistemas críticos. Esto añadirá una capa adicional de seguridad y reducirá significativamente el riesgo de acceso no autorizado.

Para mejorar la preparación ante incidentes, se recomienda incluir simulacros de respuesta a incidentes en el plan de acción. Esto permitirá al personal practicar procedimientos de manejo de crisis y fortalecerá la capacidad de reacción en situaciones reales.

10. BIBLIOGRAFÍA

ALTUBE. Rafael. Wireshark. [En línea]. 2021. [Consultado el 01 de octubre de 2022] Disponible en: https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/

BODNAR. Danielle. Ingeniería social. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en: https://www.avast.com/es-es/c-social-engineering#:~:text=En%20cualquier%20cadena%20de%20seguridad,conseguir%20que%20divulguen%20informaci%C3%B3n%20privada.

Ciberseguridad. Ciber kill chain, 2022. [consultado el 23 de septiembre de 2022]. Disponible en: https://ciberseguridad.com/guias/cyber-kill-chain/

Cisco. Cortafuegos. [Sitio Web]. 2022. [Consultado el 01 de octubre de 2022] Disponible en: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Dragonjar. Pentest. [Sitio Web]. [Consultado el 02 de octubre de 2022] Disponible en: https://www.dragonjar.org/como-realizar-un-pentest.xhtml

Elempleo. ¿Cómo combatir los ciberataques en empresas colombianas? [Sitio Web]. 2022. [Consultado el 29 de Octubre de 2022]. Disponible en https://www.elempleo.com/co/noticias/mundo-empresarial/como-combatir-los-ciberataques-en-companias-colombianas-6925

Global Technology. Consecuencias de un ciberataque. [Sitio web]. [Consultado el 31 de septiembre de 2022]. Disponible en: https://globalt4e.com/consecuencias-de-un-ciberataque/

Hornetsecurity. Ciber kill Chain. [Sitio Web]. 2021. [consultado el 25 de septiembre de 2022]. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/cyber-kill-chain/?_adin=02021864894

Impacto TIC. Mas de la mitad de las empresas colombianas sufrió ataques en este ultimo año, [En linea]. 2022. Consultado el 29 de Octubre de 2022]. Disponible en: https://impactotic.co/mas-de-la-mitad-de-las-empresas-colombianas-sufrio-ataques-el-ultimo-ano/

InterLan. Las empresas colombianas invierten menos del 5% en ciberseguridad. [Sitio web]. [Consultado el 29 de octubre de 2022]. Disponible en: https://www.interlan.com.co/2019/08/28/las-empresas-colombianas-invierten-menos-del-5-en-ciberseguridad/

Itera. ¿qué es una prueba de penetración? [sitio web]. (). [Consultado el 09 de diciembre de 2022]. Disponible en https://iteraprocess.com/2021/04/05/para-que-sirven-las-pruebas-de-penetracion/#:~:text=Las%20pruebas%20de%20penetraci%C3%B3n%20adem%C3%A1s,que%20genera%20en%20la%20organizaci%C3%B3n.

Kali. Kali Linux, S.F. [Consultado el 01 de octubre de 2022] Disponible en: https://www.kali.org/

Kaspersky. Ingeniería social: definición. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

KOROLOV MIYERS. María. Ciber kill chain un modelo de rastreo de ciberataques, 2022. [consultado el 26 de septiembre de 2022]. Disponible en:https://cso.computerworld.es/tendencias/que-es-la-cyber-kill-chain-un-modelo-de-rastreo-de-ciberataques

Nmap. Guia de referencia Nmap, 2020. [Consultado el 01 de octubre de 2022] Disponible en: https://nmap.org/man/es/index.html

Portafolio. El 73% de las empresas en el mundo han sufrido de ciberataques. [Sitio web] [Consultado el 31 de septiembre de 2022]. Disponible en: https://www.portafolio.co/economia/finanzas/ciberseguridad-el-73-de-las-empresas-en-el-mundo-ha-sufrido-ciberataques-570387

PRENAFETA. Javier. Pentesting. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/#:~:text=El%20%E2%80%9Cpentesting%E2%80%9D%20o%20%E2%80%9Ctest,pueden%20afectar%20a%20su%20sistema.

PSTYGA. Nicolas. Ciberseguridad: todos podemos ser víctimas. [Sitio web]. [Consultado el 02 de octubre de 2022] Disponible en:

https://iqlatino.org/ciberseguridad-todos-podemos-ser-victimas/?gclid=CjwKCAjw7eSZBhB8EiwA60kCW0OT9qvwbuhUdvf6qV3COhPJLu-h87H6SHNIAvo2fD4Msk1prXw_4xoCzhkQAvD_BwE

QUILQUE SALTOS. Brian. & CAMPOVERDE ANDRADE, Cinthya. Diseño e implementación de un framework para la evaluación periódica de la seguridad usando pruebas de penetración en la red interna de la Universidad de Cuenca. [en línea]. 2021. [consultado el 10 de diciembre de 2022]. Disponible en https://dspace.ucuenca.edu.ec/bitstream/123456789/37143/1/Trabajo%20de%20Titulaci%C3%B3n.pdf

Significados. Tipos de investigación. [Sitio web]. [Consultado el 14 de noviembre de 2022]. Disponible en: https://www.significados.com/tipos-de-investigacion/#:~:text=Investigaci%C3%B3n%20aplicada,la%20ingenier%C3%ADa%20o%20la%20medicina.

Universdiad Veravruzana. Noti_infosegura: ¿Debemos estar preparados para un ataque cibernético de grandes dimensiones? Un experto de seguridad nos responde, 2017. [consultado el 23 de septiembre de 2022]. Disponible en: https://www.uv.mx/infosegura/general/noti_ciberataques-16/

VANEGAS ROMERO. Alfonso. Pentesting ¿por kue es tan importante para las empresas?. [en línea]. 2021. [Consultado el 10 de diciembre de 2022]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1

VERA, Rafael. OpenVas. [Sitio web]. [Consultado el 01 de octubre de 2022] Disponible en: https://openwebinars.net/blog/que-es-openvas/

11. ANEXOS

Link video: https://www.youtube.com/watch?v=rHRww8tfPEo