PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

ANÁLISIS DE VULNERABILIDADES Y GUÍA PARA LA IMPLEMENTACIÓN DE LA ISO/IEC 27001. CASO DE ESTUDIO: NILOTEX.

AUTOR: YONFÁ CÉLLERI JOSÉ ALBERTO

DIRECTOR: MSC.OSWALDO ESPINOSA

QUITO, JULIO 2020

Dedicatoria

A Dios por la salud que me regala cada día, por la sabiduría e inteligencia que me brinda en cada paso y decisión que tomo.

A mis padres Paulina Célleri y Alberto Yonfá por el constate apoyo, dedicación, sacrificio y entrega hacia mí, por siempre buscar lo mejor para mí, por ser mi motor y mi inspiración en cada paso que doy a lo largo de mi vida. A mi hermana Doménica por ser quien ha estado siempre para mí, por ser mi apoyo, quien está pendiente de mí.

A mis abuelitos, tíos y primos quienes han sido pilar fundamental en mi formación tanto académica como en valores y han sido mi sostén a lo largo de la vida. En especial a la memoria de Subt. Piloto de Aviación José Luis Yonfa Guerrero por que en vida fue, es y siempre será un ejemplo de lucha y entrega.

A cada uno de mis amigos por el apoyo, consejos, risas que han hecho esta travesía universitaria pueda llegar a su fin. He conocido a personas que se han vuelto muy importantes en mi vida y a quienes le quedare internamente agradecido por todo su apoyo.

El camino para llegar a este punto no ha sido fácil, existieron altibajos, pero si no fuera por cada una de estas personas y de muchas más que estuvieron siempre para mí que hicieron esto posible.

Agradecimiento

Agradezco infinitamente cada docente de la facultad de Ingeniería de la Pontificia Universidad Católica del Ecuador por ser quienes impartieron sus conocimientos y me permitieron aprender no solo la teoría sino la experiencia en varios ámbitos que sin duda aporto de gran manera en mi desarrollo académico.

A la Pontificia Universidad Católica del Ecuador, por ser la mejor institución de estudios superiores en el país, la cual forma grandes profesionales y a quien me permitió representarla con todo el orgullo en la selección de futbol.

Agradezco a Dios por la familia que me dio, mis padres, hermana, tíos primos, abuelos y amigos que con su constante preocupación hicieron de mi persona un mejor ser humano y sin duda un mejor profesional. Sin más agradecer a todas las personas que forman parte de mi vida y se han convertido en pilares fundamentales en mi desarrollo.

Tabla de contenido

Tabla de Ilustraciones

1. Capítulo 1 – Introducción

1.1. Herramientas

1.1.1. Serie ISO/IEC 27000

Para entender de qué habla la normativa ISO/IEC 27000, primero debemos tener claro los conceptos y de que tratan las ISO e IEC.

1.1.1.1. ISO

ISO por sus siglas en inglés (International Organization for Standardization) o en español la Organización Internacional para la Estandarización, es una organización no gubernamental independiente compuesta por un total de 164 países en el mundo, de los cuales 121 cuentan con asociaciones nacionales de normalización, responsable de la creación, regularización y control de estándares internacionales para la industria en todos los procesos, productos y servicios que estas prestan a la población. (ISO, s.f.)

Antes de la creación de la organización ISO, existía otra organización llamada ISA (International Federation of the National Standardizing Associations), fue creada en 1926 y fundada en New York en 1928, sus actividades principalmente estaban enfocadas hacia Europa, ya que se basaba en el sistema métrico. (q-bo, 2018)

Esta organización estaba encargada de aquellas áreas que no formaban parte del área electromagnética, que estaba encargada la ICE (Internacional Electrotechnical Commission). Con el inicio de la Segunda Guerra Mundial la ISA seso sus funciones al ser la comunicación a nivel internación nula, hasta que se reestableció.

Londres, 1944 nace la UNSCC (United Nations Standards Coordinating Committee) o conocido como Comité de Coordinación de Estándares de las Naciones Unidas, que funcionaba en las mismas oficinas de la ICE, para el año de 1945 en la ciudad de New York se realizó una reunión con los delegados de diversos países que formaban parte de la UNSCC, en la cual tomaron temas relacionados a la estandarización a nivel internacional y tuvieron acercamientos con la ISA. (ISOTools, 2015)

Para el año de 1946 en Paris la ISA y la UNSCCS se reunieron con delegados de 25 países en el Instituto de Ingenieros Civiles en Londres, en el cual acordaron la creación de una nueva organización internacional, que sea la encargada de facilitar la estandarización en los países (ISOTools, 2013). Al término de esta reunión la ISA se disolvió por dos razones, la primera fue acierta irregularidades y la segunda por la inactivada que esta organización tuvo durante la Segunda Guerra Mundial. Mientras que los delegados de

la UNSCC fueron informados que cesaran sus actividades para el beneficio de la nueva organización (ISOTools, 2015). La ISO comienza oficialmente sus funciones un 23 de febrero de 1947, en Ginebra, Suiza donde tienen sus oficinas centrales. Desde su inauguración se han publicado más de 22950 estándares internacionales. (Blog Calidad ISO, 2014)

1.1.1.2. IEC

ICE por sus siglas en inglés (International Electrotechnical Commission), es una organización sin fines de lucro, casi gubernamental de normalización de estándares internacionales para las áreas de la electrónica, eléctrica y tecnologías relacionadas. (IEC, 2020) Compuesta hasta la fecha por 88 miembros que representan a los países participantes de las decisiones que se toman para la implementación de las normas, de los cuales 62 son miembros plenos y 26 son miembros asociados. (IEC, 2020)

La ICE nace en el año de 1906 EN London, UK del resultado del Congreso Eléctrico Internacional llevado a cabo en la ciudad de St. Luis (Misuri), USA en el año de 1904, donde vieron la necesidad de formar una comisión mundial para controlar y crear normas para el sector eléctrico, electrónico y las tecnologías relacionadas con los mismo. (GUILENIA S.A, s.f.)

La IEC forma parte de las tres organizaciones mundiales encargadas de desarrollar estándares internacionales, las otras dos son la ISO (International Organization for Standardization) y la ITU (Unidad Internacional de Telecomunicaciones) (admin, 2012)

La IEC enfoca la mayor atención a la existencia de un lenguaje técnico universal, teniendo en cuenta definiciones, símbolos eléctricos y electrónicos o unidades de medición, rengos normalizados, requisitos y métodos de prueba, entre otros aspectos en dichas áreas. (GUILENIA S.A, s.f.)

1.1.1.3. Serie 27000

Una vez que conocemos que es y que hace la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission), podemos adéntranos en la ISO/IEC 27000.

La ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo para la gestión de la seguridad de la información para cualquier tipo de empresa. (ISO, s.f.)

Desde 1901 la BSI (British Standards Institution) fue la primera organización de normalización a nivel mundial, fue la encargada de la publicación de importantes normas como BS 5750, publicada en 1979, que dio origen a la ISO 9001. La norma BS 7799 surgió en 1995 por primera vez con el objetivo de brindar

a las empresas británicas o no buenas prácticas para la gestión de la seguridad de la información. (ISO 27000.es, s.f.)

Esta norma fue dividida en dos partes, la primera parte (BS 7799-1) es una guía de buenas prácticas y la segunda parte (BS 7799-2) publicado en 1998 establece los requisitos de un sistema de seguridad de la información (SGSI). (Disterer, ISO/IEC 27000, 27001 and 27002 for Information Security Management, 2013)

En el año de 1999 la norma BS 7799 fue revisada. La primera parte de esta norma fue aceptada sin ningún cambio por la ISO, se la adopto como la ISO 17799 en el año 2000. Mientras que la parte dos fue revisada en el año 2002 para adecuarse a las normas ISO. En el año 2005 la ISO publico el estándar ISO 27001, al mismo tiempo se revisó y actualizo la ISO 17799, que fue renombrada como la ISO 27002:2005. (ISO 27000.es, s.f.)

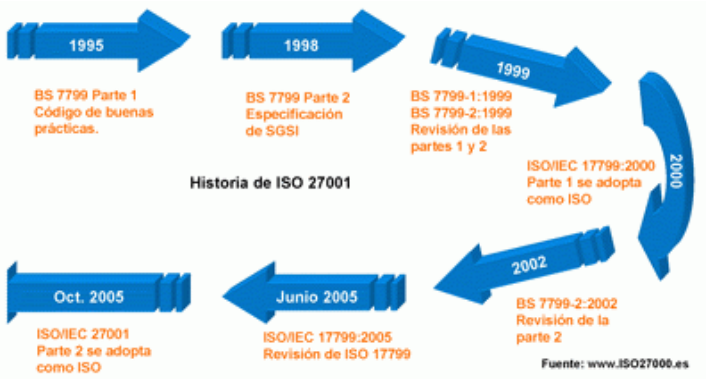

Ilustración 1. Historia de la ISO 27001 (ISO 27000.es, s.f.)

1.1.1.3.1. ISO/IEC 27000

La norma ISO/IEC 27000 contiene un vocabulario usado para todas las demás normas, además proporciona una visión general de la serie 27000, indicando el alcance de actuación y el propósito por el cual fueron publicadas. Da una introducción a los SGSI (Sistema de Gestión de Seguridad de la Información). (ISO27000.ES, 2005)

Fue publicada por primera vez en mayo del 2009, en la actualidad cuenta con cinco versiones, la última en febrero del 2018. (ISO27K information segurity, 2020) (ISO, s.f.)

1.1.1.3.2. ISO/IEC 27001

La norma ISO/IEC 27001 publicada por primera vez en octubre del 2005, tiene su origen en la norma BS 7799-2:2002 que quedó anulada. La última edición de esta norma se publicó en el año 2013, para el año 2015 se adjuntó un documento con modificaciones en cuanto a la declaración de aplicabilidad. (ISO27000.ES, 2005)

Esta norma habla de los requisitos necesarios para el desarrollo y operación de un SGSI (Sistema de Gestión de Seguridad de la Información), incluyendo un grupo de control para el control y mitigación de riesgos asociados a los SGSI. En el anexo A de esta norma se puede encontrar en forma de resumen enumerados los objetivos de control y controles que se desarrollan en la ISO/IEC 27002. (Disterer, Journal of Information Security, 2013)

1.1.1.3.3. ISO/IEC 27002

La norma ISO/IEC 27002 proporciona una guía de buenas prácticas para la implementación de controles de seguridad de la información, publicada en julio del 2005, contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. La última edición de esta norma fue actualizada en el 2013, contiene 14 dominios, 35 objetivos de control y 114 controles. (ISO27000.ES, 2005) (ISO, s.f.) (IsecT, s.f.)

1.1.1.3.4. ISO/IEC 27003

La norma ISO/IEC 27003 fue publicada por primera vez en febrero del 2010 y su última versión es la de abril del 2017. Esta norma da una guía para los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo con la norma ISO/IEC 27001. Describe el proceso de especificación y diseño desde el inicio hasta la implementación. (ISO, s.f.) (Isect, s.f.)

El origen de esta norma se da del anexo B de la norma BS 7799-2. (ISO27000.ES, 2005)

1.1.1.3.5. ISO/IEC 27004

La norma ISO/IEC 27004 fue publicada por primera vez en diciembre del 2009 y revisada en diciembre del 2016. Esta norma da una pauta para el desarrollo y la utilización de métricas y de técnicas de medición para determinar la eficacia y eficiencia de un SGSI. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.6. ISO/IEC 27005

La norma ISO/IEC 27005 da una guía de recomendaciones sobre cómo llevar la gestión de riesgos de la seguridad de la información.

En junio del 2008 fue la primera publicación de esta norma para julio del 2018 se actualizo la norma con respecto a los requisitos de la norma ISO/IEC 27001, esta es la tercera edición. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.7. ISO/IEC 27006

La norma ISO/IEC 27006 habla sobre un conjunto de requisitos de acreditación que las empresas certificadoras necesitan al momento de auditar un SGSI. (ISO, s.f.) (Isect, s.f.)

Su tercera versión es de septiembre del 2015, la primera edición es de marzo del 2007. (ISO27000.ES, 2005)

1.1.1.3.8. ISO/IEC 27007

La norma ISO/IEC 27007 fue publicada en noviembre 2011, revisada en octubre del 2017, existe una tercera versión de enero del 2020. (ISO27000.ES, 2005)

Esta norma es una guía para auditar los SGSIs. Nos indica qué auditar cuando, como establecer a los auditores, la planificación y ejecución de la auditoria, es un complemento a lo explicado en la norma ISO 19011. (ISO, s.f.) (Isect, s.f.)

1.1.1.3.9. ISO/IEC 27008

La norma ISO/IEC 27008 brinda una orientación acerca de la revisión de la implementación y operación de los controles. Fue publicada en octubre del 2011. (ISO27000.ES, 2005) (ISO, s.f.)

1.1.1.3.10. ISO/IEC 27009

La norma ISO/IEC 27009 fue publicada en junio del 2016, habla sobre los requerimientos necesarios para el uso de la norma ISO/IEC 27001 en cualquier sector. (ISO27000.ES, 2005) (ISO, s.f.)

1.1.1.3.11. ISO/IEC 27010

La norma ISO/IEC 27010 fue publicada por primera vez en el año 2012 y revisada para el año 2015. Esta norma da una orientación acerca del intercambio de información sobre riesgos de información, controles de seguridad e incidentes que suceden en las empresas, en otras palabras, da una guía del funcionamiento interno de la organización, seguridad y comunicación entre mismos sectores. (ISO, s.f.) (ISO27000.ES, 2005) (Isect, s.f.)

1.1.1.3.12. ISO/IEC 27011

La norma ISO/IEC 27011 publicada en diciembre del 2018 y revisada en diciembre del 2016. Esta norma da pautas para apoyar en la implementación de controles de seguridad de la información en organizaciones relacionadas con telecomunicaciones. (ISO27000.ES, 2005) (Isect, s.f.) (ISO, s.f.)

1.1.1.3.13. ISO/IEC 27013

La norma ISO/IEC 27013 publicada por en octubre del 2012 y actualizada en noviembre del 2015. Esta norma da una guía para la implementación integrada de un sistema de gestión de seguridad según la ISO/IEC 27001 y un sistema de gestión de servicios según la ISO/IEC 20000-1. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.14. ISO/IEC 27014

La norma ISO/IEC 27014 publica en abril del 2013. Esta norma facilita una guía acerca de los conceptos y principios para el gobierno de la seguridad de la información. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.15. ISO/IEC TR 27015

La norma ISO/IEC TR 27015 publicada en el año 2012. La norma brinda una guía de SGSI destinada a organizaciones que brindan servicios financieros y de seguros, como complemento de la ISO/IEC 27002. Esta norma se encuentra en estado retirado, desde julio del 2017 la ISO anunció que dicha norma no será actualizada con relación a la ISO/IEC 27002. (ISO27000.ES, 2005) (ISO, s.f.)

1.1.1.3.16. ISO/IEC TR 27016

Esta norma fue publicada en febrero del 2014, es una guía de valoración de como las organizaciones pueden tomar decisiones para proteger la información y el impacto económico de dichas decisiones. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.17. ISO/IEC 27017

Publicada en diciembre del 2015. Esta norma da pautas para los controles de seguridad de la información para la computación en la nube. (ISO27000.ES, 2005) (ISO, s.f.)

1.1.1.3.18. ISO/IEC 27018

La norma ISO/IEC 27018 fue publicada en julio del 2014 y su segunda versión fue lanzada en enero del 2019. Es norma brinda objetivos de control y guías para la implementación de medidas de protección para la información de identificación para aquellos proveedores de servicios de computación en la nube. (ISO27000.ES, 2005) (Isect, s.f.) (ISO, s.f.)

1.1.1.3.19. ISO/IEC TR 27019

Publicada en julio del 2013 y actualizada en octubre del 2017. Esta norma brinda una pauta que se basa en la ISO/IEC 27002 para los sistemas de control de procesos utilizados en la industria de los servicios de energía. (ISO27000.ES, 2005) (Isect, s.f.) (ISO, s.f.)

1.1.1.3.20. ISO/IEC 27021

La norma ISO/IEC 27021 fue publicada en octubre del 2017. Esta norma explica los requisitos de competencia para los profesionales que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del SGSI. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.21. ISO/IEC CD 27022

Esta norma se encuentra en desarrollo, será publicada en el año 2022, titulada como Tecnología de la información – Técnicas de seguridad – Orientación sobre procesos del SGSI. (ISO27000.ES, 2005) (ISO, s.f.)

1.1.1.3.22. ISO/IEC TR 27023

Publicada en julio del 2015. Esta norma es una guía de correspondencia entre las versiones del 2013 de la ISO/IEC 27001 y la ISO/IEC 27002 y la versión publicada en el año 2005, ayuda a la migración de la versión 2005 a la 2013 de estas dos normas. (ISO27000.ES, 2005) (ISO, s.f.)

1.1.1.3.23. ISO/IEC CD 27030

Esta norma se encuentra en desarrollo, será publicada en el año 2022, titulada como Tecnología de la información – Técnicas de seguridad – Directrices para la seguridad y la privacidad en Internet de las cosas (IoT). (ISO27000.ES, 2005) (Isect, s.f.)

1.1.1.3.24. ISO/IEC 27031

Publicada en marzo 2011. Esta norma describe los conceptos y principios de la tecnología de información y comunicación para la continuidad del negocio, facilita métodos y procesos para poder identificar los aspectos para mejorar la preparación de una organización en temas de TIC. (ISO27000.ES, 2005) (ISO, s.f.)

1.1.1.3.25. ISO/IEC 27032

Publicada en julio del 2012. La norma proporciona una orientación para mejorar el estado de la ciberseguridad en temas de protección de la privacidad de las personas en la red, abarca también seguridad de información, seguridad de red, seguridad de internet y protección de infraestructura de información crítica. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.26. ISO/IEC 27033

Publicada en el año 2015, esta norma consta de 6 partes, la cuales topan temas relacionados a la seguridad de la red. La primera parte facilita una visión general de la seguridad de la red y definiciones relacionadas, la segunda habla de las directrices para el diseño e implementación de la seguridad de red, la tercera habla de los escenarios de redes de referencia: amenazas, técnicas de diseño y problemas de control, la cuarta parte esta titulada como asegurando las comunicaciones entre redes usando pasarelas de seguridad, mientras que la quita parte esta titulada como asegurando las comunicaciones a través de redes usando Redes Privadas Virtuales (VPN), la sexta y última parte se denomina asegurando el acceso a la red IP inalámbrica. (ISO27000.ES, 2005) (ISO, s.f.) (Isect, s.f.)

1.1.1.3.27. ISO/IEC 27034

Publicada en 2011 da una orientación a las organizaciones para integrar la seguridad en los procesos que estas utilizan para administrar sus aplicaciones. (ISO27000.ES, 2005)

1.1.1.3.28. ISO/IEC 27035

Esta norma fue publicada en 2016, es una norma multiparte, consta de conceptos básicos y fases para la gestión de incidentes de seguridad de la información en cualquier tipo de organización. (ISO27000.ES, 2005)

1.1.1.3.29. ISO/IEC 27036

Norma publicada en el año 2014, consta de cuatro partes que hablan del aseguramiento de la información y sistemas de información dentro del área de las relaciones con los proveedores. (ISO27000.ES, 2005)

1.1.1.3.30. ISO/IEC 27037

Publicada en el año 2012 en el mes de octubre. Esta norma brinda directrices para las actividades de manejo de evidencia digital como es identificación, recopilación, consolidación y prevención de evidencia digital que puede ser de valor probatorio. (ISO27000.ES, 2005)

1.1.1.3.31. ISO/IEC 27038

Publicada en marzo del 2013. Esta norma habla de las técnicas para realizar redacción digital en documentos digitales. Es una guía de especificaciones para la seguridad en la redacción digital. (ISO27000.ES, 2005)

1.1.1.3.32. ISO/IEC 27039

Publicada en febrero del 2015 y corregida en abril del 2016. Esta norma brinda pautas a las organizaciones para la implementación de sistemas de detección y prevención de intrusiones. (ISO27000.ES, 2005)

1.1.1.3.33. ISO/IEC 27040

Publicada en enero en el 2015. Esta norma da una orientación técnica detallada para la seguridad de almacenamiento de datos. (ISO27000.ES, 2005)

1.1.1.3.34. ISO/IEC 27041

Publicada en junio del 2015. Esta norma de pauta acerca de los mecanismos de los métodos y procesos que se utilizan en la investigación de incidentes de seguridad de la información. (ISO27000.ES, 2005)

1.1.1.3.35. ISO/IEC 27042

Esta norma fue publicada en junio de 2015. Esta norma brinda una guía acerca del análisis e interpretación de evidencia digital, abarca las mejores prácticas para selección, diseño e implementación. (ISO27000.ES, 2005)

1.1.1.3.36. ISO/IEC 27043

Publicada en marzo del 2015. Esta norma habla de principios y procesos de investigación de incidentes en los que se ven involucrados evidencia digital, esto va desde la preparación previa hasta el cierre de la investigación. (ISO27000.ES, 2005)

1.1.1.3.37. ISO/IEC 27045

Esta norma se encuentra en desarrollo y va a topar temas relacionados a los procesos de seguridad y privacidad den sistemas de Big Data. (ISO27000.ES, 2005)

1.1.1.3.38. ISO/IEC 27050

La norma ISO/IEC 27050 habla de la información almacenada en dispositivos electrónicos con relación a la identificación, preservación, recolección, procesamiento, revisión, análisis y producción. Está elaborada en 3 partes la norma ISO/IEC 27050-1 publicada en noviembre del 2016 y actualizada en el año 2019 hace referencia a conceptos generales, la norma ISO/IEC 27050-2 da una orientación para el gobierno y gestión del descubrimiento electrónico, esta norma fue publicada en octubre 2018 y finalmente la norma IOS/IEC 27050-3 habla de un código de buenas prácticas que brinda requisitos y recomendaciones acerca de las actividades del descubrimiento electrónico, publicada en el año 2017 y actualizada en el año 2020. (ISO27000.ES, 2005)

1.1.1.3.39. ISO/IEC CD 27070

Esta norma se encuentra en fase de desarrollo y trata de los requisitos de seguridad para las raíces virtualizadas de confianza en la nube. (ISO27000.ES, 2005)

1.1.1.3.40. ISO/IEC 27071

Se encuentra en fase de desarrollo, esta norma dará recomendaciones de control de seguridad para establecer conexiones confiables entre los dispositivos y los servicios brindados en la nube. (ISO27000.ES, 2005)

1.1.1.3.41. ISO/IEC 27099

Esta norma se encuentra en fase de desarrollo, indicara los requisitos de gestión de seguridad de la información para los proveedores de servicios de infraestructura de clave pública, PKI (Public Key Infrastructure). (ISO27000.ES, 2005)

1.1.1.3.42. ISO/IEC 27100

Esta norma se encuentra en fase de desarrollo, esta norma tratará sobre la ciberseguridad dando una descripción general y conceptos asociados. (ISO27000.ES, 2005)

1.1.1.3.43. ISO/IEC TS 27101

Se encuentra en fase de desarrollo, esta norma brindará directrices para el desarrollo de marcos de ciberseguridad. (ISO27000.ES, 2005)

1.1.1.3.44. ISO/IEC 27102

Publicada en agosto del 2019. Esta norma da pautas para la compra de un ciberseguro como una opción para el tratamiento de riesgos para gestionar el impacto de un ciberaccidente. (ISO27000.ES, 2005)

1.1.1.3.45. ISO/IEC TR 27103

Publicada en febrero del 2018, la norma habla de cómo sacar el mayor beneficio a los estándares existentes en un marco de ciberseguridad. (ISO27000.ES, 2005)

1.1.1.3.46. ISO/IEC TR 27550

Publicada en septiembre del 2019. Esta norma habla de ingeniería de privacidad en los procesos del ciclo de vida del sistema, busca satisfacer los requisitos de privacidad relacionados con la protección de datos personales. (ISO27000.ES, 2005)

1.1.1.3.47. ISO/IEC 27551

Se encuentra en fase de desarrollo. Esta norma hablará de los requisitos para la autenticación de entidad no vinculable basada en atributos. (ISO27000.ES, 2005)

1.1.1.3.48. ISO/IEC WD 27553

Se encuentra en fase de desarrollo. La norma especificara los requisitos para la autenticación biométrica en los dispositivos móviles. (ISO27000.ES, 2005)

1.1.1.3.49. ISO/IEC AWI 27554

Esta norma se encuentra en fase de desarrollo. Da pautas sobre el uso de la ISO 3100 para la evaluación de riesgos relacionados con la gestión de identidad. (ISO27000.ES, 2005)

1.1.1.3.50. ISO/IEC 27555

Esta norma se encuentra en fase de desarrollo, la norma dará una orientación acerca de la eliminación de datos personales, PII (Personally Identifiable Information). (ISO27000.ES, 2005)

1.1.1.3.51. ISO/IEC AWI 27556

Se encuentra en fase de desarrollo. Dará un marco centrado en el usuario para el manejo de información de identificación personal (PII) basada en preferencia de privacidad. (ISO27000.ES, 2005)

1.1.1.3.52. ISO/IEC PDTS 27570

Se encuentra en fase de desarrollo. Esta norma habla de las ciudades inteligentes y de las pautas de privacidad que deben tener. (ISO27000.ES, 2005)

1.1.1.3.53. ISO/IEC 27701

Publicada en agosto del 2019. Esta norma específica los requisitos y da una orientación para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de privacidad (PIMS). (ISO27000.ES, 2005)

1.1.1.3.54. ISO 27799

Publicada por primera vez en junio del 2008 y actualizada en julio del 2016. Esta norma brinda una orientación para la interpretación e implementación de la ISO/IEC 27002 en temas de informática de la salud. (ISO27000.ES, 2005)

1.1.2. Kali Linux

1.1.2.1. ¿Qué es?

Kali Linux es una distribución de Linux basada en Debían, usada para pruebas avanzadas de penetración y auditoria de seguridad.

Kali Linux es desarrollado, financiado y mantenido por Offensive Security. Fue lanzado el 13 de marzo del 2013 como sucesor del BlackTrack Linux, es un proyecto de código abierto. (OffSec Services Limited, s.f.).

Al ser una distribución de Debian la instalación de paquetes y configuración es análoga, la documentación de Debian se puede utilizar para esta distribución. (Orcero, 2018)

1.1.2.2. Categorías de Herramientas

Kali Linux cuenta con más de 600 herramientas para poder cumplir todas las funciones para las que están desarrolladas como auditoria de seguridad, escaneo de puertos, suites de crackeo Wifi, programas para descubrir claves, etc.

Las categorías con las que cuenta Kali Linux son:

- Recopilación de Información.
- Análisis de Vulnerabilidad.
- Herramientas de exportación.
- Ataques Inalámbricos
- Herramientas forenses
- Aplicaciones Web
- Pruebas de Estrés
- Sniffing y Spoofing
- Ataques de contraseña
- Mantener el acceso
- Piratería de hardware
- Ingeniería inversa
- Herramientas de informes

(KaliTools, s.f.)

1.1.3. BlackArch Linux

1.1.3.1. ¿Qué es?

BlackArch Linux es una distribución de pruebas de penetración basada en Arch Linux. Contiene alrededor de 2468 herramientas y siguen en aumento. (BlackArch Linux, 2020)

Esta distribución es compatible con instalaciones existentes de ArchLinux o basadas en la misma. Está enfocada hacia usuarios con un grado de experiencia mayor en GNU/Linux

1.1.3.2. Categorías de Herramientas

BlackArch Linux actualmente cuenta con 2468 herramientas para realizar los test de penetración.

Las categorías de estas herramientas son

- Blackarch-webapp
- Escaner negro
- Blackarch-proxy
- Blackarch-windows
- Blackarch-dos
- Desensamblador blackarch
- Galleta negra
- Blackarch-voip
- Blackarch-recon
- Parodia de Blackarch
- Blackarch-crypto
- Blackarch-backdoor
- Forense negro
- Blackarch-fuzzer
- Blackarch-networking
- Blackarch Explotación
- Blackarch-wireless
- Blackarch-binary
- Blackarch-mobile
- Blackarch-reversing
- Blackarch-social
- Blackarch-automation
- Blackarch-music
- Blackarch-hardware
- Blackarch-defensivo
- Blackarch-descompiler
- Blackarch-malware
- Blackarch-honeypot
- Huella digital
- Blackarch-bluetooth

- Auditoria de código blackarch
- Tunel negro
- Sniffer blackarch
- Blackarch-debugger

(BlackArch Linux, 2020)

1.2. Metodología

1.2.1. PSP

1.2.1.1. ¿Qué es?

El Proceso de Software Personal (Personal Software Process) como su nombre lo indica es un proceso individual que busca ayudar a los ingenieros a mejorar su productividad y la gestión del tiempo.

1.2.1.2. Historia

Fue propuesto por Watts Humphrey en el año de 1995 en el Instituto de Ingeniería en Software (Software Engineering Institute o SEI), teniendo como guía el modelo para evaluar y mejorar la madurez de las capacidades (CMM). Para el año de 1997, con la publicación del libro “An Introduction to the Personal Software Process” el PSP estaba orientado hacia los ingenieros. (Gómez, Aguileta, Góme, & Aguilar, 2014)

Humphrey para ir refinando el proceso, escribo más de 60 programas. Cuando el proceso estaba más pulido fue aplicando a grupos de estudiantes de la maestría en Ingeniería de Software de la Universidad de Carnegie Mellon. (Gómez, Aguileta, Góme, & Aguilar, 2014)

1.2.1.3. Para que sirve

El PSP ayuda a hacer bien el trabajo de los ingenieros, aplicando métodos avanzados a tareas diarias, donde los ingenieros aprenden a controlar el trabajo que están realizando.

1.2.1.4. Versiones del Proceso

El proceso de PSP cuenta con 6 versiones ascendentes donde analizan y recopilan distintas mediciones, estas son.

1.2.1.4.1. PSP0

En esta versión solo se registra los tiempos y los defectos en los programas desarrollados. Se compone de 3 fases que son:

- Planificación: se documenta lo que se va a realizar.

- Desarrollo: El proceso de elaboración.
    - Diseño
    - Codificación
    - Verificación
- Postmortem: Se completa el plan.

(Gómez, Aguileta, Góme, & Aguilar, 2014)

1.2.1.4.2. PSP0.1

En esta versión se añade un estándar conocido como PIP (Persona Improvement Proposal), donde se puede tener acciones de mejoras para el desempeño.

1.2.1.4.3. PSP1

Con las mediciones de las versiones anteriores en esta se estima el tamaño del producto y la estimación de los tiempos que se requerirá para la construcción de los futuros productos.

1.2.1.4.4. PSP1.1

En esta versión se añade la planificación y calendarización de actividades.

1.2.1.4.5. PSP2.0

En esta versión se aprende a evaluar y mejoran en la estimación de tiempos, de igual manera en la calidad.

1.2.1.4.6. PSP2.1

Para esta última versión se añaden técnicas de especificación de diseño y análisis para reducir defectos.

2. Capítulo 2 - Caso de Estudio: Nilotex

2.1. Situación Actual

2.1.1. Historia

En plena mitad del mundo, en Quito – Ecuador, de un pequeño galpón de madera y con una básica maquinaria textil, nació NILOTEX, una empresa especializada en la fabricación de telas de punto, cordones y cintas elásticas.

Nació como una solución para la industria textil ecuatoriana en el área del tejido de punto y tejidos angostos en crochet.

La experiencia textil, química e industrial de 35 años de su fundador, complementada con los 25 años de trabajo de la empresa NILOTEX, nos ha permitido desarrollar productos innovadores y diseños exclusivos a un precio justo, los cuales aportan valor agregado al producto final elaborado por nuestros clientes. (Nilotex, 2020)

2.1.2. Misión

NILOTEX nació con la misión de entregar al mercado nacional productos innovadores y de diseños exclusivos, con la más alta calidad; contribuyendo al crecimiento de nuestros clientes.

Proporcionar en tiempo oportuno soluciones flexibles, innovadoras y con estándares de excelencia en el desarrollo de productos textiles. Centrados en satisfacer las necesidades y expectativas de nuestros clientes, el crecimiento sostenido de la empresa, el bienestar de los empleados y soluciones de responsabilidad social y ambiental.

Todo esto enmarcado bajo los principios de lealtad, responsabilidad, honradez y solidaridad. (Nilotex, 2020)

2.1.3. Visión

Gracias a la visión emprendedora y al trabajo constante, NILOTEX se ha convertido en uno de los más importantes referentes en el sector textil e industrial tanto a nivel nacional como internacional.

Ser una organización inteligente con miembros altamente capacitados y convencidos de la filosofía NILOTEX, que rebasa las aspiraciones personales y de sus familias, con proyección a un crecimiento humano, digno y solidario. (Nilotex, 2020)

2.1.4. Valores

Calidad, seguridad y satisfacción definen perfectamente los valores de Nilotex. Una empresa que demuestra día a día la importancia de trabajar con un equipo de profesionales avalado por una dilatada experiencia en el sector textil ecuatoriano.

Además, queremos ser dignos de la confianza de nuestros clientes y proveedores, asumiendo los compromisos y responsabilidad en el día a día. Con una actitud positiva y mucha ambición estamos dispuestos a progresar y a aprender mediante la reflexión y la planificación para obtener los mejores resultados. (Nilotex, 2020)

2.1.5. Compromiso

En Nilotex aspiramos a ser el primer proveedor de cada uno de nuestros clientes por su volumen de compras y por su grado de confianza.

Además, buscamos socios comerciales en nuestros clientes y proveedores; y nos centramos en la innovación para diferenciar nuestros productos, nuestros servicios y nuestra comunicación, de la competencia. (Nilotex, 2020)

2.1.6. Nuestro Equipo

Apoyados en el pilar fundamental de nuestra empresa como es el talento humano y porque es la mayor fortaleza de nuestra actividad económica, nos preocupamos por ellos, brindándoles estabilidad laboral, una constante capacitación, apoyándolos día a día en sus actividades, y manteniendo un ambiente de trabajo óptimo. (Nilotex, 2020)

2.1.7. Tecnología

En nuestras nuevas y funcionales instalaciones, con maquinaria de punta en tejeduría, tintorería, acabados y una moderna planta de tratamiento de aguas; punto a punto se teje nuestra gran variedad de productos

Para Nilotex es muy importante la satisfacción de nuestros clientes, y por tanto hacemos mucho hincapié en la calidad de nuestros productos y de nuestros procesos. (Nilotex, 2020)

2.2. Test de Penetración

2.2.1. ¿Qué es?

Conocido también como pruebas de penetración o de intrusión es un procedimiento sistemático para la detección de posibles vulnerabilidades de forma autorizada.

Es una simulación de ataques malicioso a un sistema informático, una red o una organización en condiciones reales.

2.2.2. Para que sirve

El objetivo del test de penetración en encontrar posibles vulnerabilidades en el sistema de una empresa o estructura de red. De igual manera que datos de la empresa pueden ser robados.

2.2.3. Tipos de Test

Existen 3 tipos de test a realizar, dependiendo del conocimiento que se tenga de la empresa y de la información que se tenga, así tenemos:

- **Test de penetración de caja blanca (White box):** es el test más completo. Este test se caracteriza porque el evaluador conoce y tiene toda la información acerca del sistema, aplicación o arquitectura, parte de un análisis integral.
- **Test de penetración de caja negra (Black box):** Este test es un análisis a ciegas, esto quiere decir que desconocemos la información de la empresa. Este test simula un ataque malicioso real.
- **Test de penetración de caja gris (Gray box):** En este test es una mezcla de los dos anteriores en donde se conoce cierta información de la empresa. En este test se invertirá tiempo y recursos para identificar las vulnerabilidades.

2.2.4. Tipos de pruebas que se realizan

Existen varios tipos de pruebas que se pueden realizar y cada uno tiene una acción específica en la organización.

- **Test de penetración en la red:** Este test busca problemas en la infraestructura de la red de una empresa.
- **Test de penetración de la aplicación Web:** detectar vulnerabilidades en sitios o aplicaciones web de la empresa, vigilar los puntos de acceso a los sistemas.
- **Test de penetración inalámbrica:** averiguar puntos de acceso a dispositivos no fiables, configuración de red, identificar estados de parches y versiones.

2.2.5. Fases de un test de penetración

Existen 5 fases para la elaboración de un test de penetración, son las siguientes:

- **Fase de recolección de datos:** También conocida como fase de reconocimiento. En esta fase se recopila y obtiene toda la información posible acerca del sistema que se va a atacar.
- **Fase de búsqueda de vulnerabilidades:** También conocida como fase de Análisis de vulnerabilidades o fase de escaneo. En esta fase se analiza la información obtenida en la fase anterior buscando posibles vectores de ataque, se escanean puertos y servicios.
- **Fase de explotación de vulnerabilidades:** También conocida fase de enumeración, en esta fase se accede a los sistemas de la organización usando la información obtenida en las fases anteriores como credenciales, etc. En esta fase se obtiene información referente a usuarios, nombre de equipos, servicios de red.
- **Fase Post-exploración:** También conocida como fase de acceso, finalmente se obtiene acceso al sistema, aprovechando las vulnerabilidades obtenidas en fases previas, se ganan privilegios dentro del sistema.
- **Fase de mantenimiento de acceso:** En esta fase lo que se busca es mantener el acceso durante algún tiempo. En esta fase también se elaboran informes indicando las vulnerabilidades encontradas y como se han explotado.

2.2.6. Puesta en Practica

Para la puesta en práctica de este análisis se usarán 3 herramientas, de las cuales dos son del sistema Kali Linux, en este sistema se utilizará Zenmap que cuenta con una interfaz gráfica y la otra herramienta a usarse en este sistema será la terminal de Kali Linux, a través de la cual se ejecuta por la línea de comandos. La tercera herramienta que se utilizará es el sistema BlackArch con su terminal mediante línea de comando. Los comandos a aplicarse para identificar la vulnerabilidad, serán ejecutados en las tres herramientas por igual para luego analizar sus resultados y tomar la mejor decisión para la elaboración de la guía de implementación de la ISO/IEC 27001.

2.2.6.1. Recolección de información

2.2.6.1.1. Obtención de la IP publica

```
C:\Users\Privada>ping nilotex.com

Haciendo ping a nilotex.com [190.57.149.194] con 32 bytes de datos:
Respuesta desde 190.57.149.194: bytes=32 tiempo=8ms TTL=48
Respuesta desde 190.57.149.194: bytes=32 tiempo=9ms TTL=48
Respuesta desde 190.57.149.194: bytes=32 tiempo=9ms TTL=48
Respuesta desde 190.57.149.194: bytes=32 tiempo=9ms TTL=48

Estadísticas de ping para 190.57.149.194:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 8ms, Máximo = 9ms, Media = 8ms
```

Ilustración 2. Ping nilotex.com (Yonfá, 2020)

Realizamos un PING al dominio de la empresa se puede obtener la IP publica de la empresa

```
:\Users\Privada>tracert www.nilotex.com

raza a la dirección www.nilotex.com [190.57.149.194]
obre un máximo de 30 saltos:

 1    <1 ms    <1 ms    <1 ms  192.168.100.1
 2  2283 ms     3 ms     3 ms  host-186-4-232-1.netlife.ec [186.4.232.1]
 3     7 ms     4 ms     4 ms  10.201.194.69
 4     7 ms     4 ms     3 ms  10.201.194.29
 5    13 ms     3 ms     4 ms  10.201.194.21
 6     8 ms     4 ms     4 ms  10.201.194.61
 7     2 ms     2 ms     2 ms  10.201.194.1
 8     2 ms     2 ms     2 ms  10.201.222.13
 9     3 ms     7 ms     6 ms  10.201.222.29
10    10 ms     8 ms     8 ms  10.201.222.28
11     9 ms     8 ms     8 ms  10.201.212.52
12     8 ms     8 ms     8 ms  10.201.111.141
13     9 ms     8 ms     8 ms  200.110.120.10
14     *        *        *     Tiempo de espera agotado para esta solicitud.
15     *        *        *     Tiempo de espera agotado para esta solicitud.
16     *        *        *     Tiempo de espera agotado para esta solicitud.
17     *        *        *     Tiempo de espera agotado para esta solicitud.
18     9 ms     9 ms     9 ms  mail.nilotex.com [190.57.149.194]

raza completa.
```

Ilustración 3. TRACERT www.nilotex.com (Yonfá, 2020)

Con el comando TRACERT también se puede obtener la dirección. Este comando realiza un seguimiento desde la IP de salida hasta el destino que queremos detectar.

2.2.6.1.2. Whois

Posteriormente se utilizó la herramienta Whois en la dirección IP del domino de la empresa, la cual realiza una consulta de la información pública de dicha empresa.

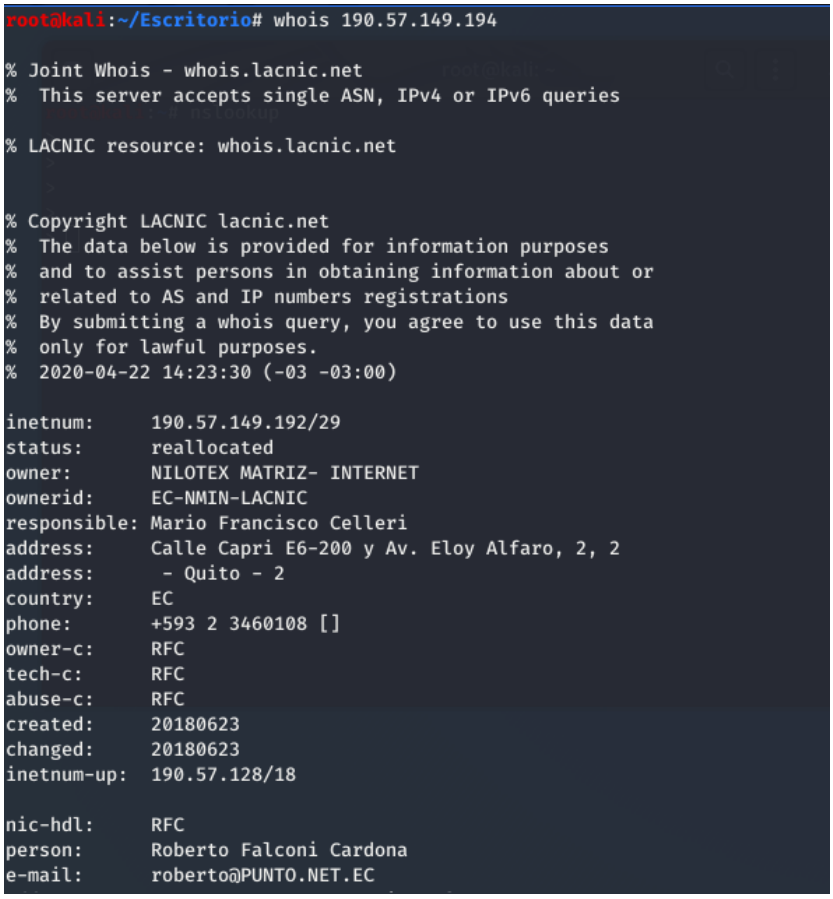

Ilustración 4. Whois – Kali Linux (Yonfá, 2020)

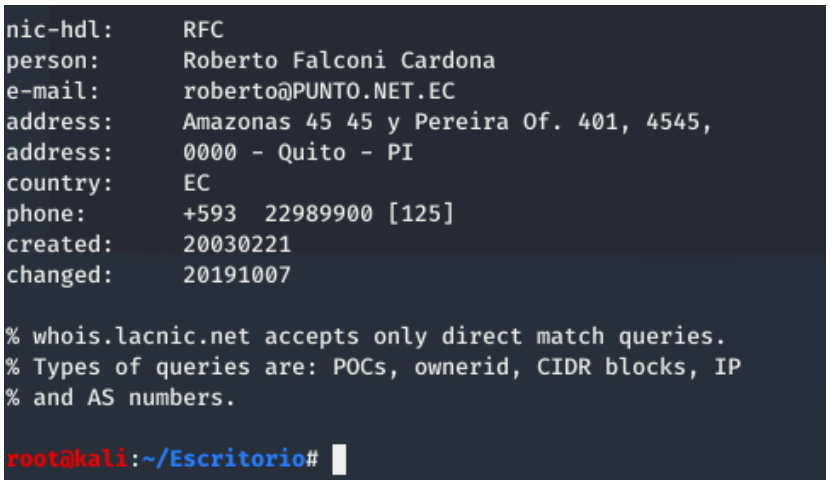

Ilustración 5. Whois (Yonfá, 2020)

Ilustración 6. Whois - BlackArch (Yonfá, 2020)

Ilustración 7. Whois - BlackArch (Yonfá, 2020)

2.2.6.1.3. Análisis DNS

2.2.6.1.3.1. Dnsenum

Se realizó un análisis con la herramienta Dnsenum que nos permite enumerar la información DNS de un dominio y poder detectar direcciones IP no contiguas. (Filip Waeytens, s.f.)

En esta sección se utilizó la opción –w que hace referencia a whoi, que sirve para obtener información acerca de un propietario de un dominio o dirección IP.

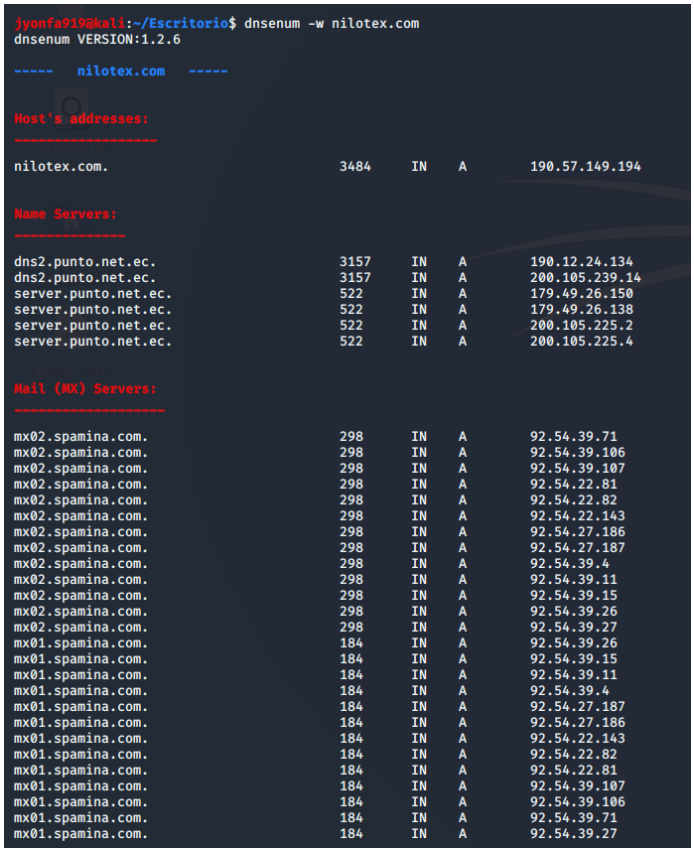

Ilustración 8. dsnenum –w – Kali Linux (Yonfá, 2020)

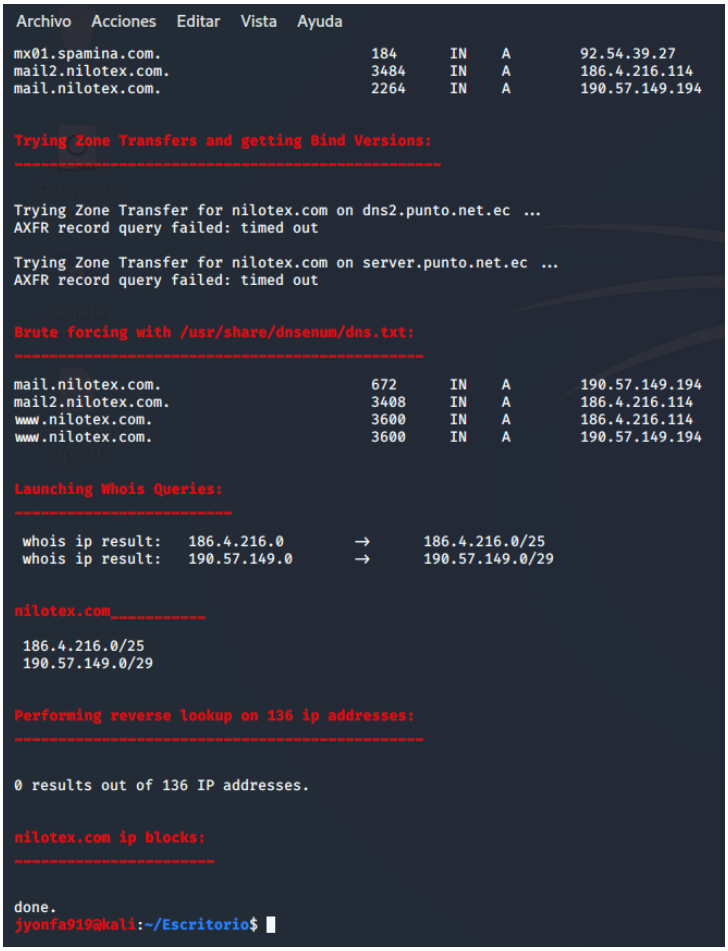

Ilustración 9. dsnenum –w – Kali Linux (Yonfá, 2020)

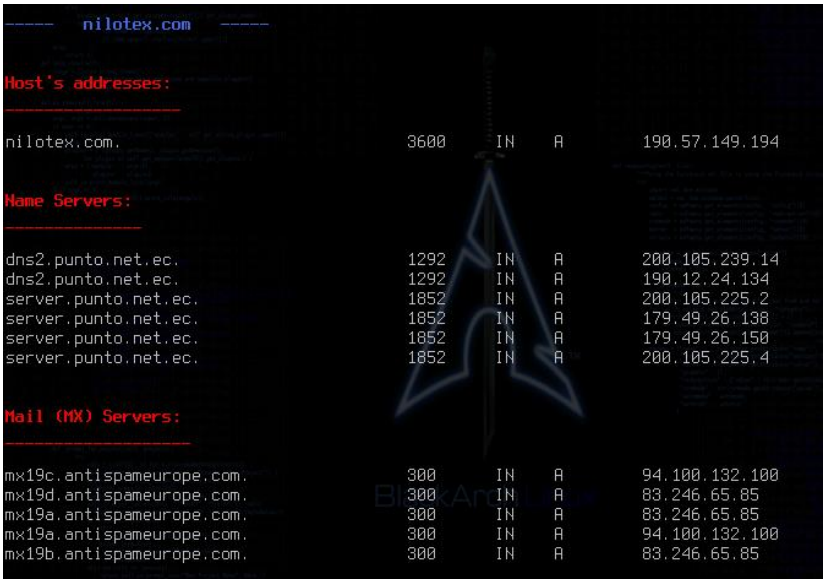

Ilustración 10. dnsuenum -w - BlackArch (Yonfá, 2020)

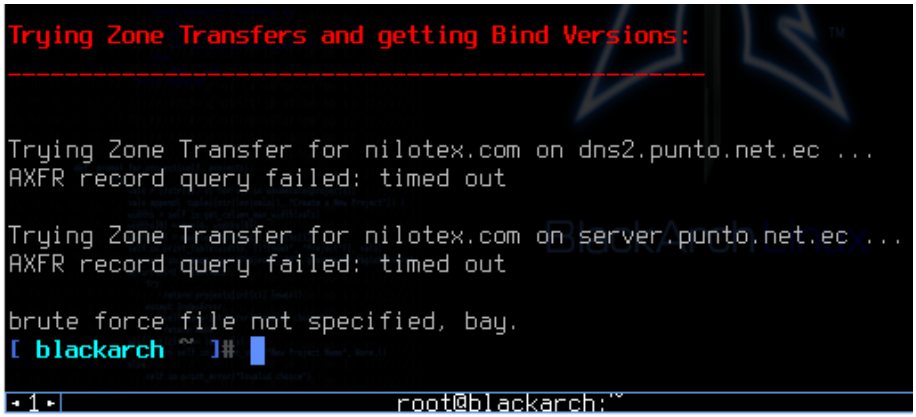

Ilustración 11. dnsenum -w - BlackArch (Yonfá, 2020)

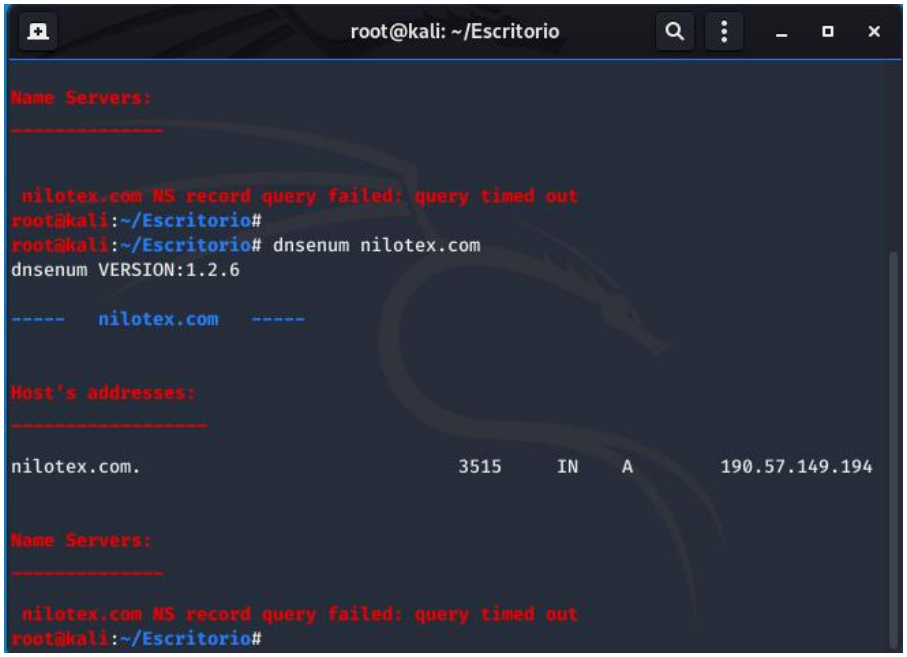

Ilustración 12. Dnsenum – Kali Linux (Yonfá, 2020)

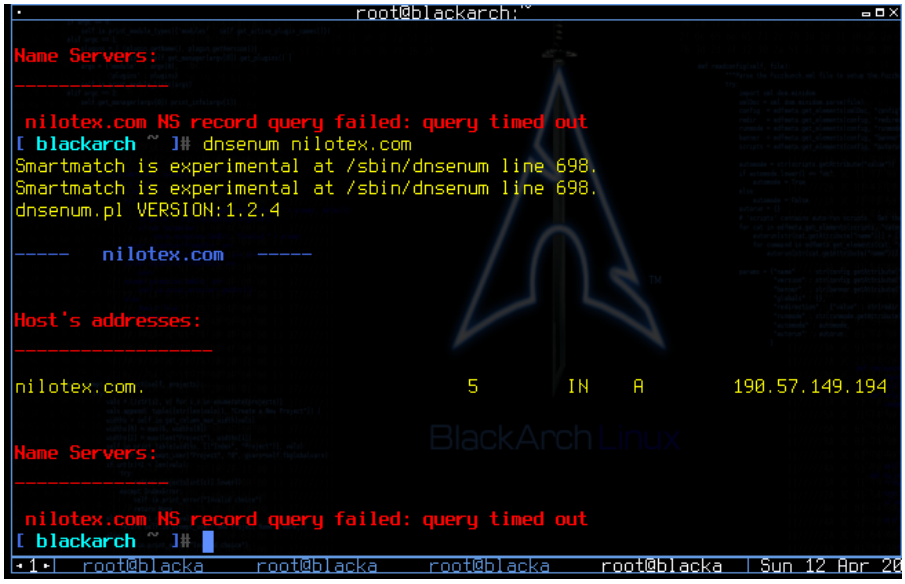

Ilustración 13. Dnsenum (Yonfá, 2020)

2.2.6.1.3.2. Dnsmap

Con la herramienta dnsmap podemos obtener servidores de acceso remoto, servidores mal configurados o sin parches y nuevos nombres de dominio, Descubrir dispositivos embebidos configurados mediante servicios de DNS dinámico. (pagvac, s.f.)

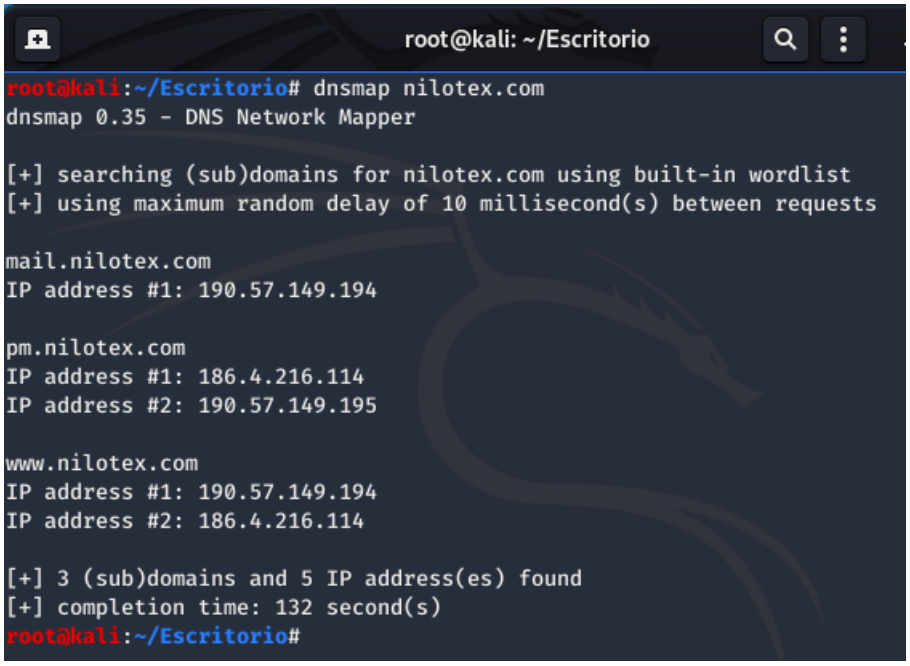

Ilustración 14. Dnsmap – Kali Linux (Yonfá, 2020)

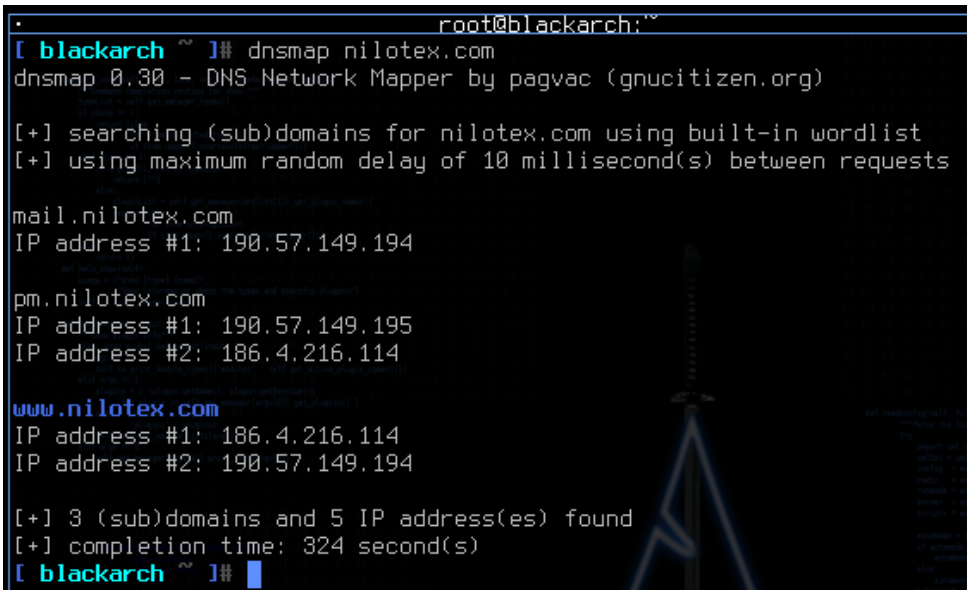

Ilustración 15.Dnsmap - BlackArch (Yonfá, 2020)

2.2.6.1.3.3. Dnstracert

Esta herramienta nos ayuda a seguir la pista de los paquetes que se envían desde un host a través de los servidores que recorre. (Groothuis, s.f.)

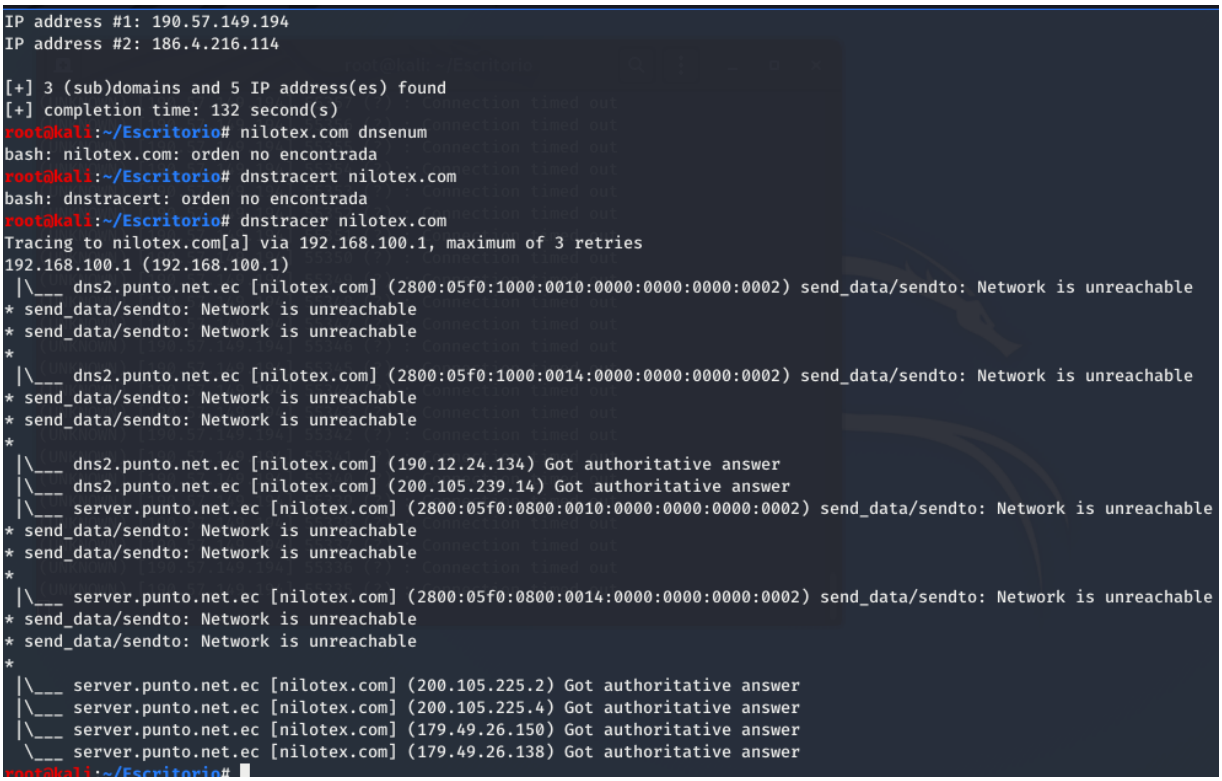

Ilustración 16. Dnstracert – Kali Linux (Yonfá, 2020)

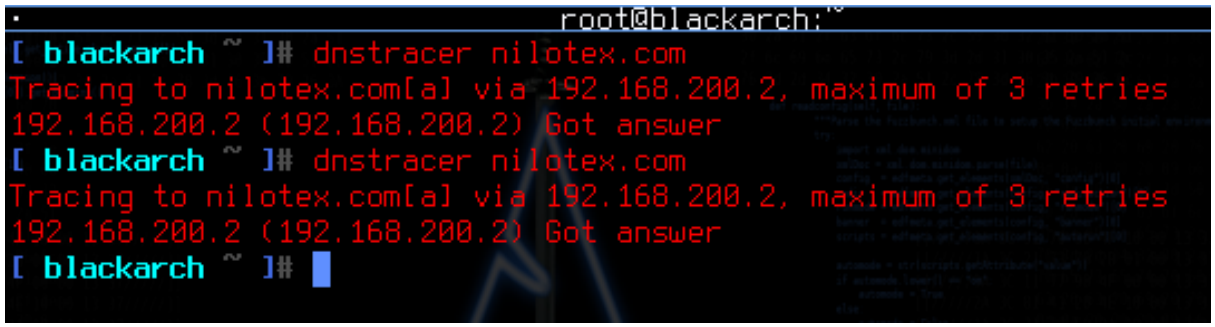

Ilustración 17. Dnstracert - BlackArch (Yonfá, 2020)

2.2.6.1.4. Análisis de Ruteo

2.2.6.1.4.1. Netdiscover

La herramienta netdescover se utiliza para el descubrimiento de direcciones.

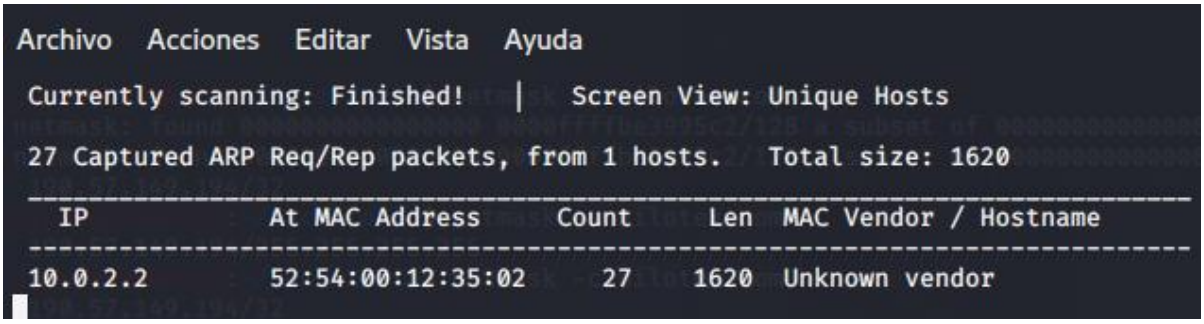

Ilustración 18.Netdiscover – Kali Linux (Yonfá, 2020)

2.2.6.1.5. Análisis OSINT

2.2.6.1.5.1. Theharvest

Con esta herramienta podemos recopilar cuentas de correo electrónico, nombres de usuario, nombres de host que será importantes en fases futuras.

Las fuentes de ayuda para estas búsquedas son Google, Google perfiles, Bing, PGP servidores, LinkedIn, entre otras. (Martorella, s.f.)

Ilustración 19. Theharvest – Kali Linux (Yonfá, 2020)

Ilustración 20. Theharvest – Kali Linux (Yonfá, 2020)

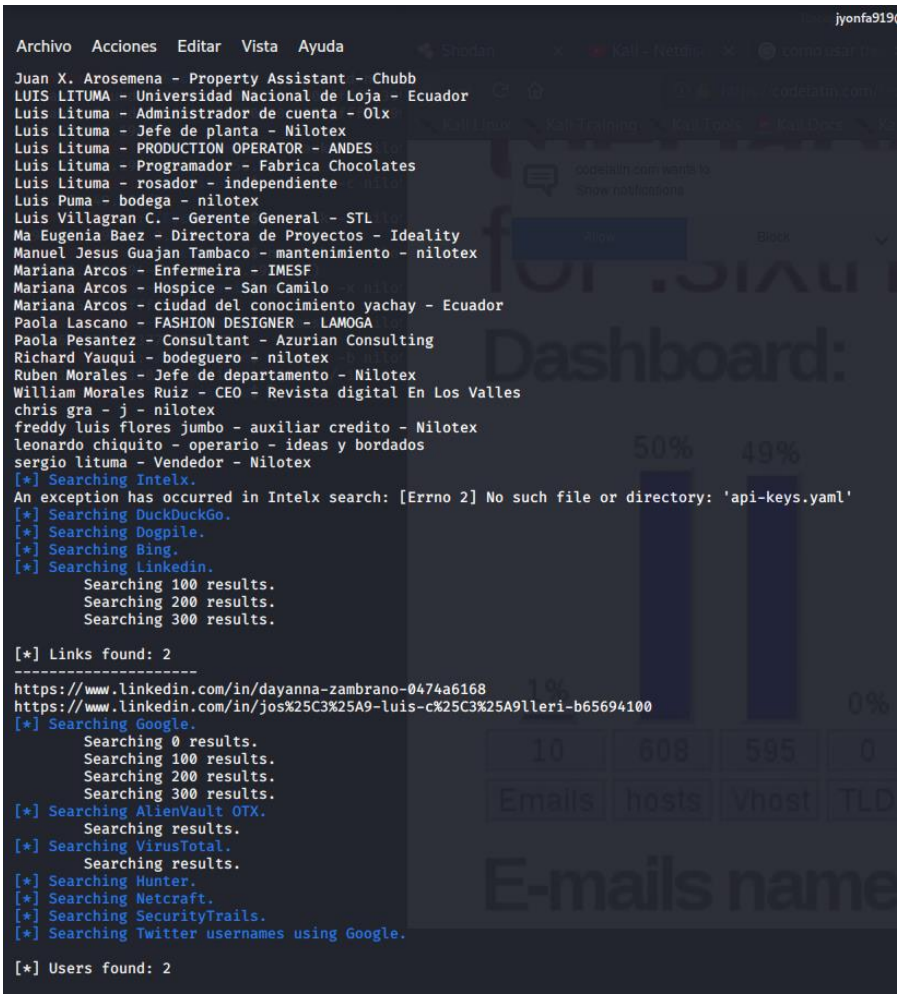

Ilustración 21. Theharvest – Kali Linux (Yonfá, 2020)

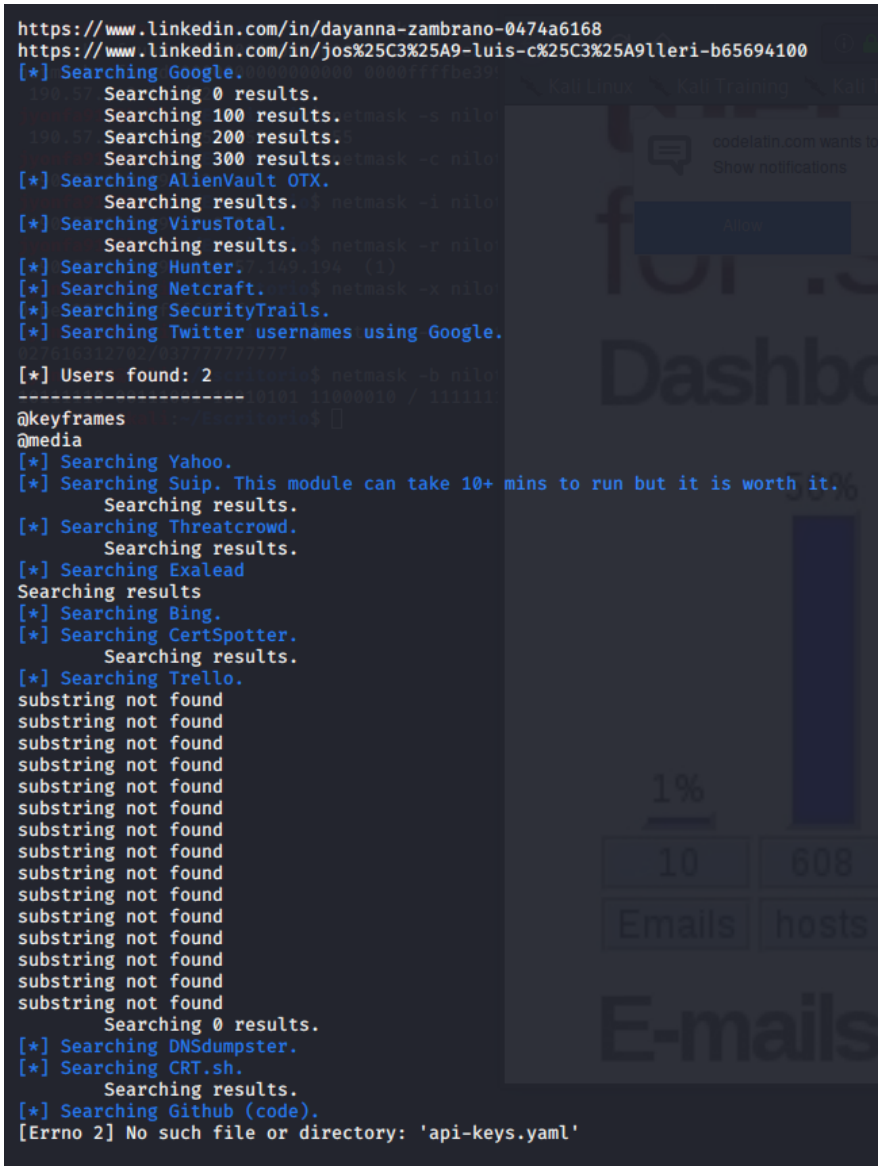

Ilustración 22. Theharvest – Kali Linux (Yonfá, 2020)

2.2.6.1.9. Análisis SSL

2.2.6.1.9.1. Sslscan

SSLScan es una herramienta que permite comprobar la seguridad de nuestras conexiones SSL con determinados servidores. (Velasco, 2014)

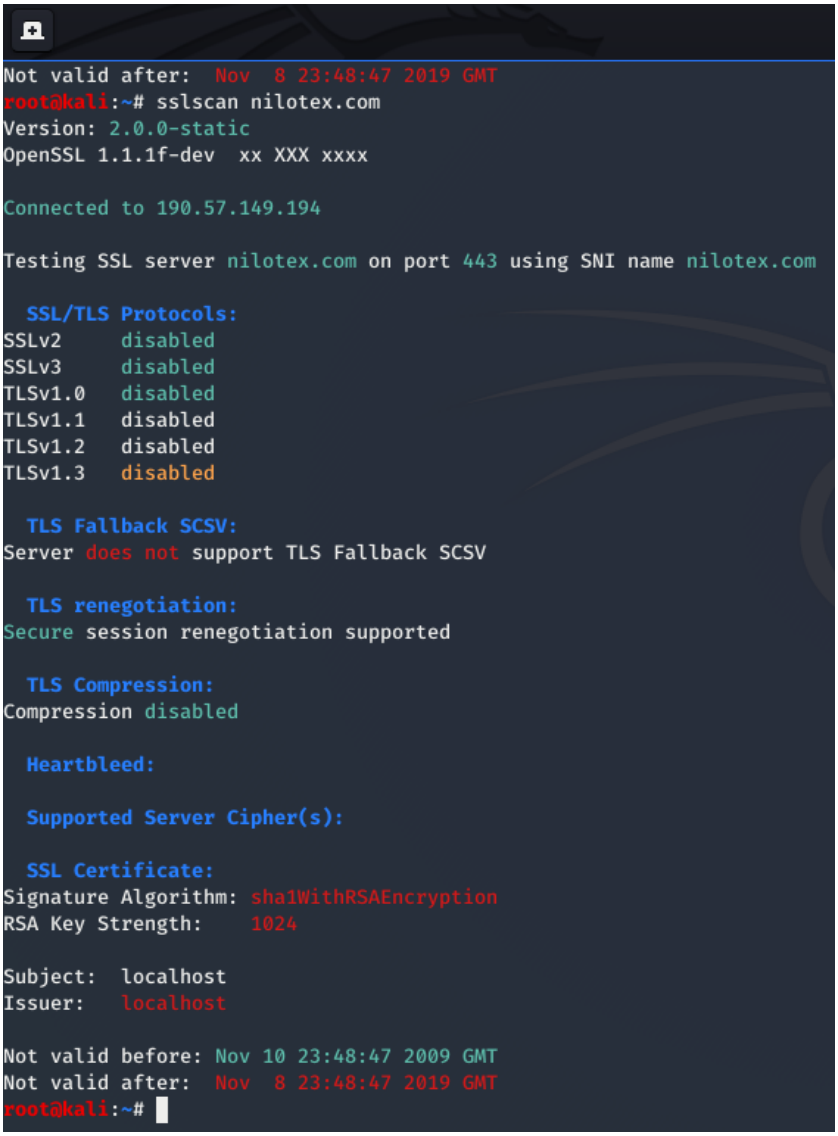

Ilustración 23. Sslscan – Kali Linux (Yonfá, 2020)

2.2.6.1.10. Escáner de redes

2.2.6.1.10.1. Nmap

Es una herramienta que nos permite la exploración de la red, esta herramienta utiliza paquetes IP para determinar que host están disponibles en la red, servicios, entre otras características.

```
root@kali:~# nmap -O 190.57.149.194
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-11 19:35 -05
Nmap scan report for 190.57.149.194
Host is up (0.0085s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
110/tcp  open  pop3
443/tcp  open  https
587/tcp  open  submission
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.06 seconds
```

Ilustración 24. Nmap -O - Kali Linux (Yonfá, 2020)

```
root@kali: ~/Escritorio
root@kali:~/Escritorio# nmap -O 190.57.149.194
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-06 20:28 -05
Nmap scan report for mail.nilotex.com (190.57.149.194)
Host is up (0.0072s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Aggressive OS guesses: Oracle Virtualbox (92%), Linux 1.0.9 (89%), Cisco IP Phon
e 7912-series (89%), QEMU user mode network gateway (88%), ZyXEL Prestige 660R A
DSL router (88%), Casio QT-6000 or QT-6100 point-of-sale machine (87%), Sitecom
WL-174 wireless ADSL router or ZyXEL B-3000 WAP (87%), Samsung CLP-310N or CLX-3
175RW, or Xerox Phaser 6110 printer (86%), Ricoh Aficio SP C210SF printer (86%),
 Samsung CLX-3160FN printer (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds
root@kali:~/Escritorio#
```

Ilustración 25. Nmap -O - Kali Linux (Yonfá, 2020)

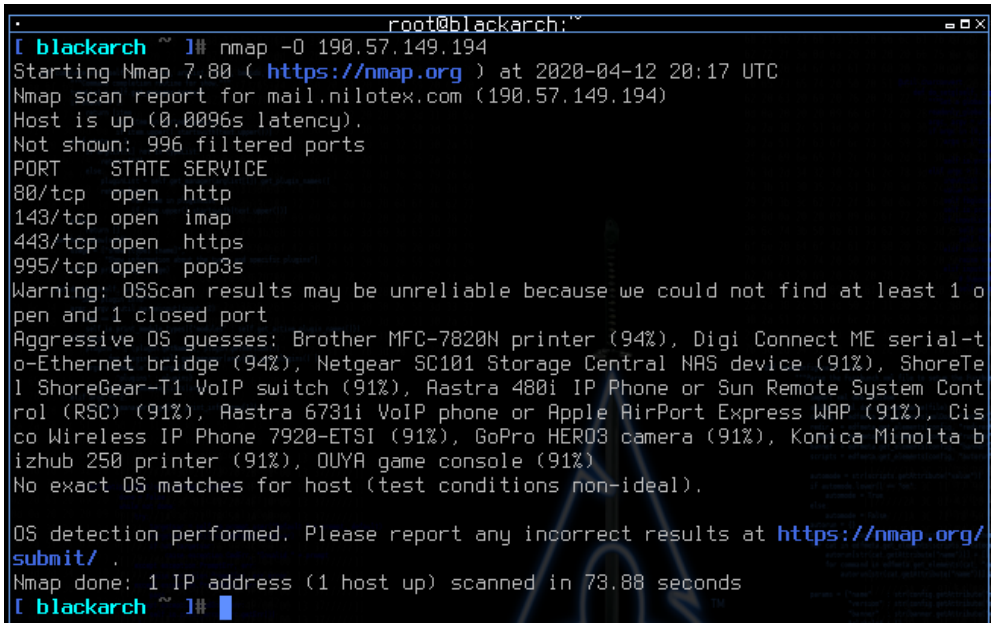

Ilustración 26. Nmap -O - BlackArch (Yonfá, 2020)

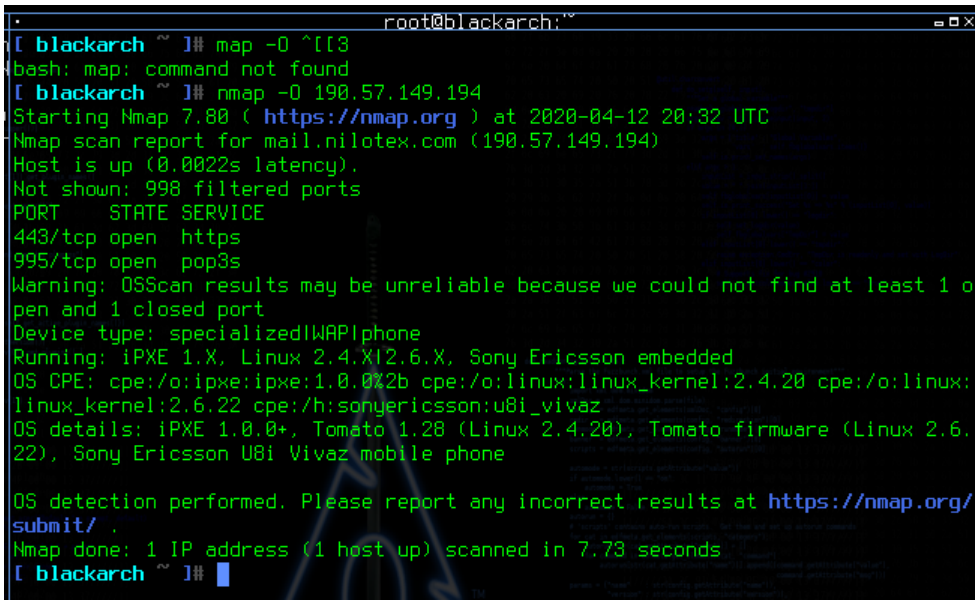

Ilustración 27. Nmap -O - BlackArch (Yonfá, 2020)

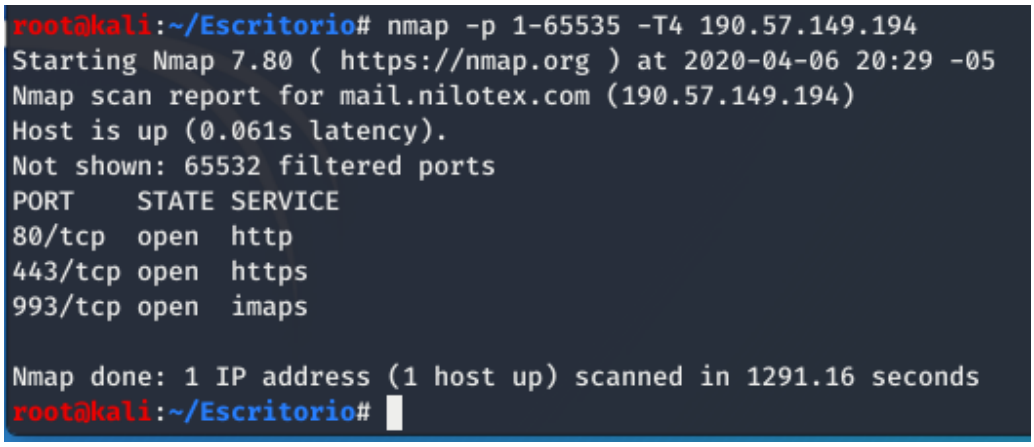

Ilustración 28. Nmap -P - Kali Linux (Yonfá, 2020)

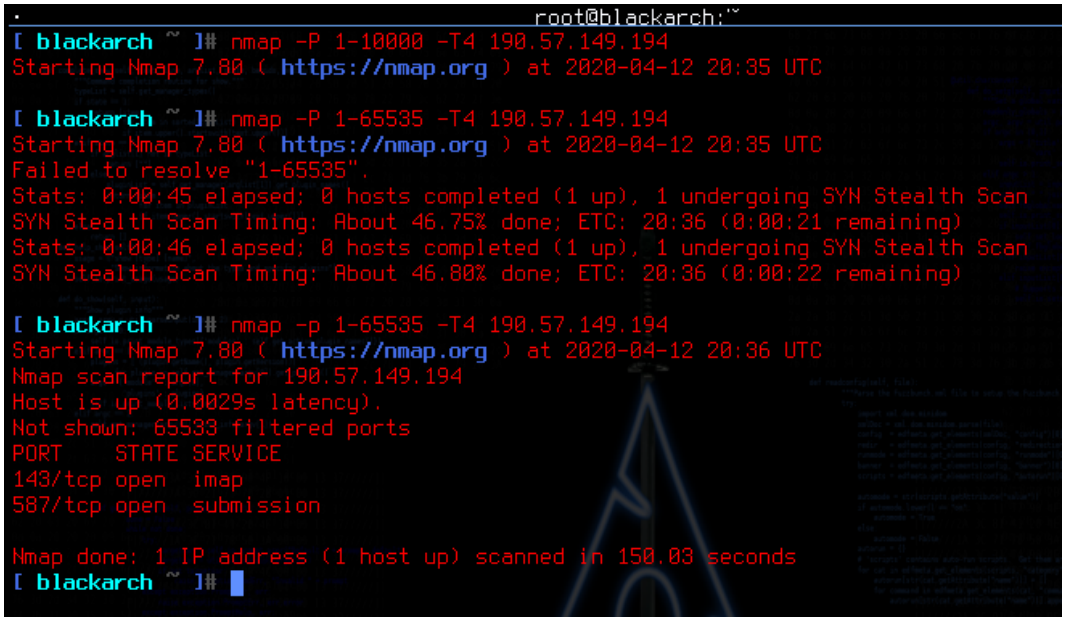

Ilustración 29. Nmap -p -BlackArch (Yonfá, 2020)

2.2.6.2. Análisis de Vulnerabilidades

El análisis de vulnerabilidades en la red de una empresa ayudará a detectar las posibles fallas y riesgos de seguridad que esta posee en sus routers, software, redes, etc., que puede ser aprovechadas con fines maliciosos. (Grupo CFI, s.f.)

Existen diversas herramientas que nos permiten realizar este análisis e identificar las vulnerabilidades que posee una red, en este caso utilizaremos “scripts” que la herramienta nmap posee para este escaneo.

2.2.6.2.1. Auth

El script “Auth” ejecuta todos los scripts relacionados con la autentificación. (ESET, 2015) (Leacock, 2019).

Con el script Auth las vulnerabilidades que se pretenden detectar son las asociadas a autentificación o bypass de los sistemas escaneados, este script trabaja con credenciales de autentificación, esto quiere decir que incluye comprobaciones de inicio de sesión, enumeración de usuarios, acceso al servidor, comprobación de inicio de sesión predeterminada entre otras. (NMAP.ORG, s.f.) (ceos3c, 2019)

KALI LINUX - ZENMAP

Empezamos el análisis utilizando la herramienta Zenmap que cuenta con una interfaz gráfica, para este escaneo utilizamos el script Auth.

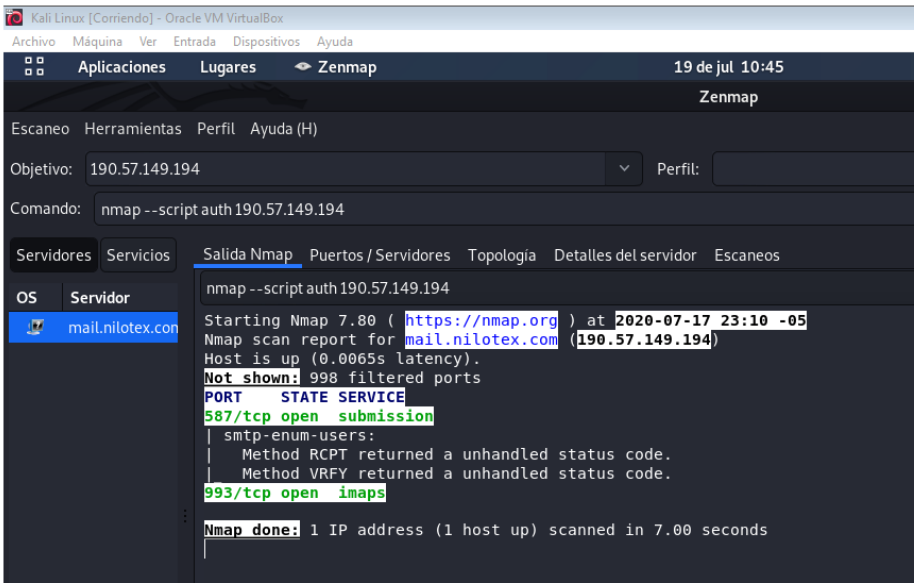

Ilustración 30. Zenmap – Auth – Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Auth

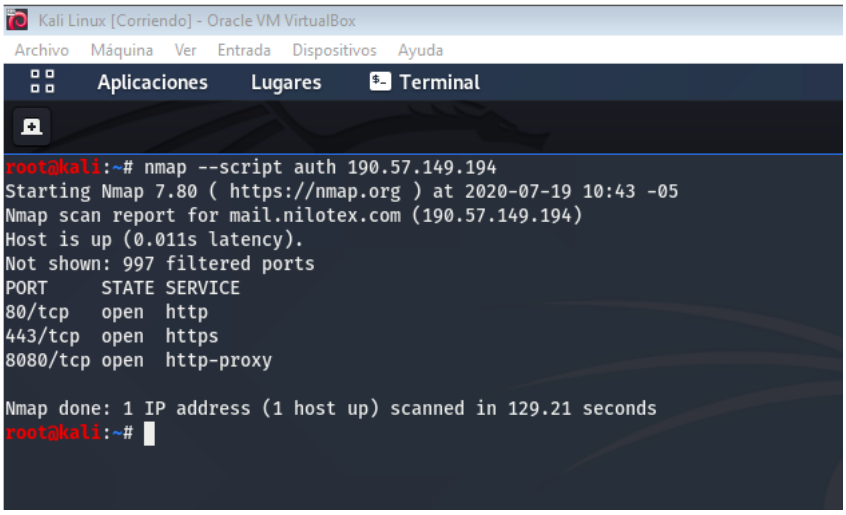

Ilustración 31. Nmap – Auth (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Auth, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas

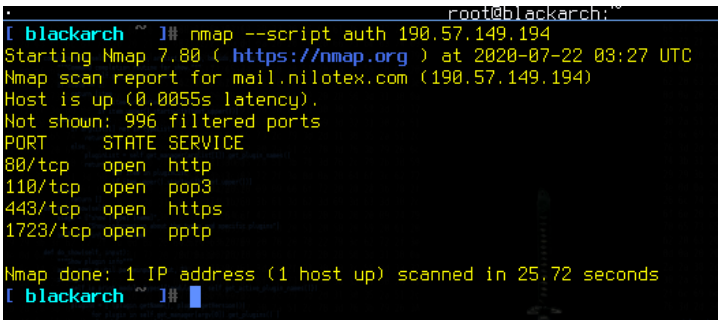

Ilustración 32. Nmap - Auth - BlackArch (Yonfá, 2020)

Después de finalizar la utilización del script Auth de las tres formas, como resultados podemos observar que no existe ningún problema o vulnerabilidad en cuanto a la autentificación en los puertos que se encuentran abiertos.

2.2.6.2.2. Default

El script default ejecuta todos los scripts básicos que la herramienta nmap posee en sus librerías. (ESET, 2015) (Leacock, 2019).

Para la ejecución del script default se toma en cuenta varias métricas como son la velocidad, confiabilidad, nivel de intrusión, privacidad entre otros. Este script ejecuta un montón de script individuales a la vez

buscando nombre del grupo de trabajo, nombre NetBIOS, comprobaciones de inicio de sesión anónimas FTP entre otros más.

KALI LINUZ – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Default.

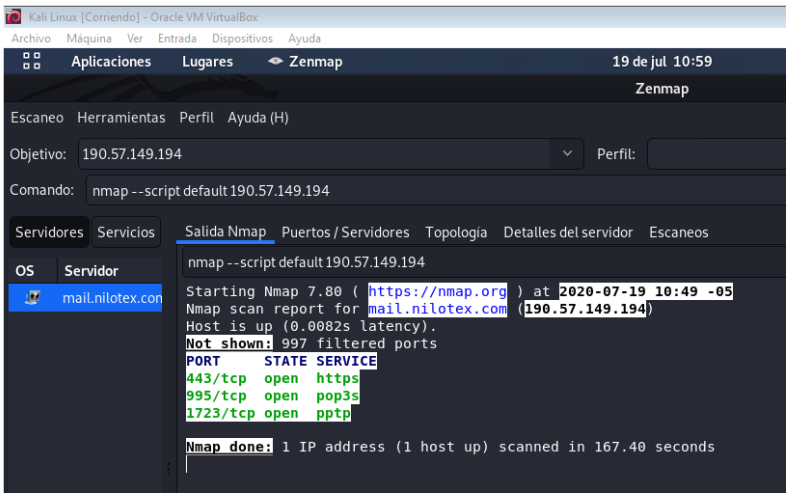

Ilustración 33. Zenmap - Default - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Default.

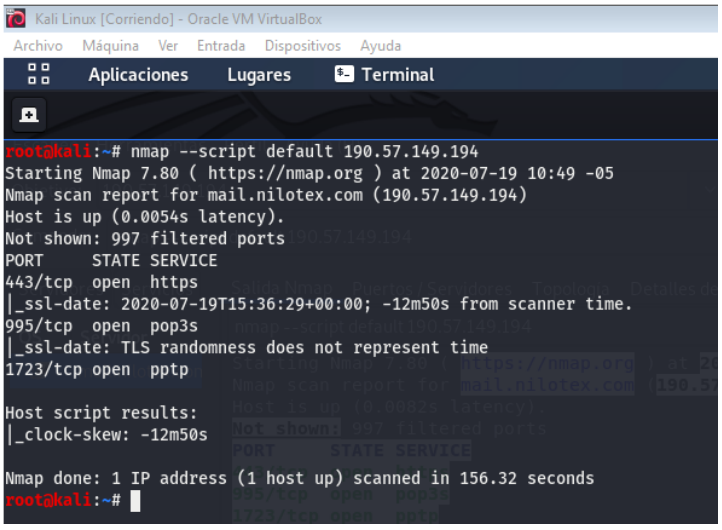

Ilustración 34. Nmap - Default - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Default, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas.

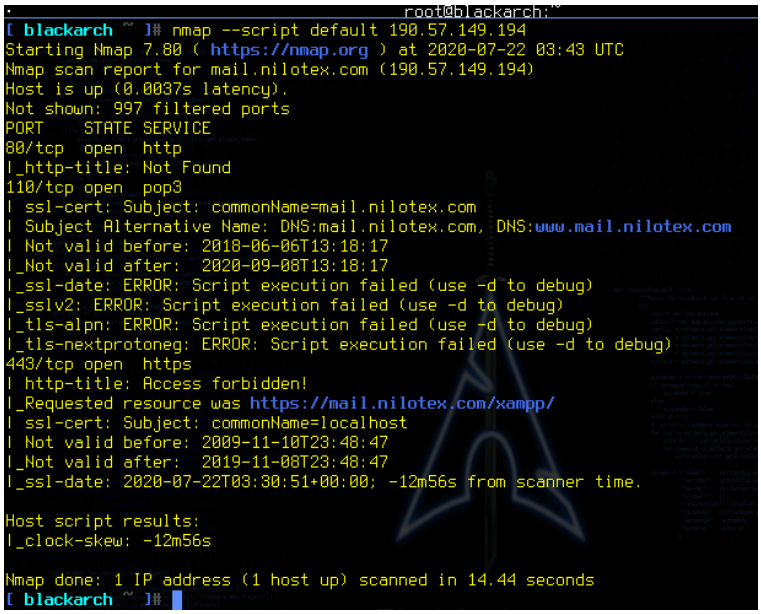

Ilustración 35. Nmap - Default - BlackArch (Yonfá, 2020)

Una vez finalizada la exploración usando el script Default podemos observar que en todos los sub-scripts que este script utiliza no se han encontrado vulnerabilidades en los puertos que las herramientas analizan.

2.2.6.2.3. Discovery

El script Discovery permite recuperar información de la víctima o target (denominado mercado meta u objetivo), utilizando accesos a registros públicos, directorios de servicio, entre otros (ESET, 2015) (Leacock, 2019).

La ejecución del script Discovery se la realiza para obtener tanta información como sea posible, este grupo de script busca información de cisc, comprobación de zonas DNS, enumeración SMB, dispositivos habilitados para SNMP, enumero recursos compartidos de Windows, entre otros.

KALI LINUZ – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Discovery.

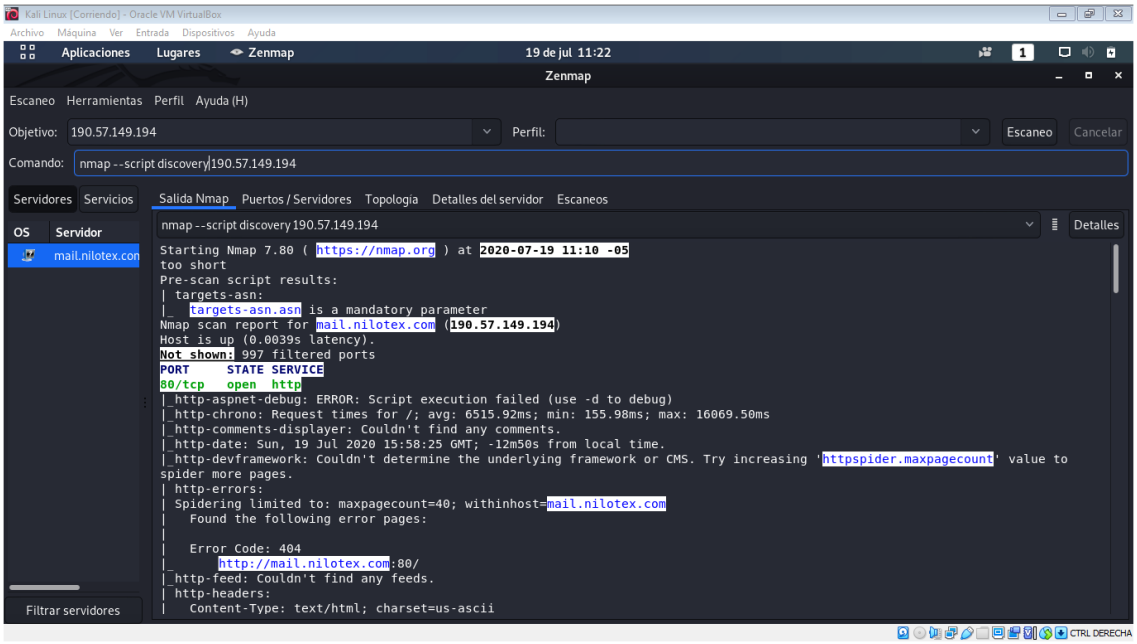

Ilustración 36. Zenmap - Discovery - Kali Linux (Yonfá, 2020)

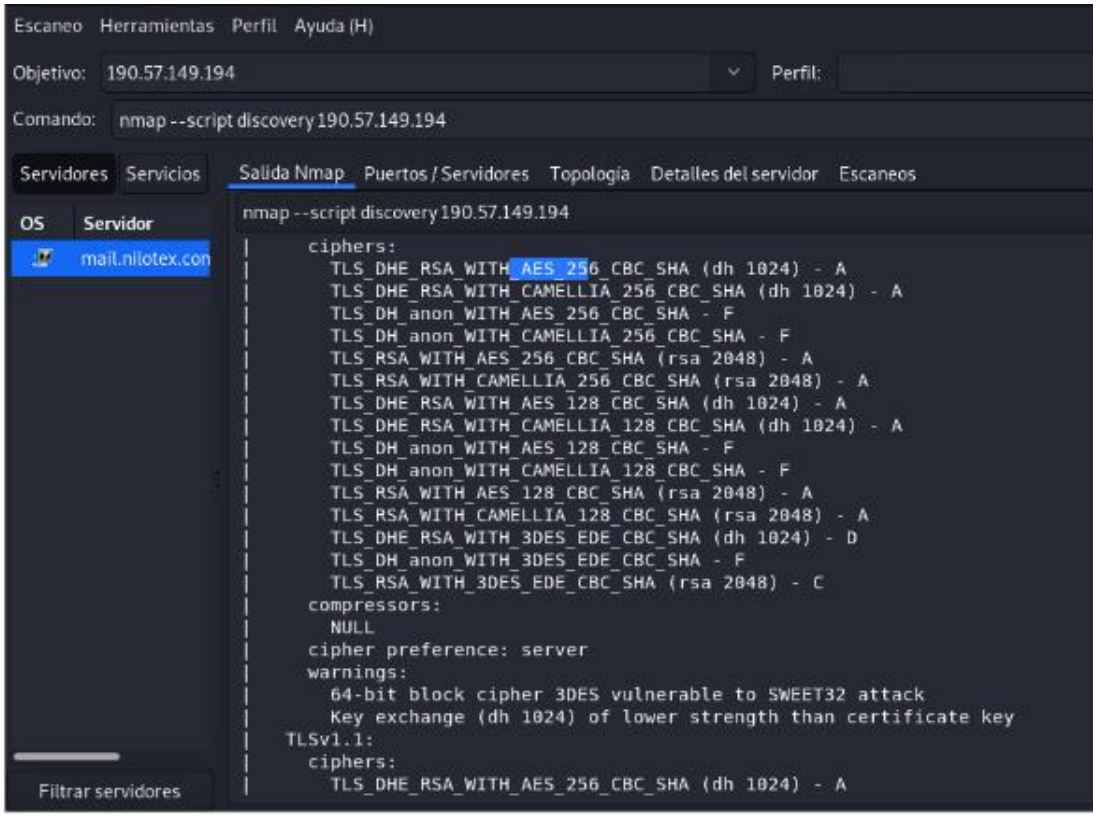

Ilustración 37. Zenmap - Discovery - Kali Linux (Yonfá, 2020)

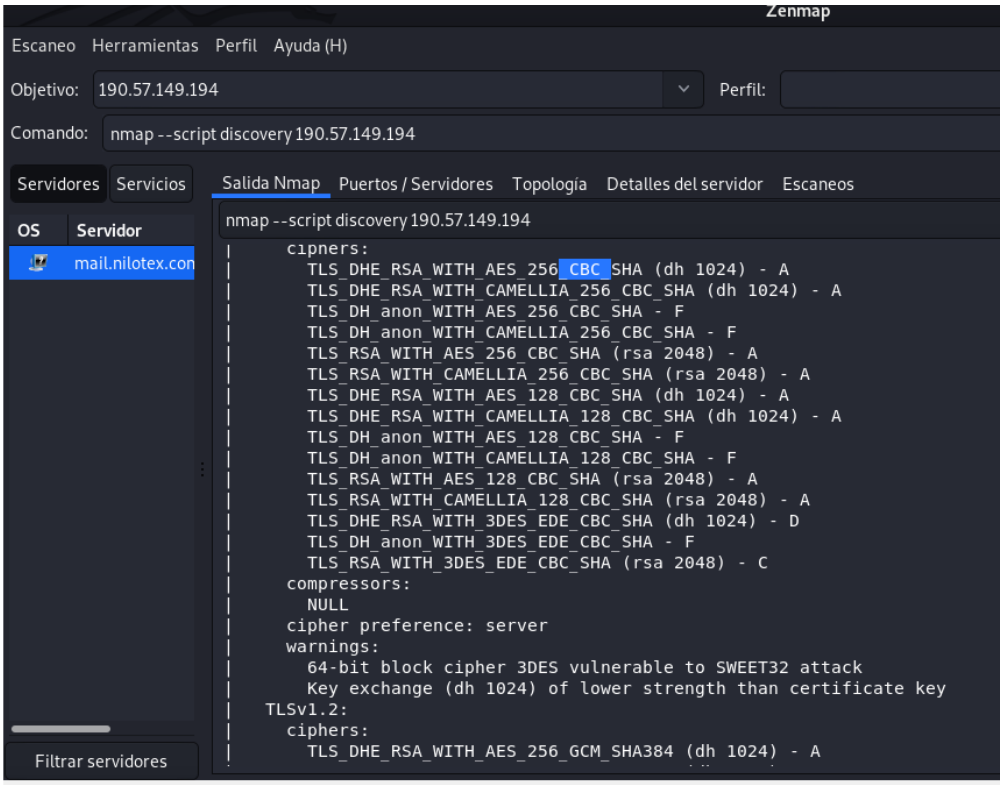

Ilustración 38. Zenmap - Discovery - Kali Linux (Yonfá, 2020)

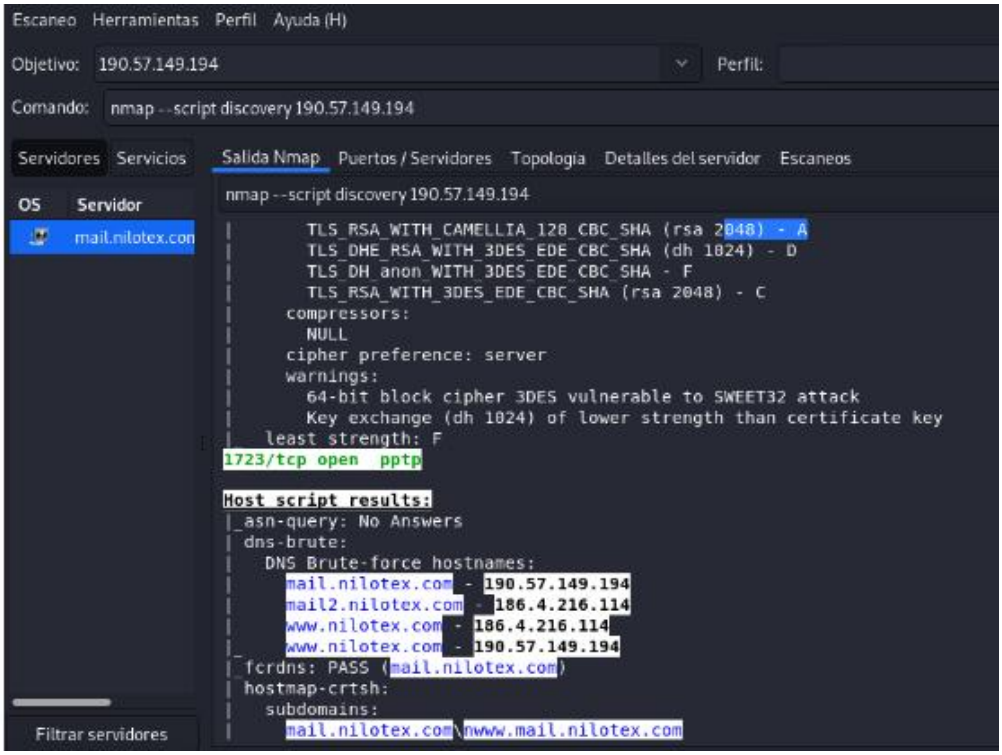

Ilustración 39. Zenmap - Discovery - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Discovery.

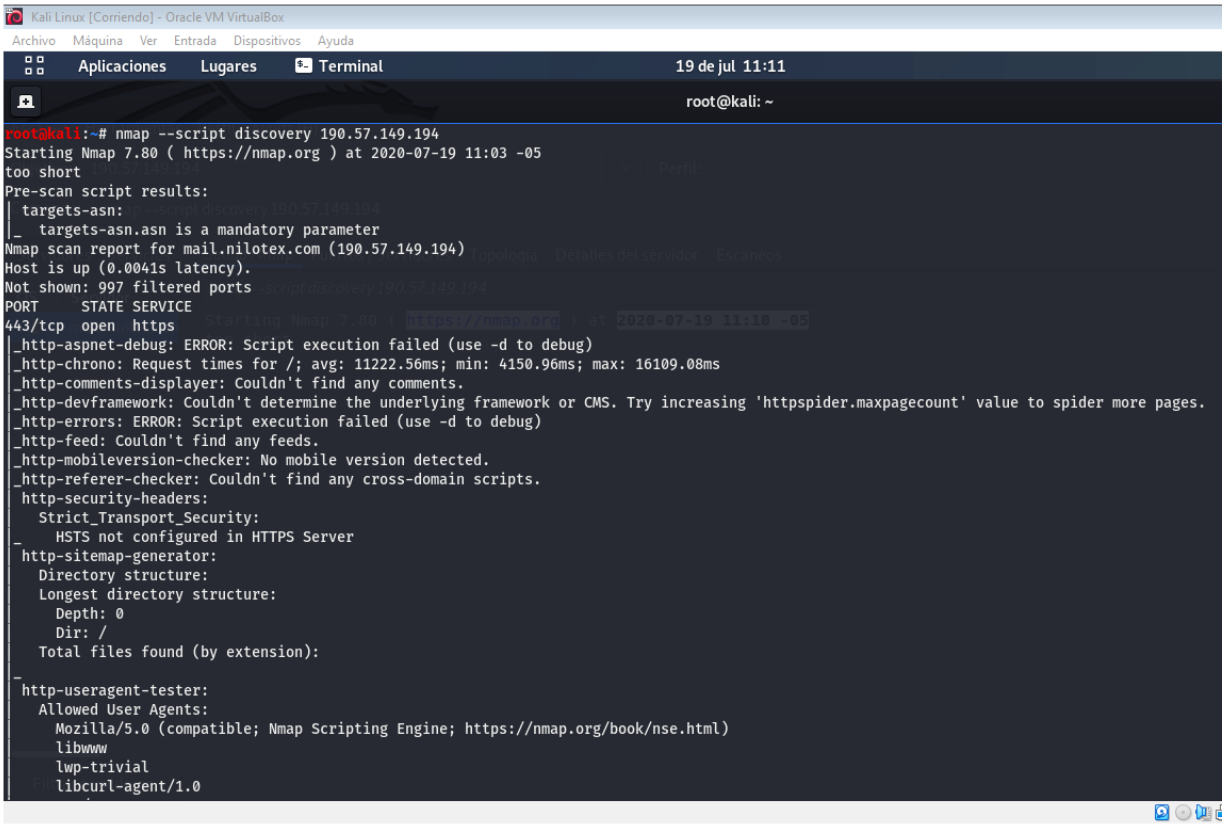

Ilustración 40. Nmap - Discovery - Kali Linux (Yonfá, 2020)

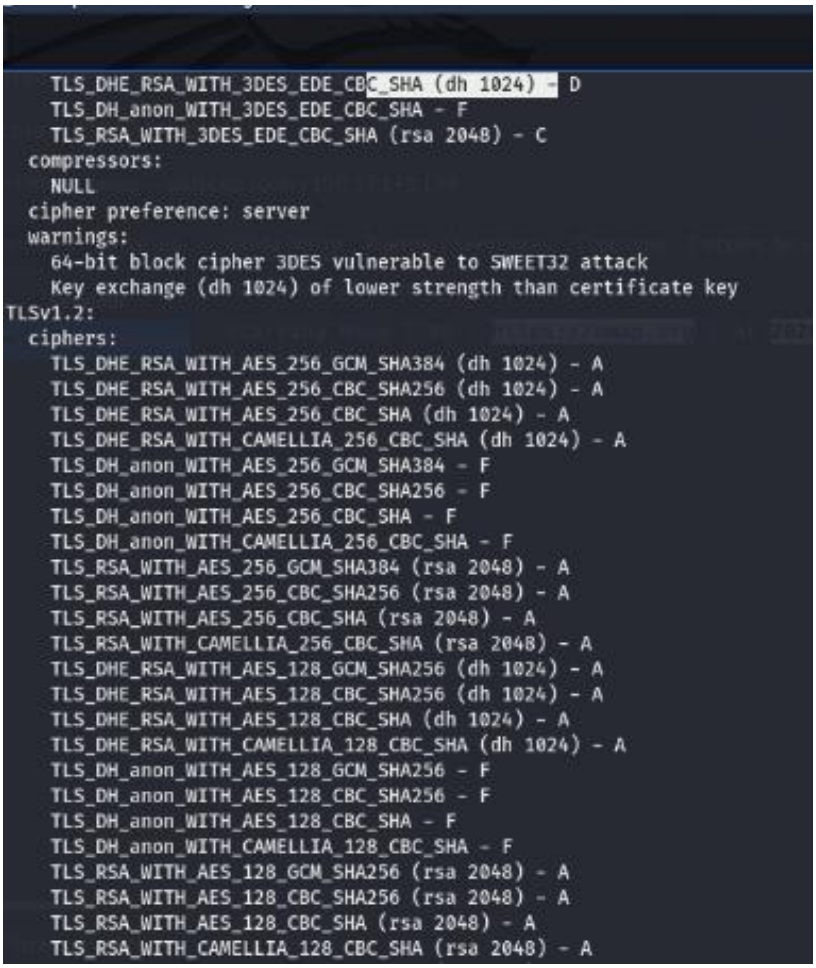

Ilustración 41. Nmap - Discovery - Kali Linux (Yonfá, 2020)

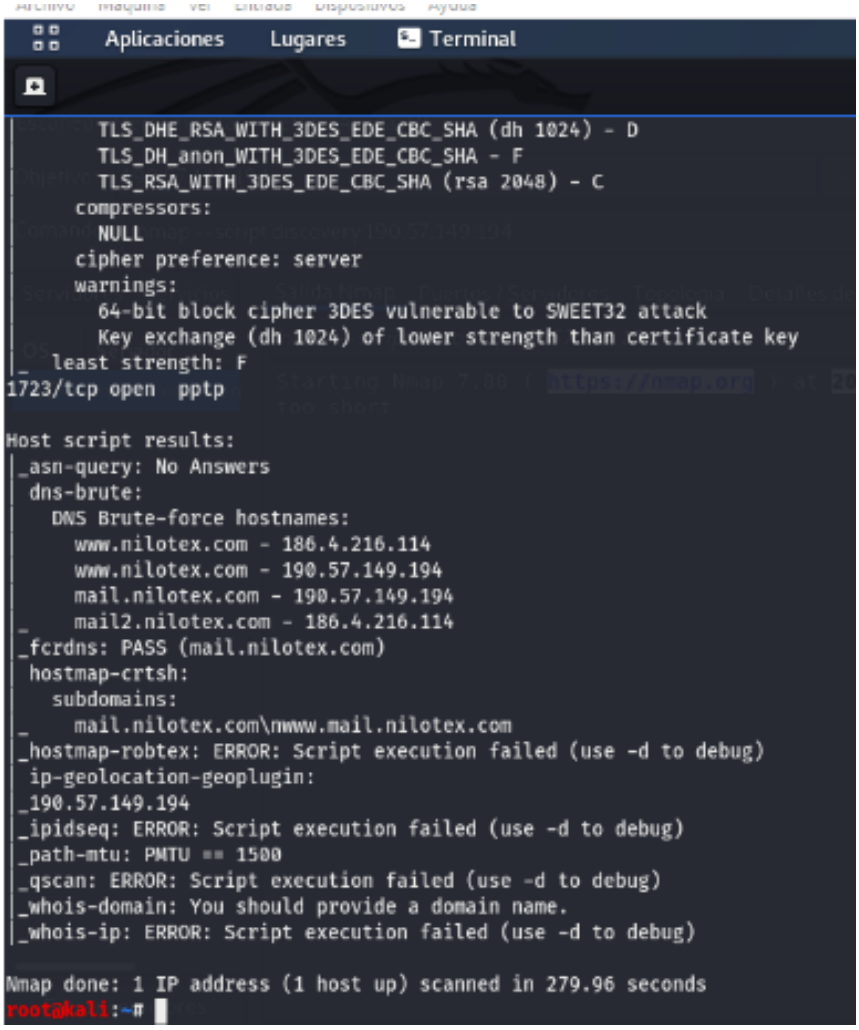

Ilustración 42. Nmap - Discovery - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Discovery, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas

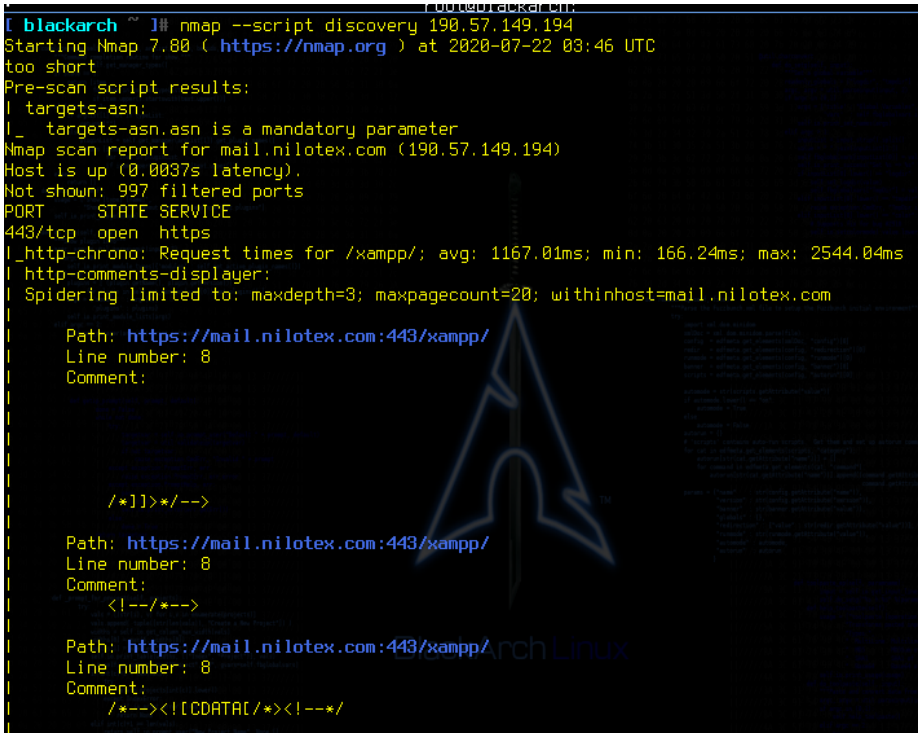

Ilustración 43. Nmap - Discovery - BlackArch (Yonfá, 2020)

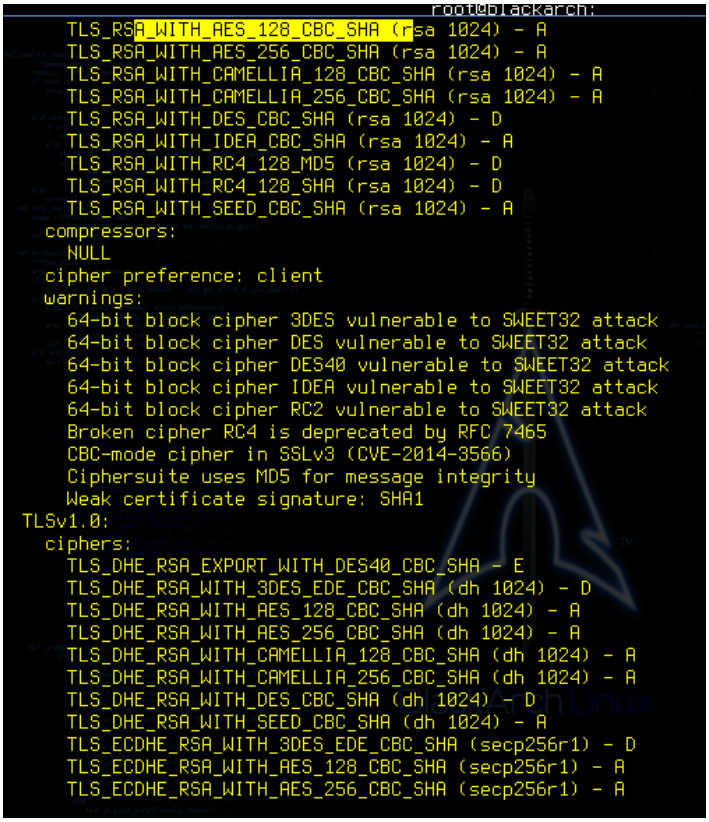

Ilustración 44. Nmap - Discovery - BlackArch (Yonfá, 2020)

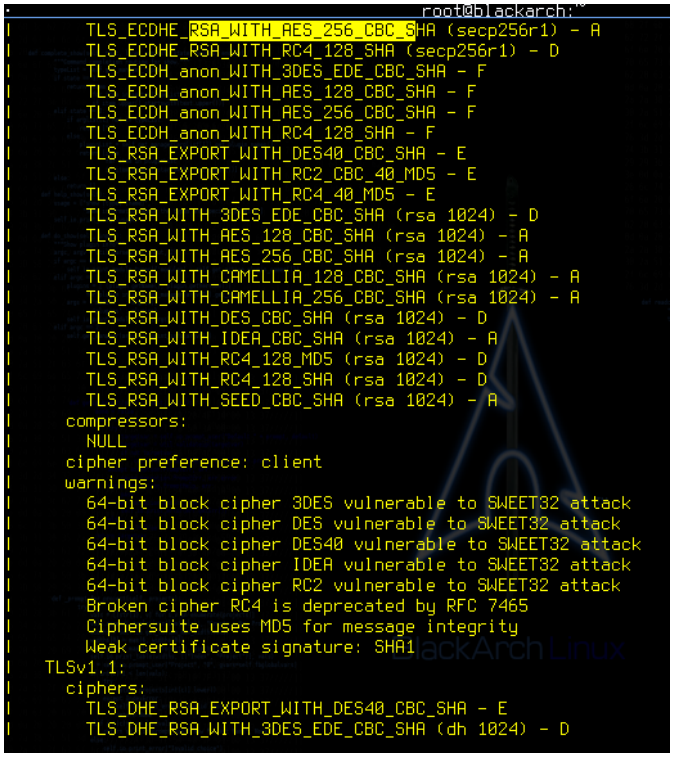

Ilustración 45. Nmap - Discovery - BlackArch (Yonfá, 2020)

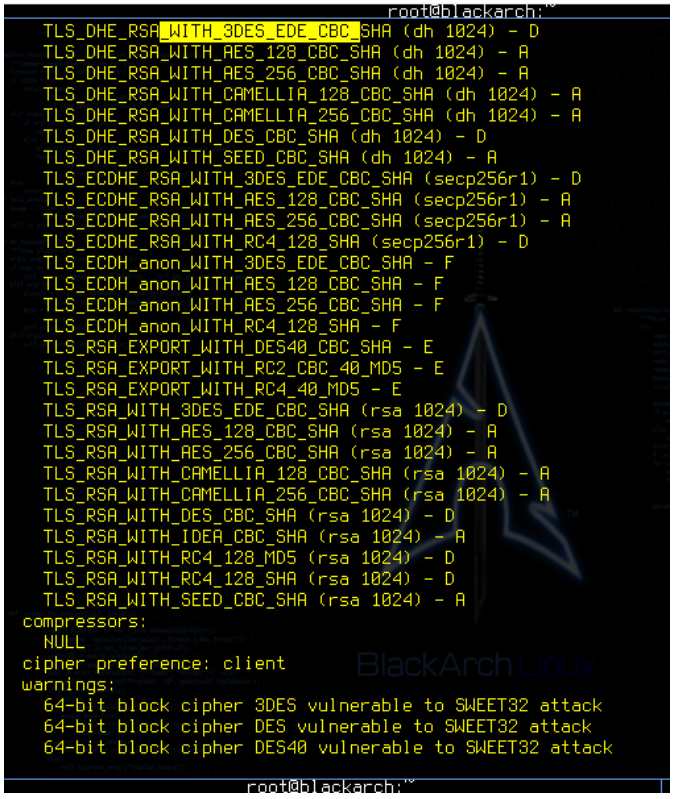

Ilustración 46. Nmap - Discovery - BlackArch (Yonfá, 2020)

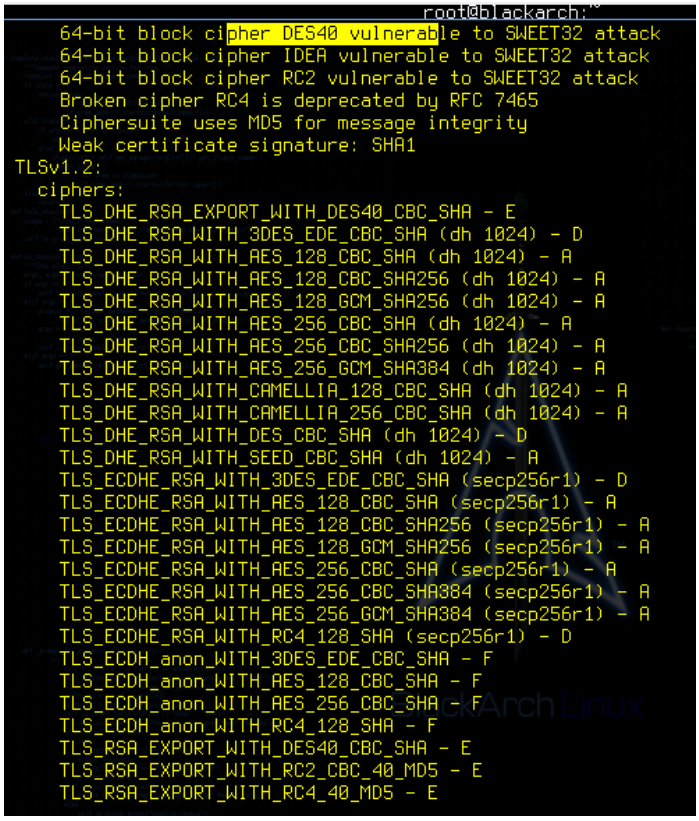

Ilustración 47. Nmap - Discovery - BlackArch (Yonfá, 2020)

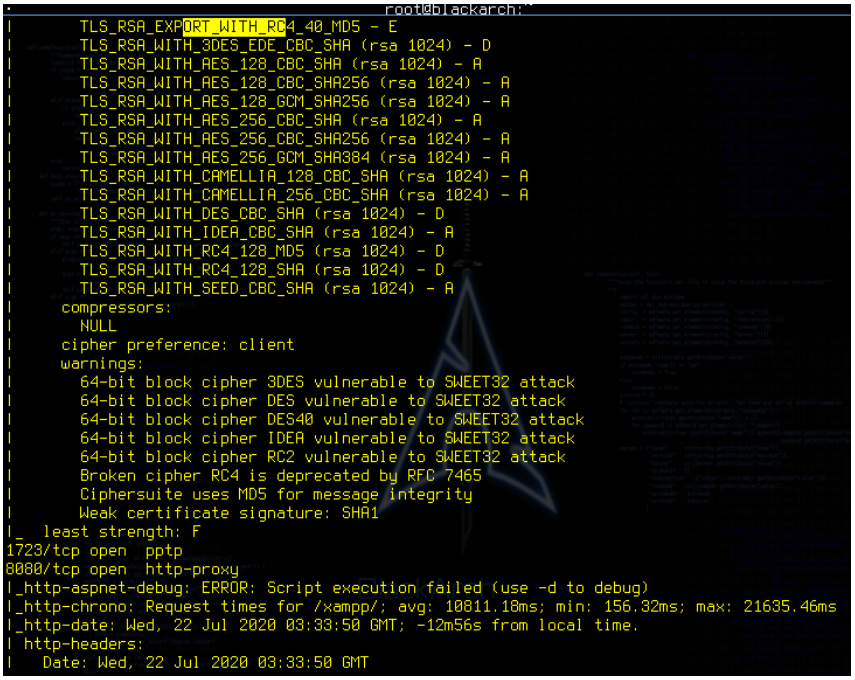

Ilustración 48. Nmap - Discovery - BlackArch (Yonfá, 2020)

Una vez terminado el escaneo utilizando el script Discovery con las tres herramientas podemos darnos cuenta de que presenta vulnerabilidades del tipo cifrado de bloque, más adelante se explicara y detallara las vulnerabilidades encontradas.

2.2.6.2.4. External

El script External utiliza recursos externos para su análisis, esto quiere decir que consulta datos a terceros, ya sea del propio sistema o del sistema objetivo. (ESET, 2015) (Leacock, 2019).

El script External ejecuta varios scripts a la vez con el fin de comprobar el acceso y el estado de los servicios que se ejecutan en el destino mediante el uso de servicios de prueba externos que incluyen detección de DNS, política HTTP entre dominios, búsquedas de bases de datos XSSed. Estos scripts involucran el tráfico de datos entre el equipo de escaneo y el cliente.

KALI LINUX – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script External.

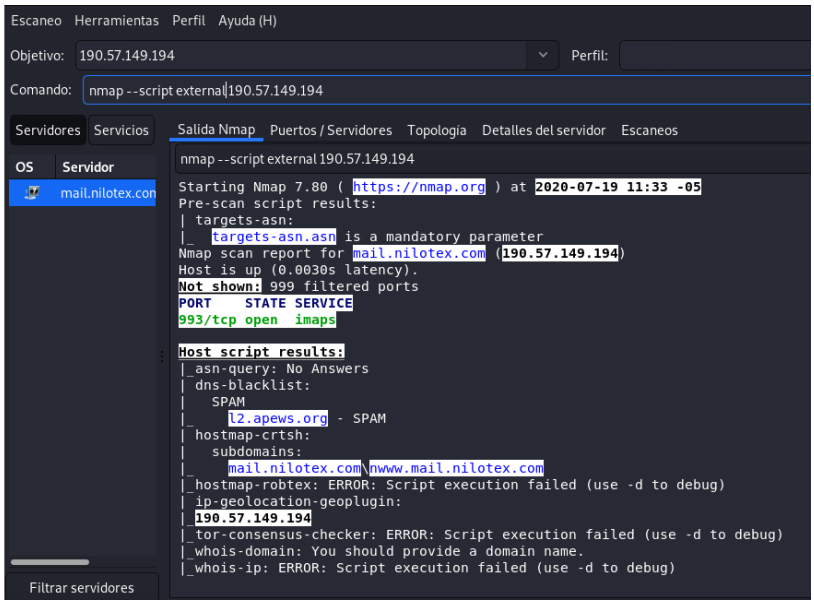

Ilustración 49. Zenmap - External - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script External.

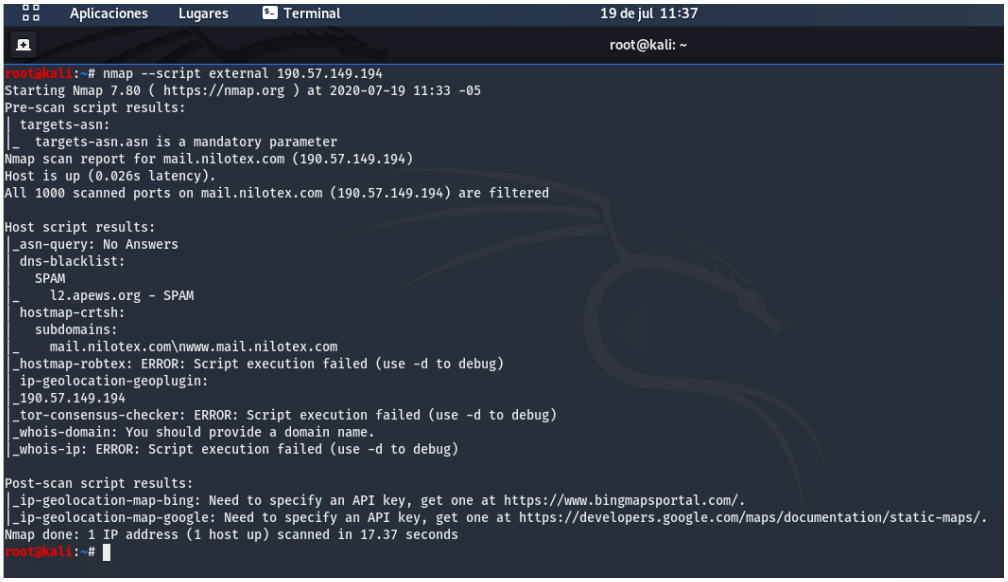

Ilustración 50.Nmap - External - Kali Linux (Yonfá, 2020).

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script External, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas

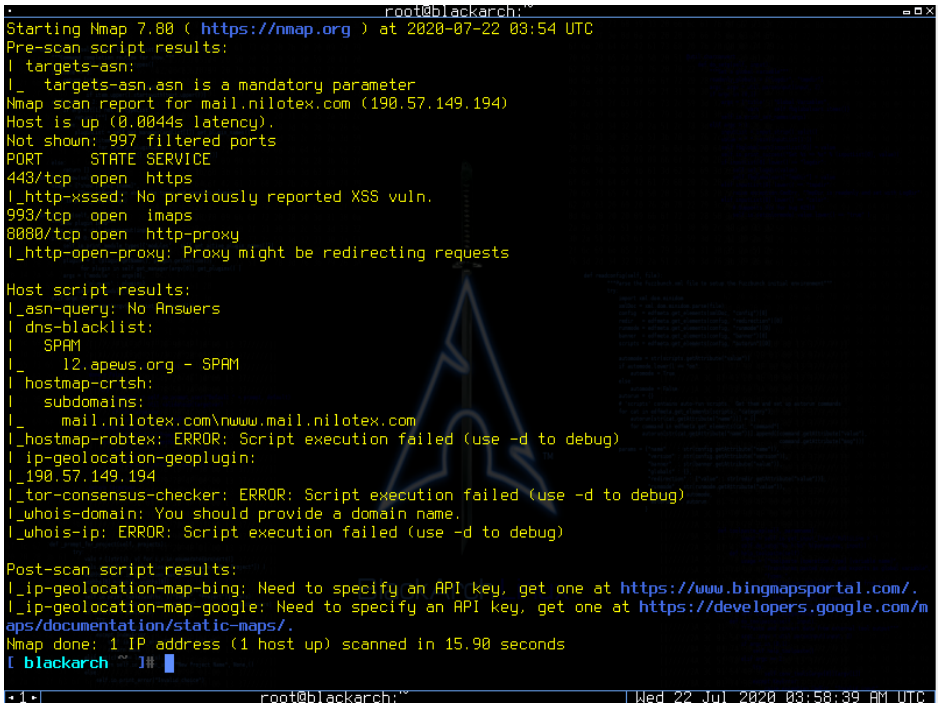

Ilustración 51. Nmap - External - BlackArch (Yonfá, 2020)

Después de terminar el escaneo con el script External podemos observar que no se encontraron vulnerabilidades en cuanto al script utilizado.

2.2.6.2.5. Intrusive

El script Intrusive utiliza varios recursos del sistema objetivo y puede dejar rastro de la intrusión. (ESET, 2015) (Leacock, 2019).

El script Intrusive es uno de los que contienen un riesgo alto de que pueda bloquear el sistema, ya que pueden ser percibidos como maliciosos. Este script puede intentar utilizar el servidor de destino como un proxy HTTP e intentar adivinar la cadena de comunidad SNMP.

KALI LINUX – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Intrusive.

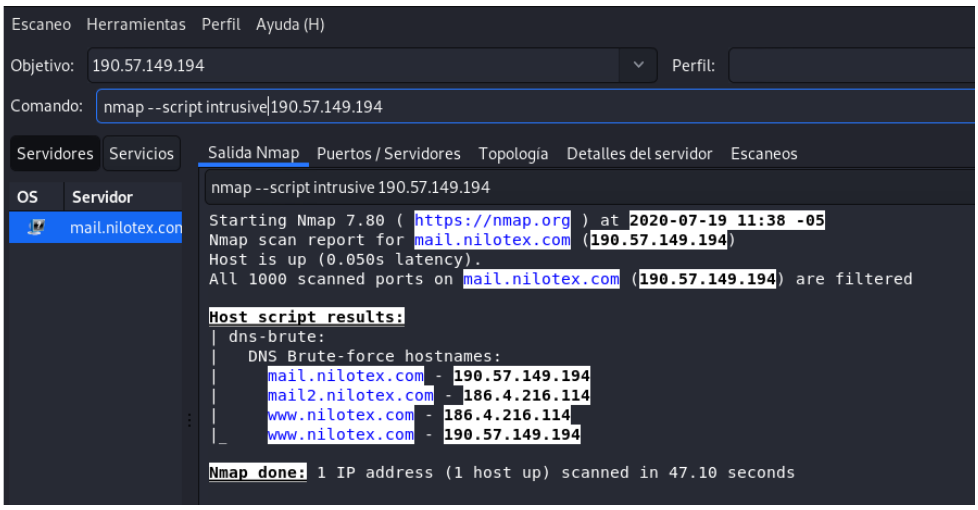

Ilustración 52. Zenmap - Intrusive - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Intrusive.

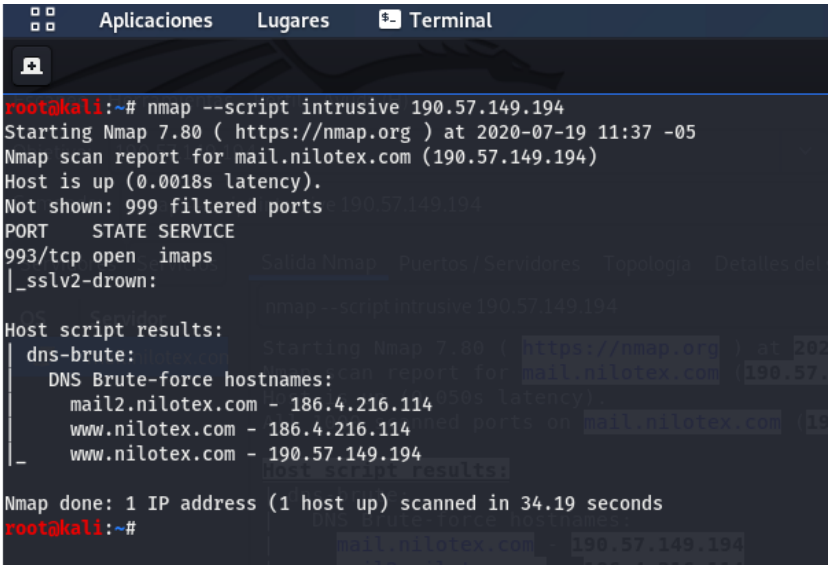

Ilustración 53. Nmap - Intrusive - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Intrusive, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas.

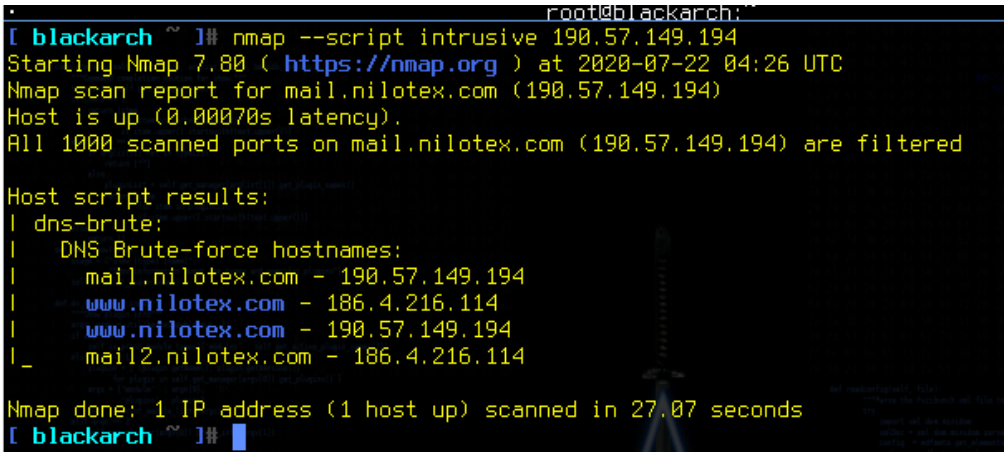

Ilustración 54. Nmap - Safe - BlackArch (Yonfá, 2020)

Una vez finalizada el escaneo con el script Intrusive los resultados obtenidos muestran que no se presentó ningún tipo de vulnerabilidad.

2.2.6.2.6. Malware

El script Malware revisa conexiones abiertas en puertas traseras (blackdoors) o por códigos maliciosos, comprueba si el sistema está infectado con algún malware. (ESET, 2015) (Leacock, 2019).

Este script Malware busca si el destino está infectado con algún malware o puerta trasera. Lo que busca el script es servidores SMPT que se ejecuten en puertos inusuales, busca demonios de suplantación de identidad que proporcione una respuesta falsa.

KALI LINUX – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Malware.

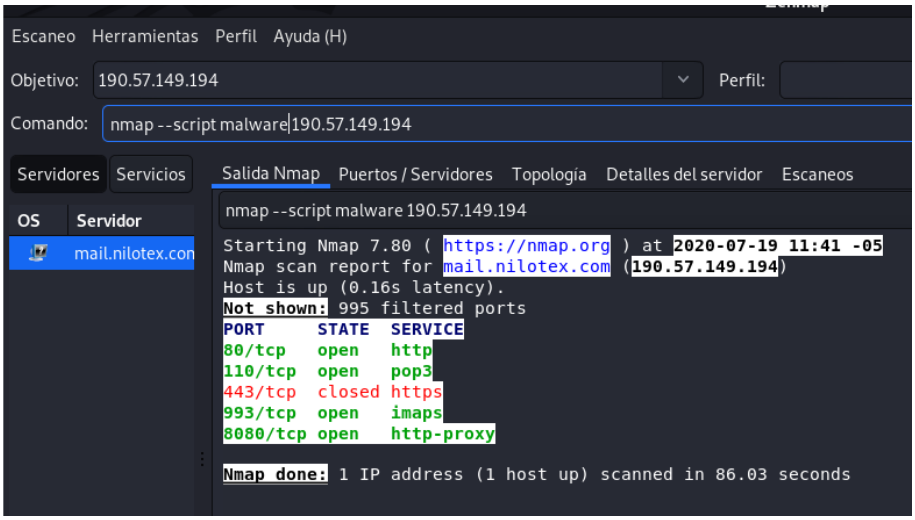

Ilustración 55. Zenmap - Malware - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Malware.

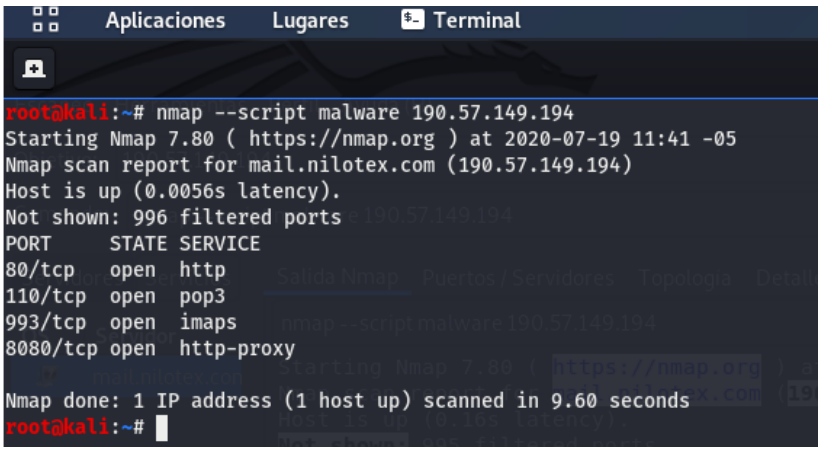

Ilustración 56. Nmap - Malware - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Malware, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas

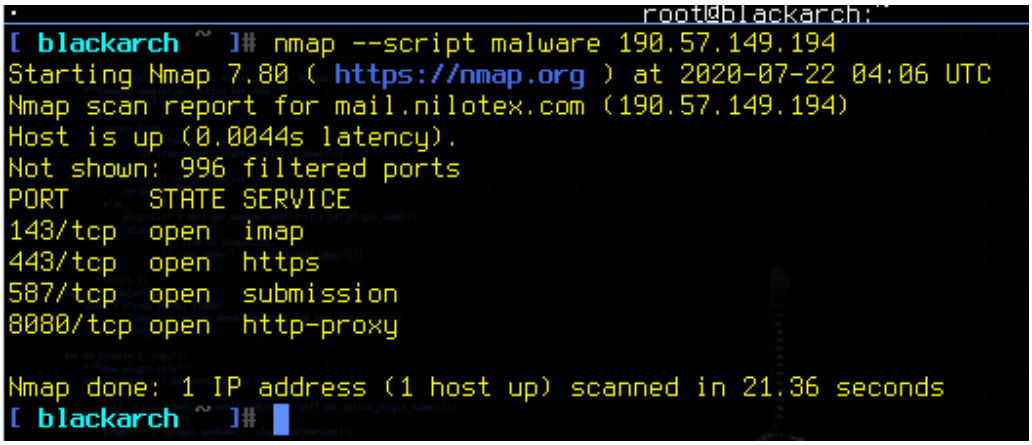

Ilustración 57. Nmap - Malware - BlackArch (Yonfá, 2020)

Una vez finalizada el escaneo con el script Malware los resultados obtenidos muestran que no se presentó ningún tipo de vulnerabilidad.

2.2.6.2.7. Safe

El script Safe ejecuta una serie de script que no son intrusivos, esto quiere decir que no generar logs o rastro en el sistema. (ESET, 2015) (Leacock, 2019).

El script Safe es menos intrusivo y casi indetectable, es utilizado para la enumeración de DNS, para la detección y recursividad de DHCP, búsqueda de índices HTTP, versiones de software, comprobaciones de reenvió de IP, recupera una clave de host SSH, entre otras más.

KALI LINUX – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Safe.

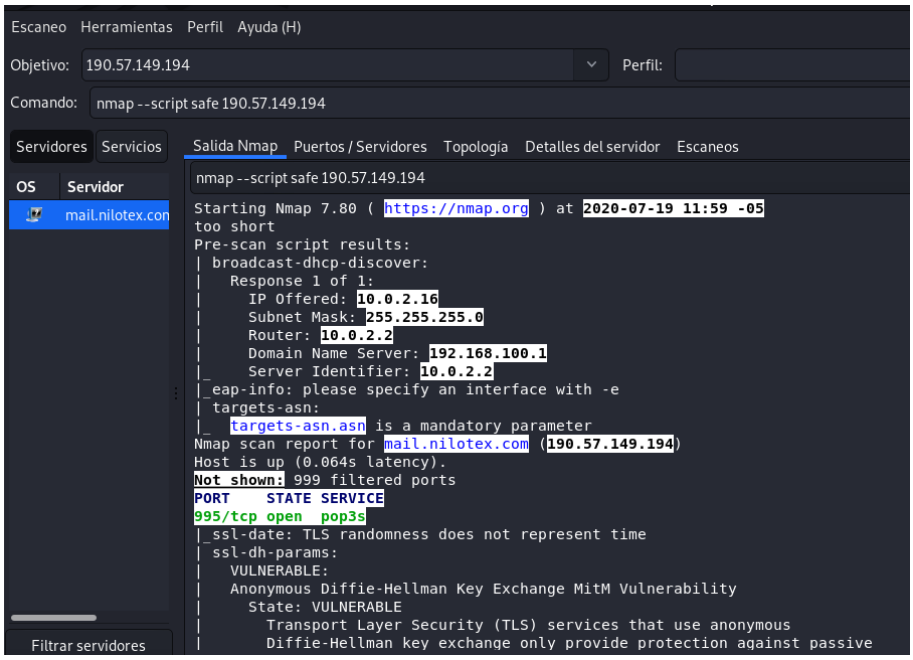

Ilustración 58. Zenmap - Safe - Kali Linux (Yonfá, 2020)

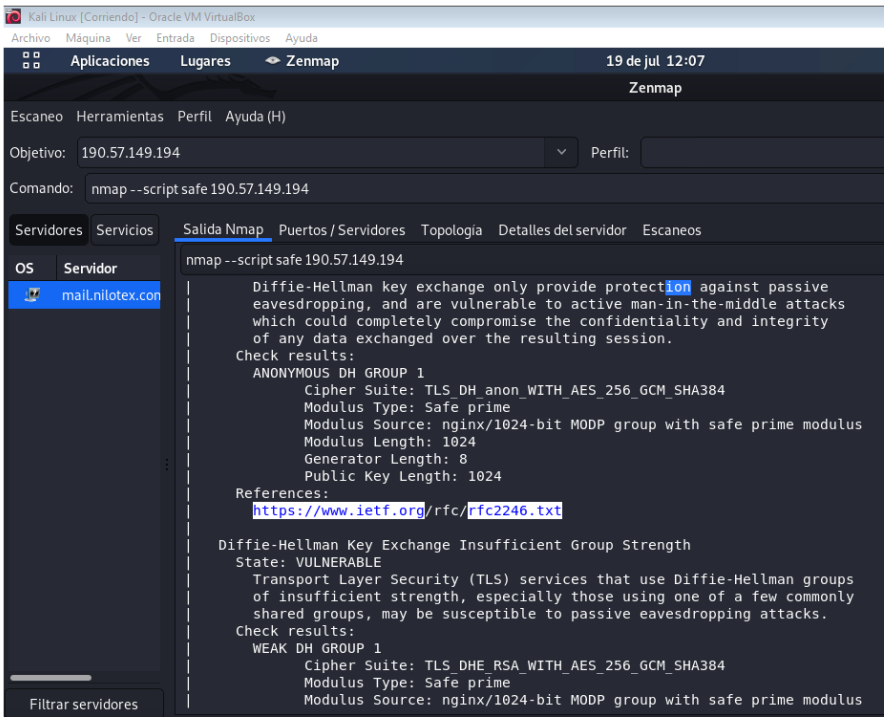

Ilustración 59. Zenmap - Safe - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Safe.

Ilustración 60. Nmap - Safe - Kali Linux (Yonfá, 2020)

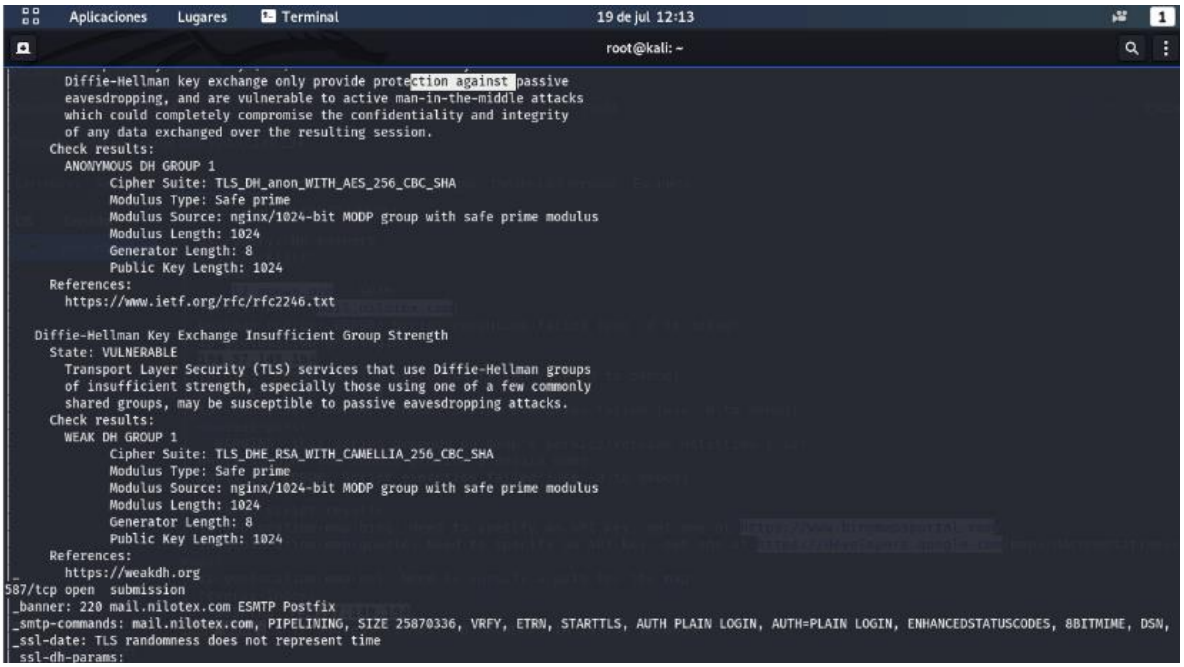

Ilustración 61. Nmap - Safe - Kali Linux (Yonfá, 2020)

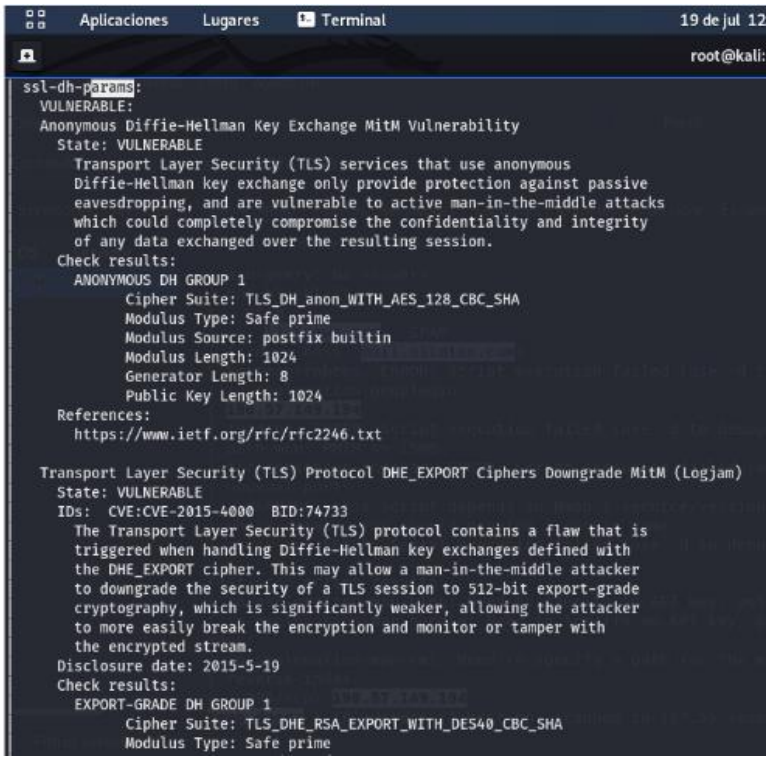

Ilustración 62. Nmap - Safe - Kali Linux (Yonfá, 2020)

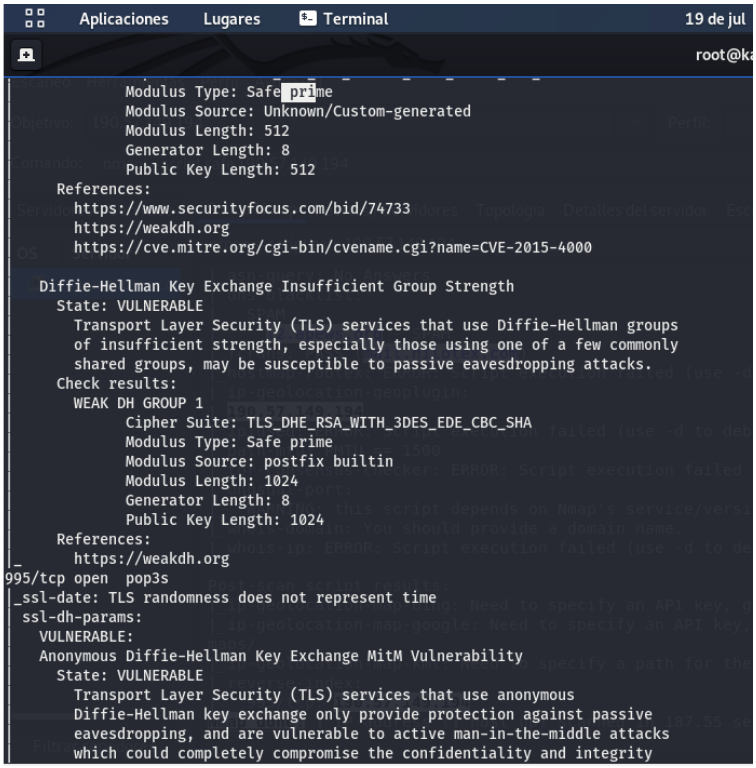

Ilustración 63. Nmap - Safe - Kali Linux (Yonfá, 2020)

Ilustración 64. Nmap - Safe - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Safe, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas.

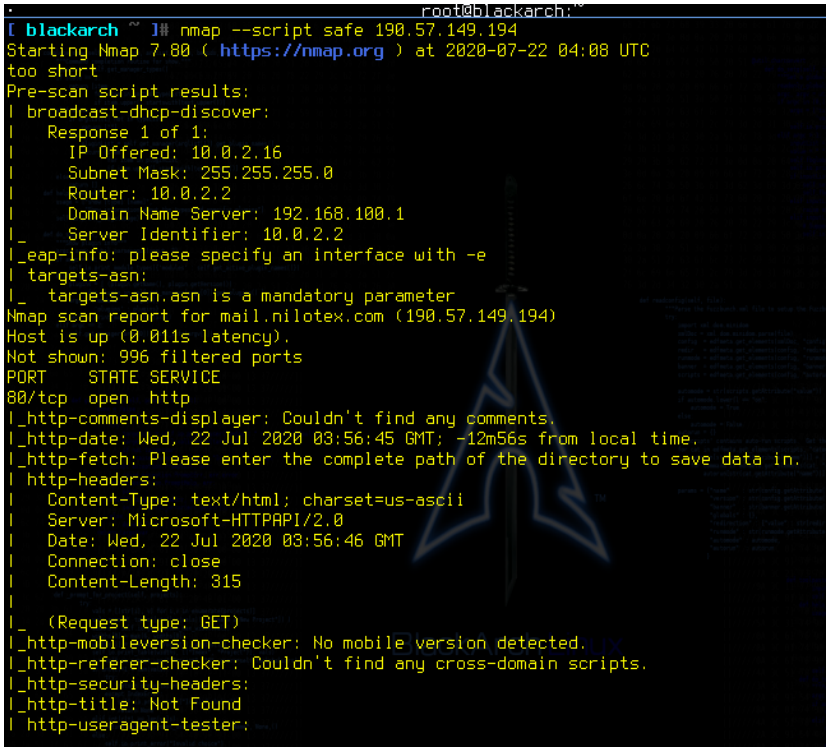

Ilustración 65. Nmap - Safe - BlackArch (Yonfá, 2020)

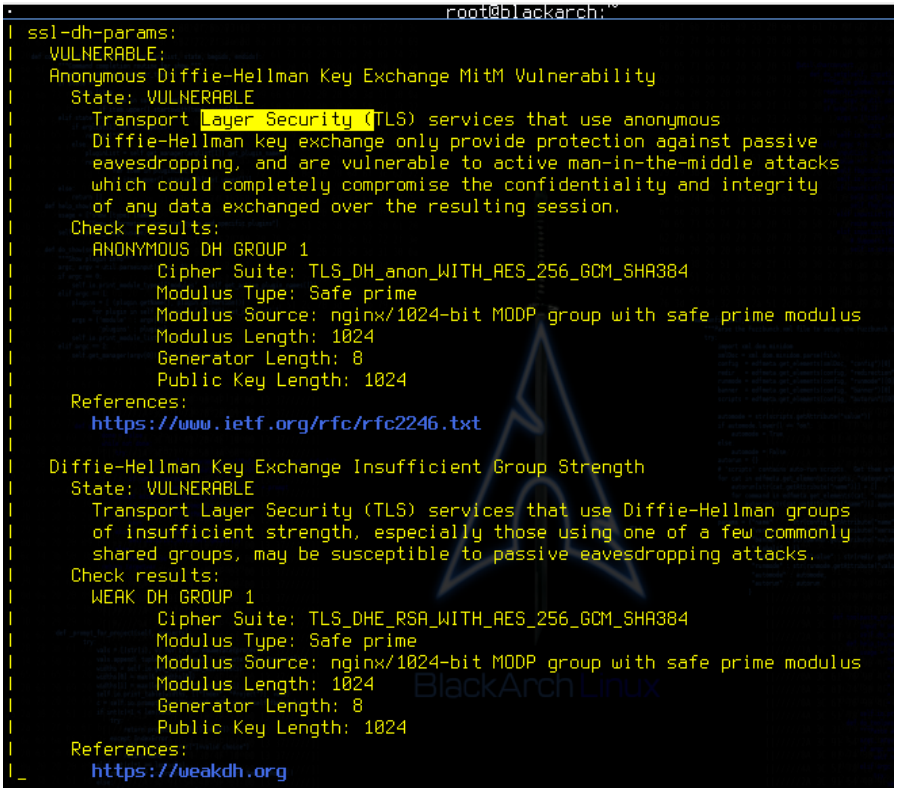

Ilustración 66. Nmap - Safe - BlackArch (Yonfá, 2020)

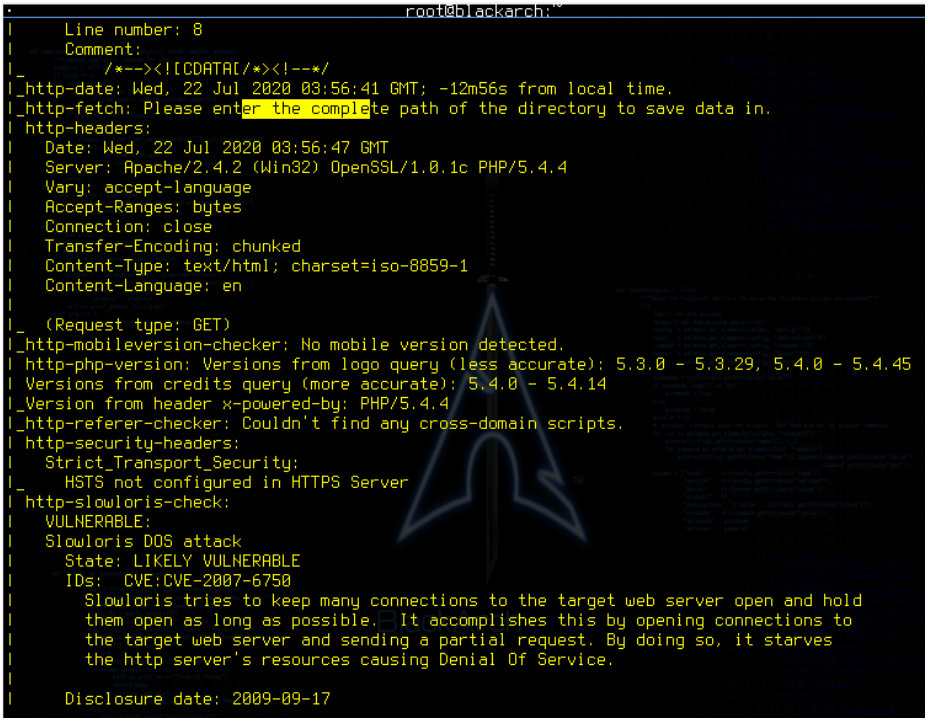

Ilustración 67. Nmap - Safe - BlackArch (Yonfá, 2020)

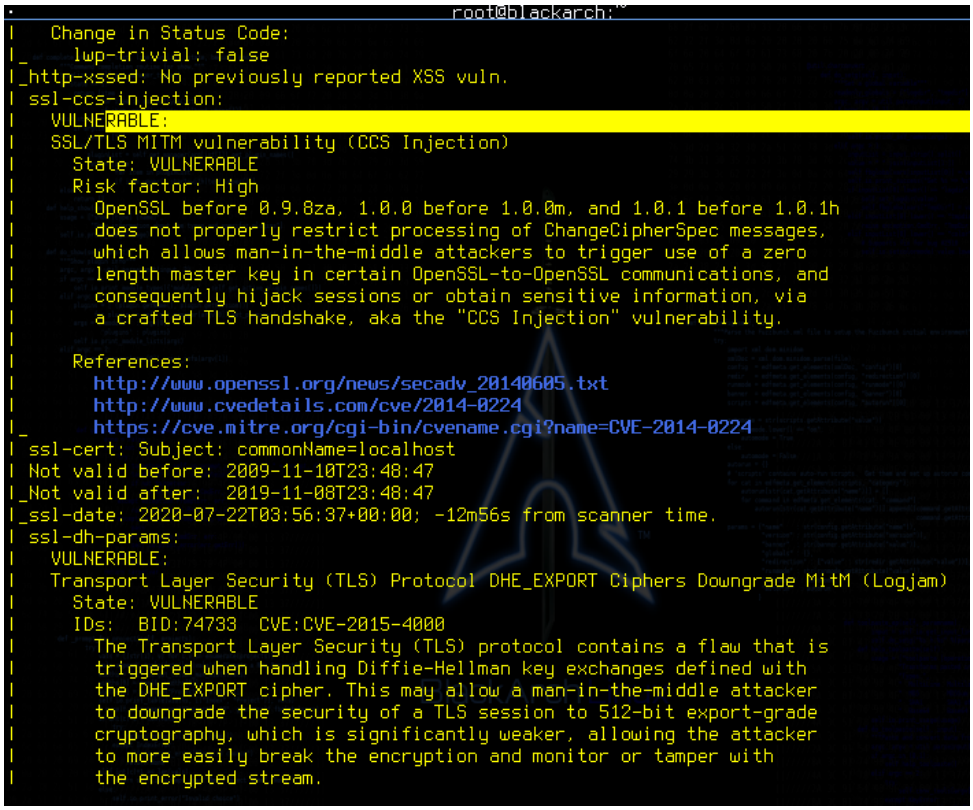

Ilustración 68. Nmap - Safe - BlackArch (Yonfá, 2020)

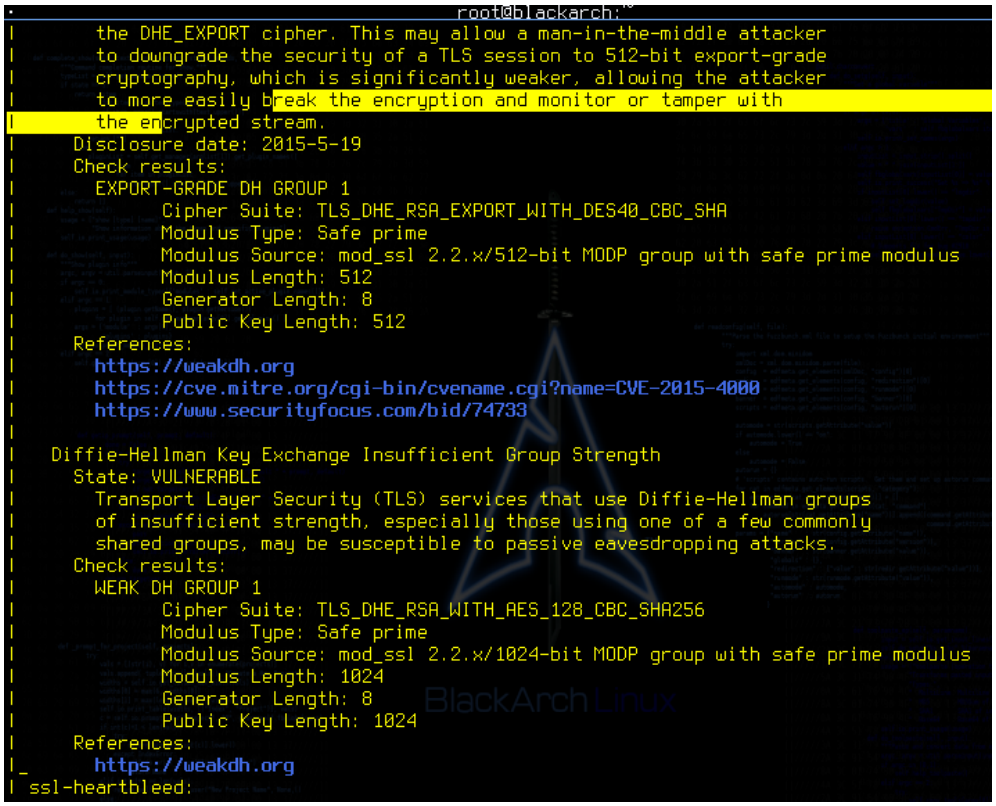

Ilustración 69. Nmap - Safe - BlackArch (Yonfá, 2020)

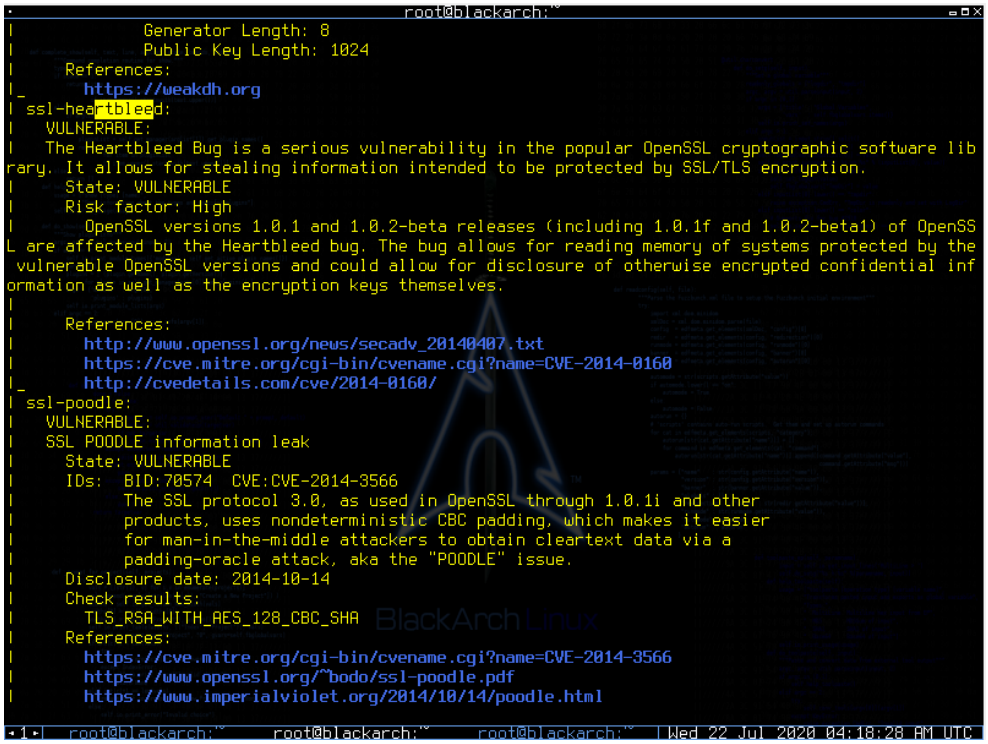

Ilustración 70. Nmap - Safe - BlackArch (Yonfá, 2020)

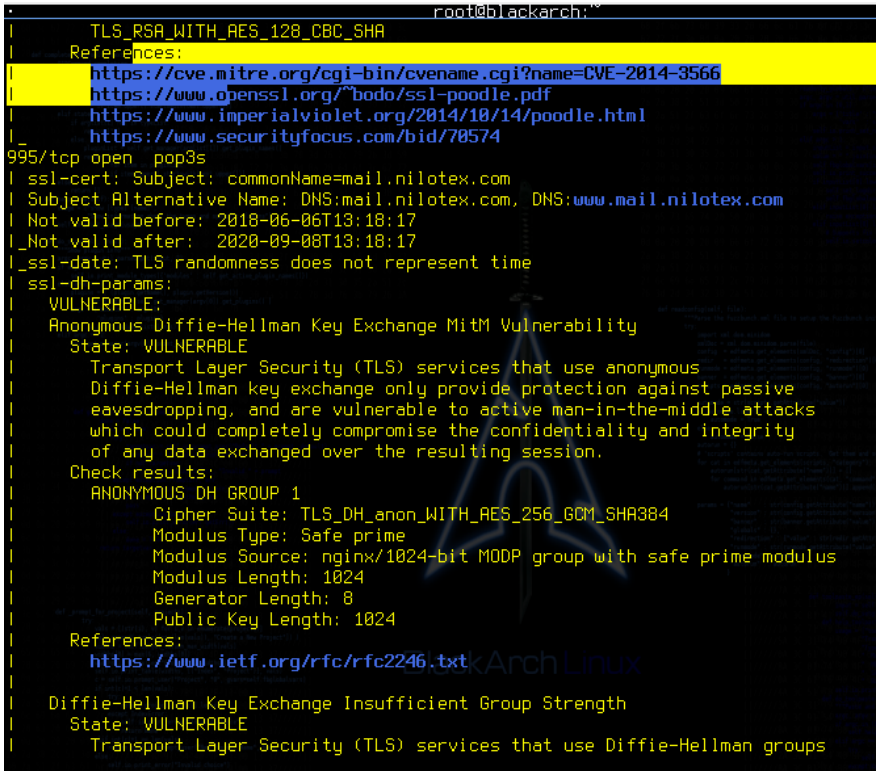

Ilustración 71. Nmap - Safe - BlackArch (Yonfá, 2020)

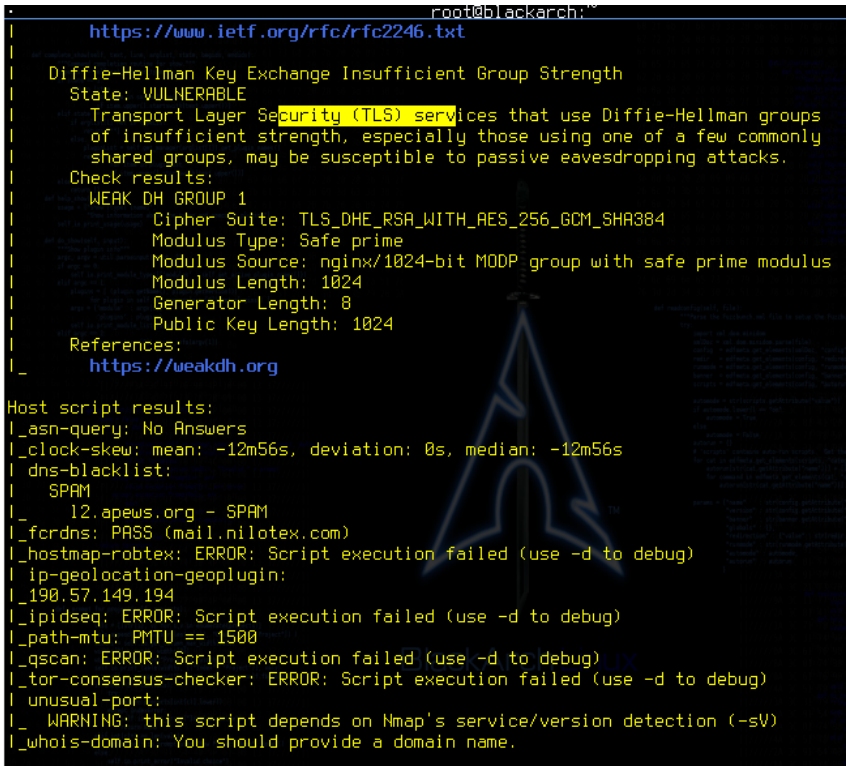

Ilustración 72. Nmap - Safe - BlackArch (Yonfá, 2020)

Una vez finalizada la exploración usando el script Safe podemos observar que el análisis arrojo algunas vulnerabilidades en cuanto a los protocolos y la encriptación de la información, más adelante se describirá cada vulnerabilidad para comprender su efecto.

2.2.6.2.8. Vuln

El script Vuln realiza un escaneo de las vulnerabilidades más conocidas, es muy utilizado para auditorias y futuras correcciones en los sistemas analizados. (ESET, 2015) (Leacock, 2019).

Este script busca las vulnerabilidades más comunes, en esta lista podemos encontrar vulnerabilidades del tipo HTTP slowloris, inicio de sesión anónimo, inyección SQL, rebote FPT, entre muchas más. Este script solo presenta los resultados si es que los encuentra, caso contrario no retorna nada.

KALI LINUX – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Vuln.

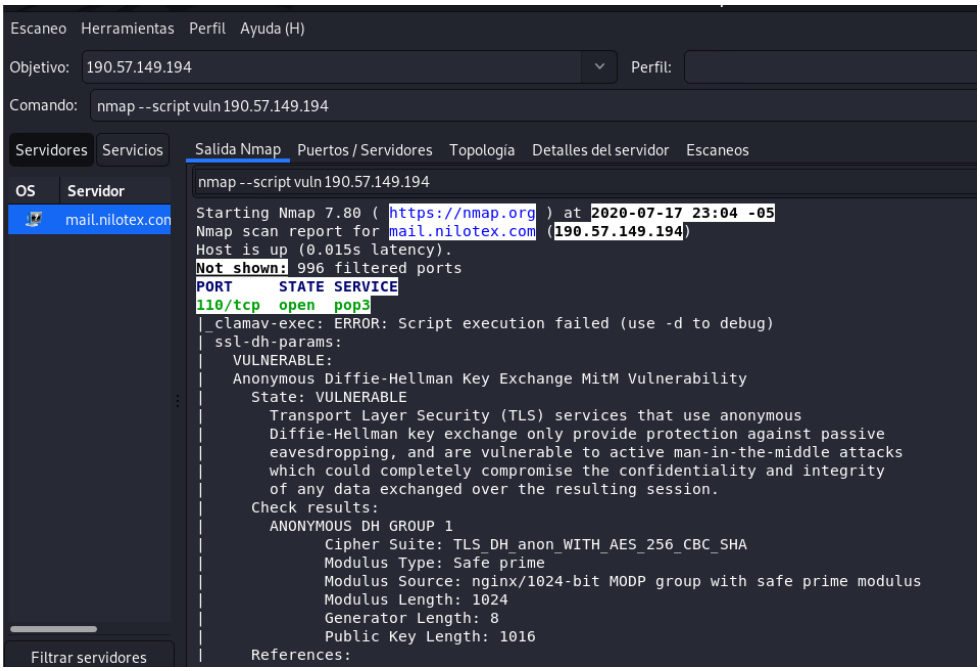

Ilustración 73. Zenmap - Vuln - Kali Linux (Yonfá, 2020)

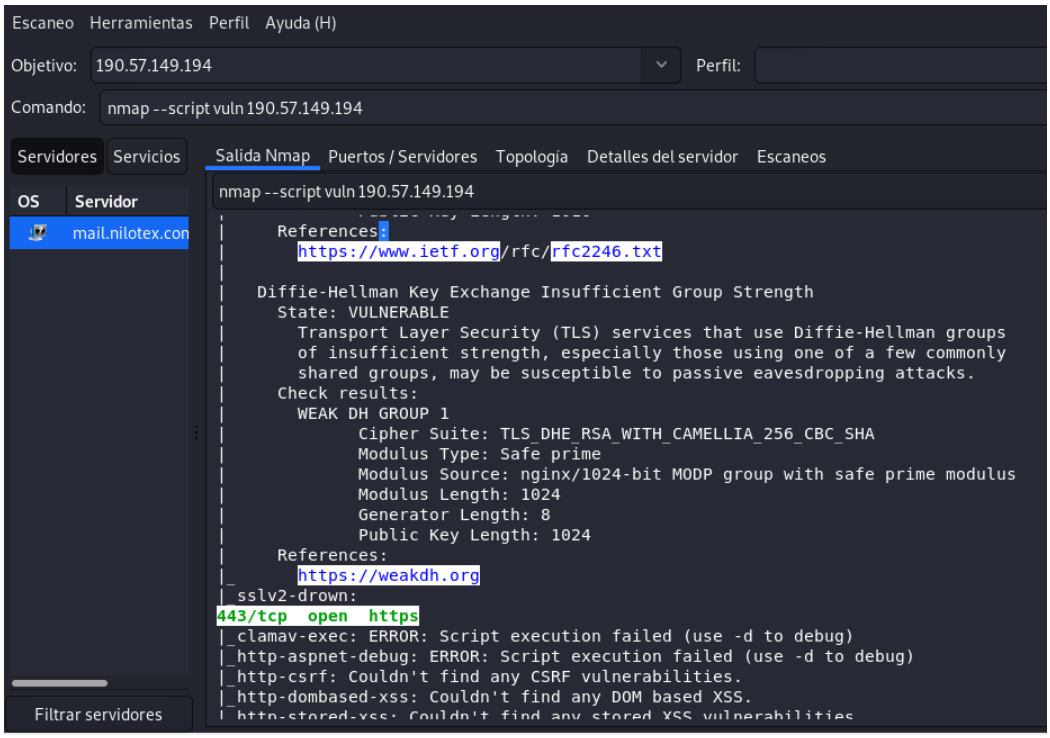

Ilustración 74. Zenmap - Vuln - Kali Linux (Yonfá, 2020)

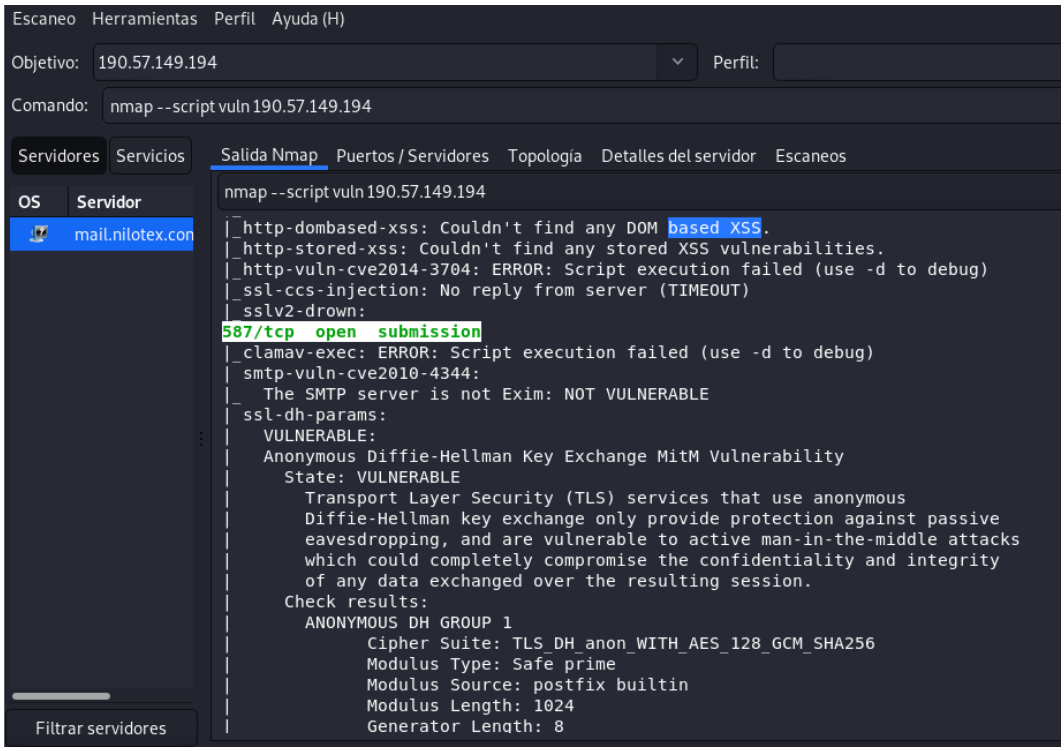

Ilustración 75. Zenmap - Vuln - Kali Linux (Yonfá, 2020)

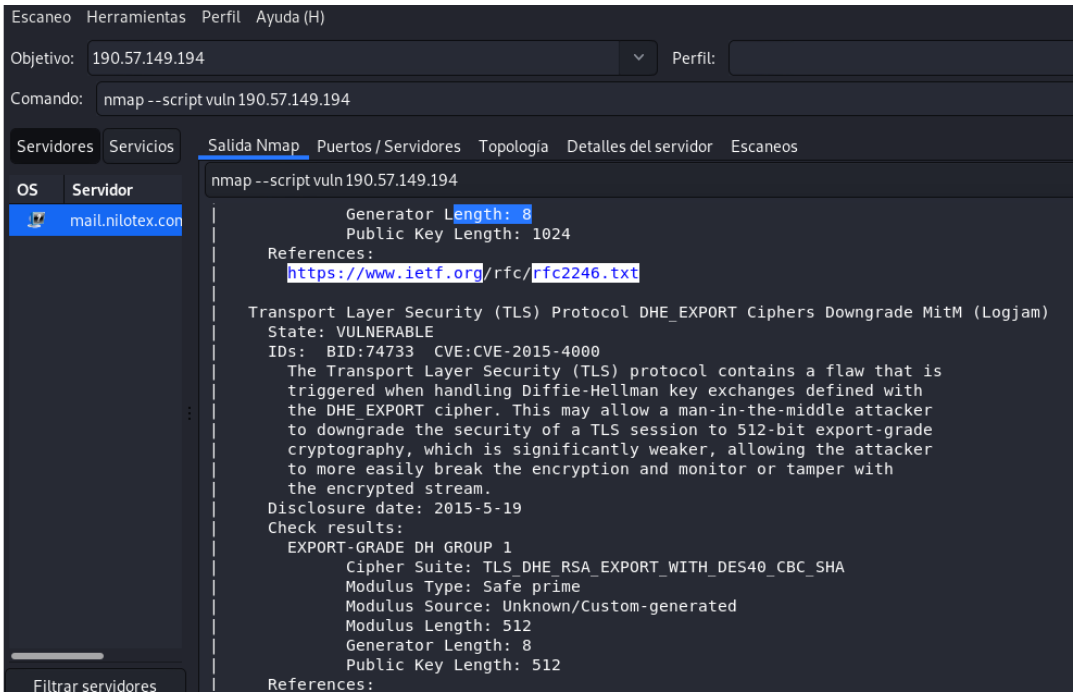

Ilustración 76. Zenmap - Vuln - Kali Linux (Yonfá, 2020)

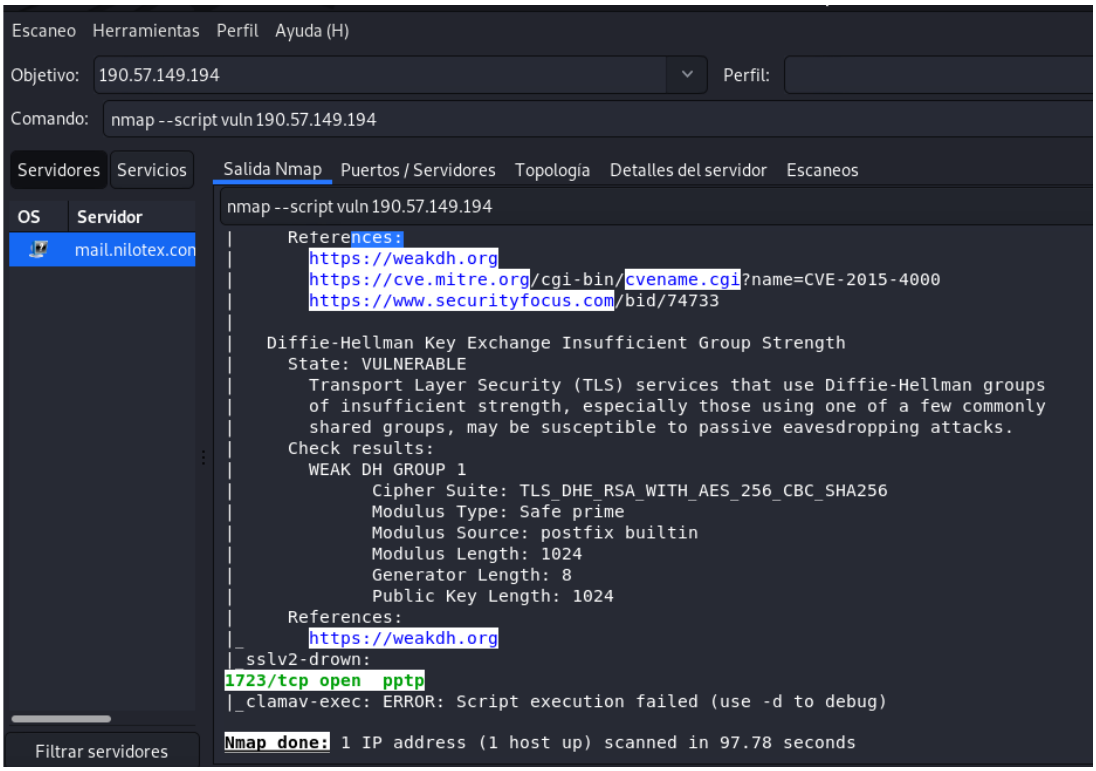

Ilustración 77. Zenmap - Vuln - Kali Linux (Yonfá, 2020)

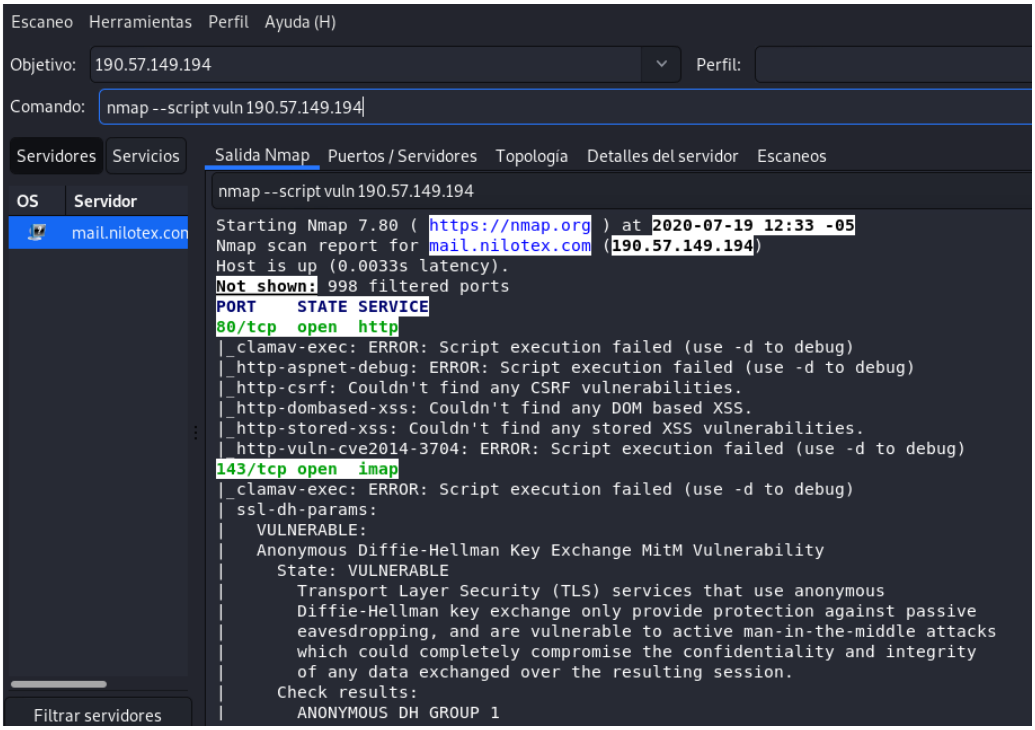

Ilustración 78. Zenmap - Vuln - Kali Linux (Yonfá, 2020)

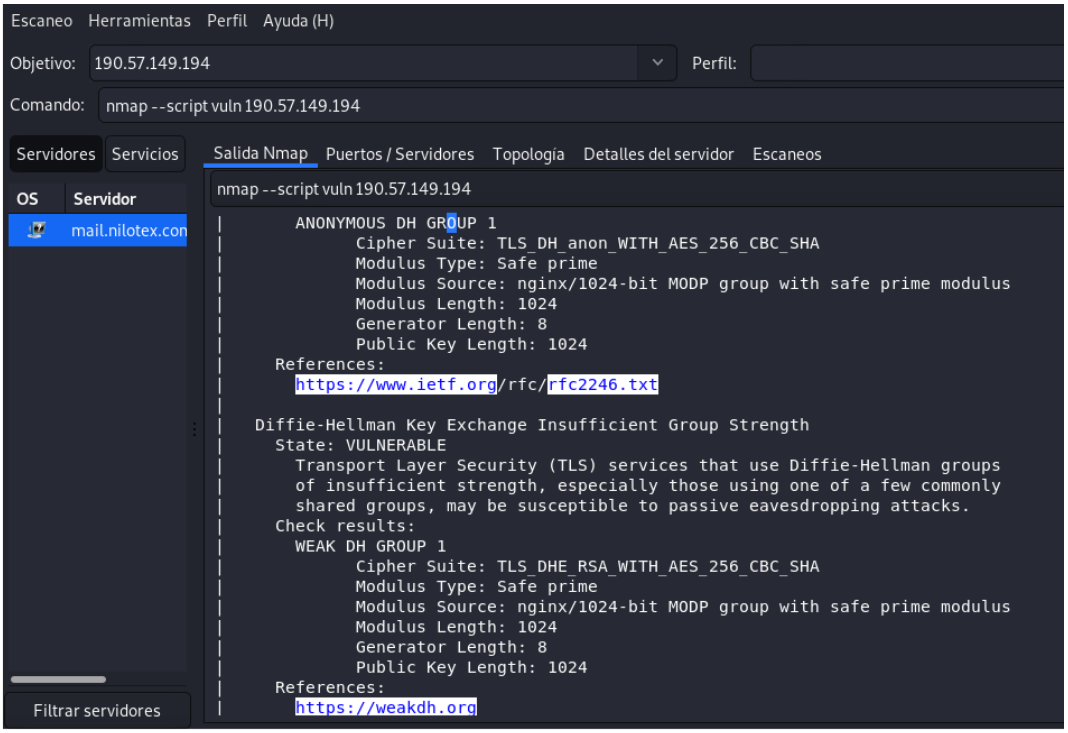

Ilustración 79. Zenmap - Vuln - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Vuln.

Ilustración 80. Nmap - Vuln - Kali Linux (Yonfá, 2020)

Ilustración 81. Nmap - Vuln - Kali Linux (Yonfá, 2020)

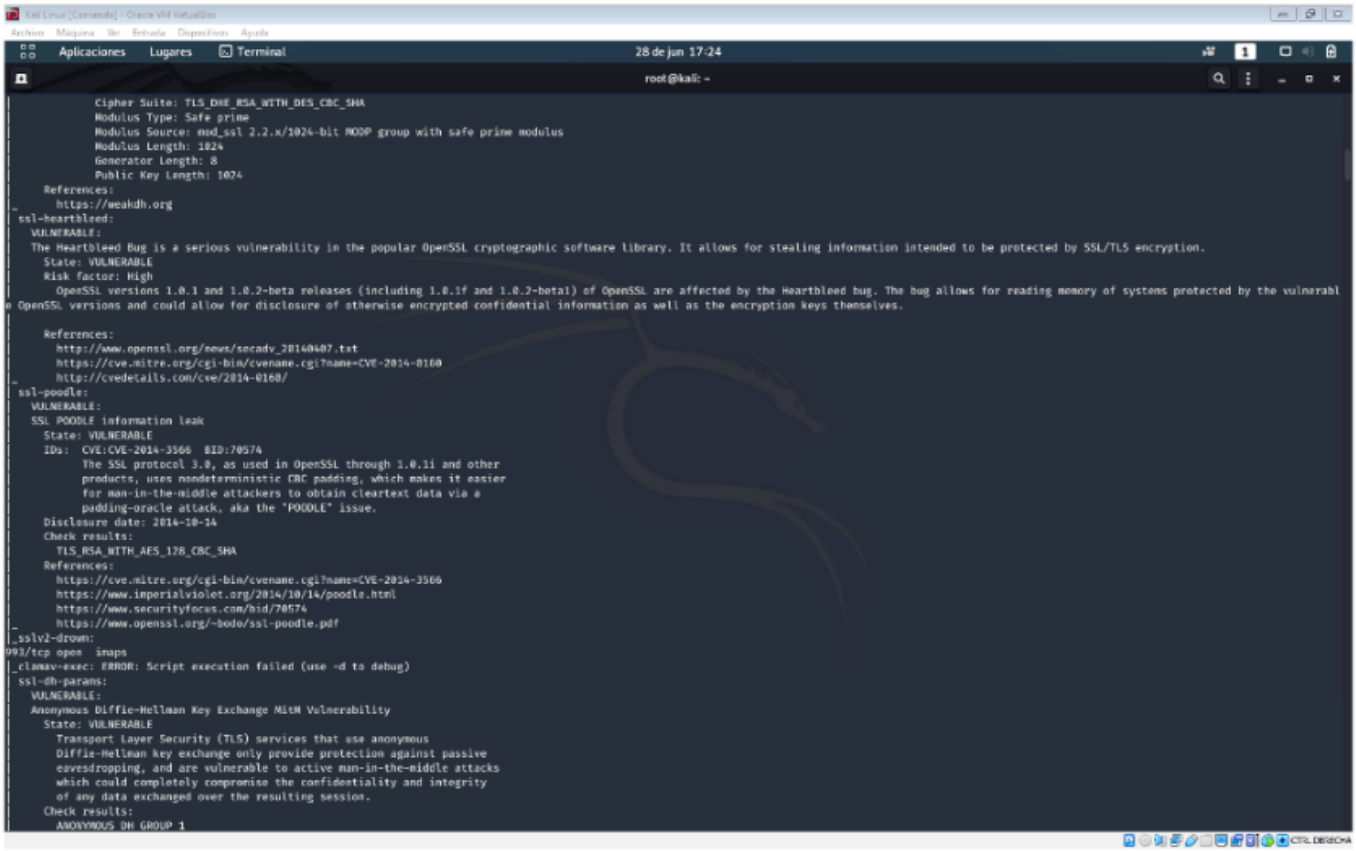

Ilustración 82. Nmap - Vuln - Kali Linux (Yonfá, 2020)

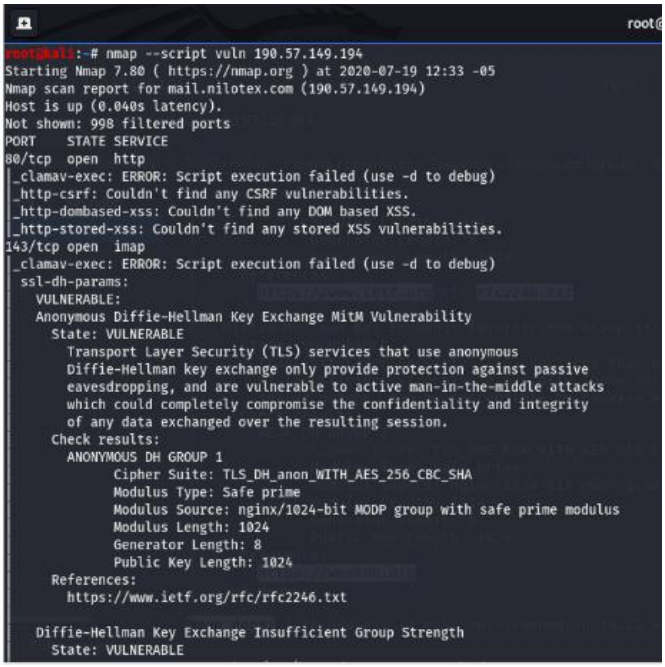

Ilustración 83. Nmap - Vuln - Kali Linux (Yonfá, 2020)

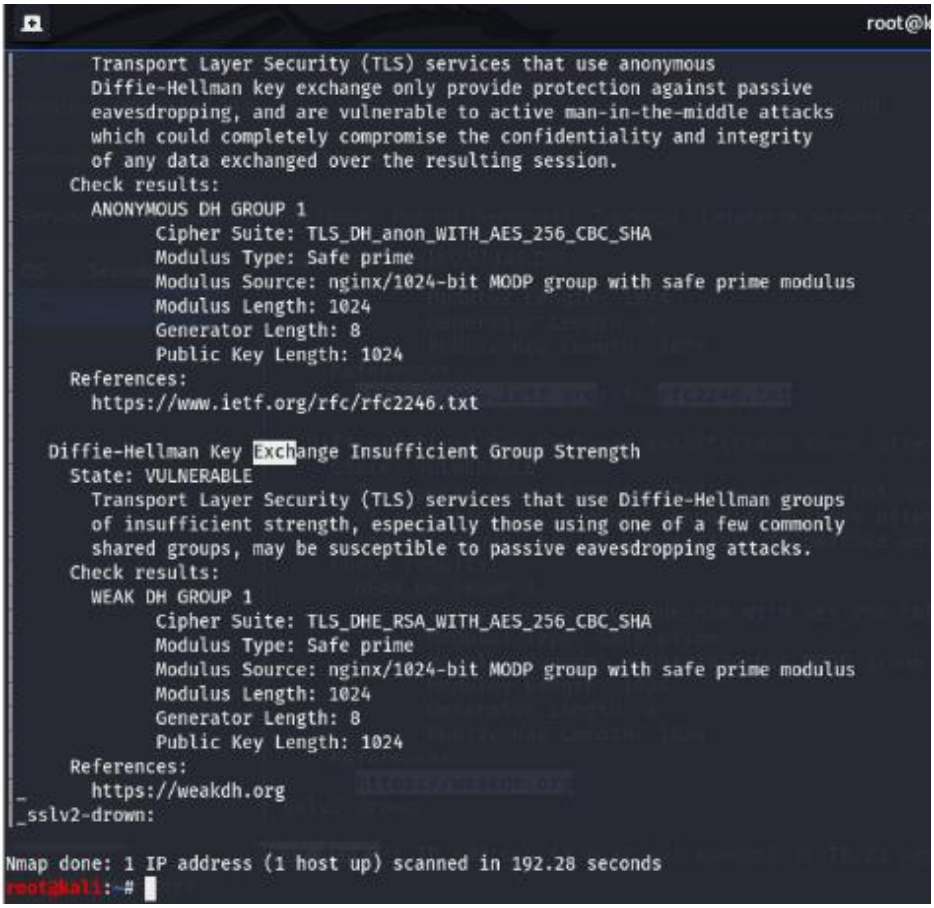

Ilustración 84. Nmap - Vuln - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Vuln, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas.

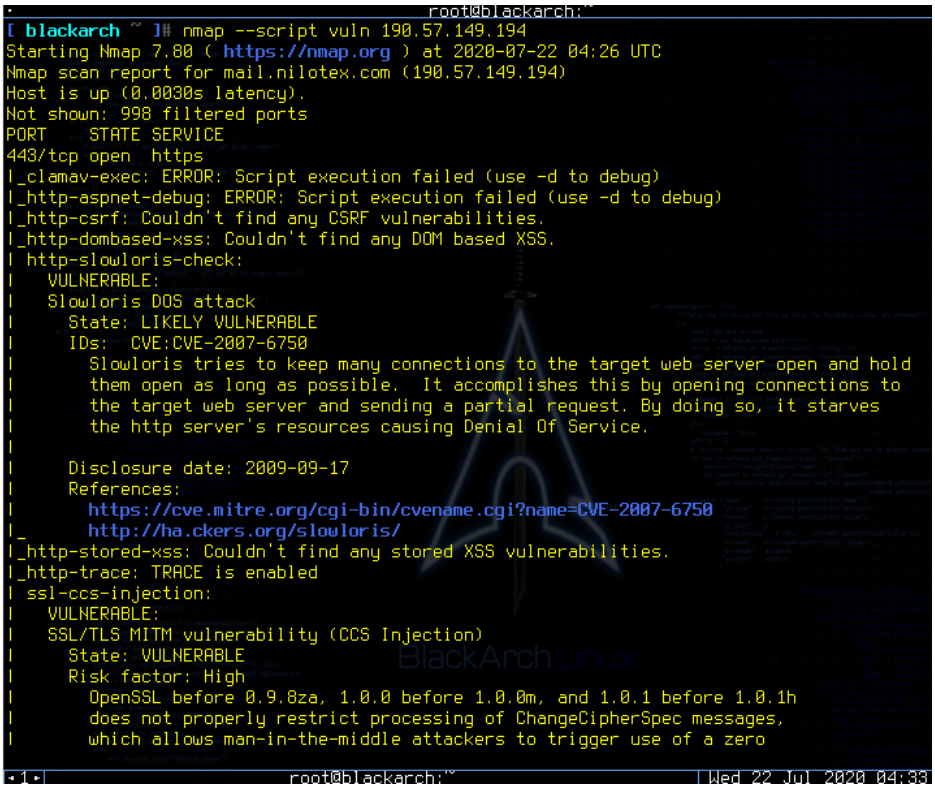

Ilustración 85. Nmap - Vuln - BlackArch (Yonfá, 2020)

Ilustración 86. Nmap - Vuln - BlackArch (Yonfá, 2020)

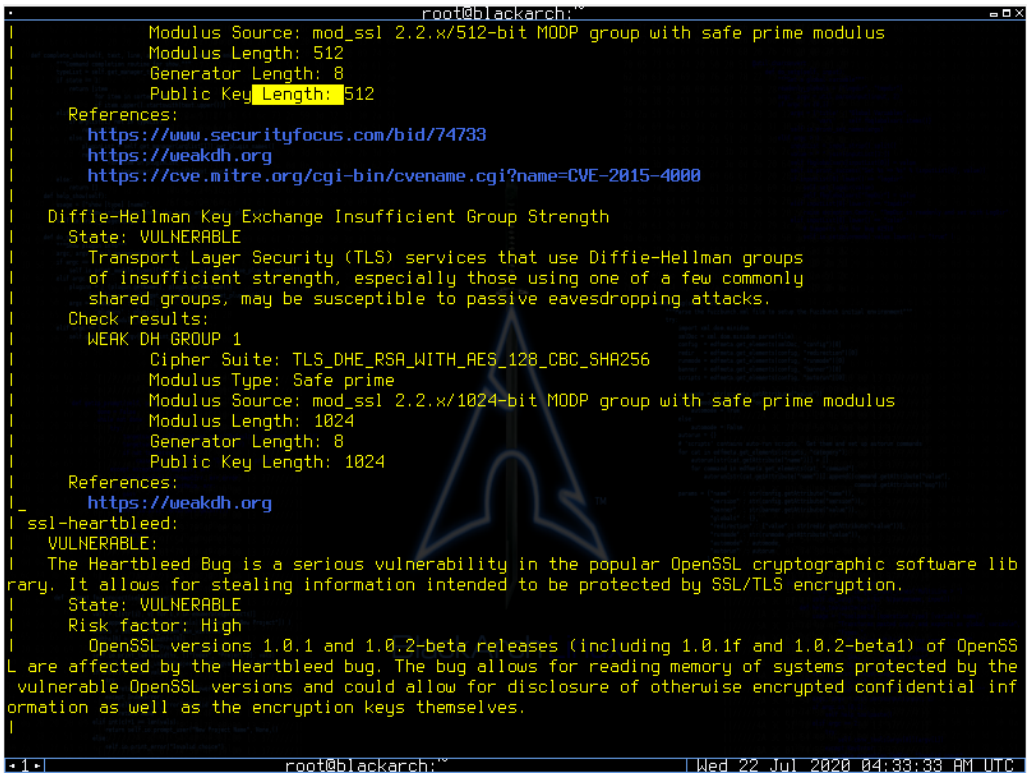

Ilustración 87. Nmap - Vuln - BlackArch (Yonfá, 2020)

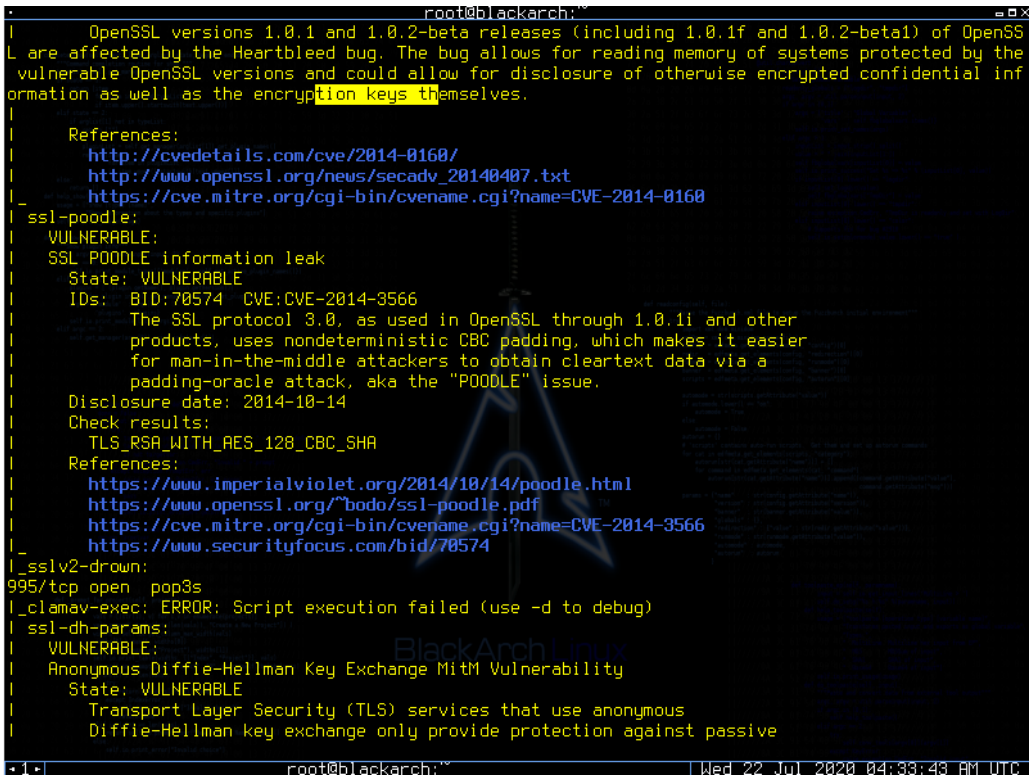

Ilustración 88. Nmap - Vuln - BlackArch (Yonfá, 2020)

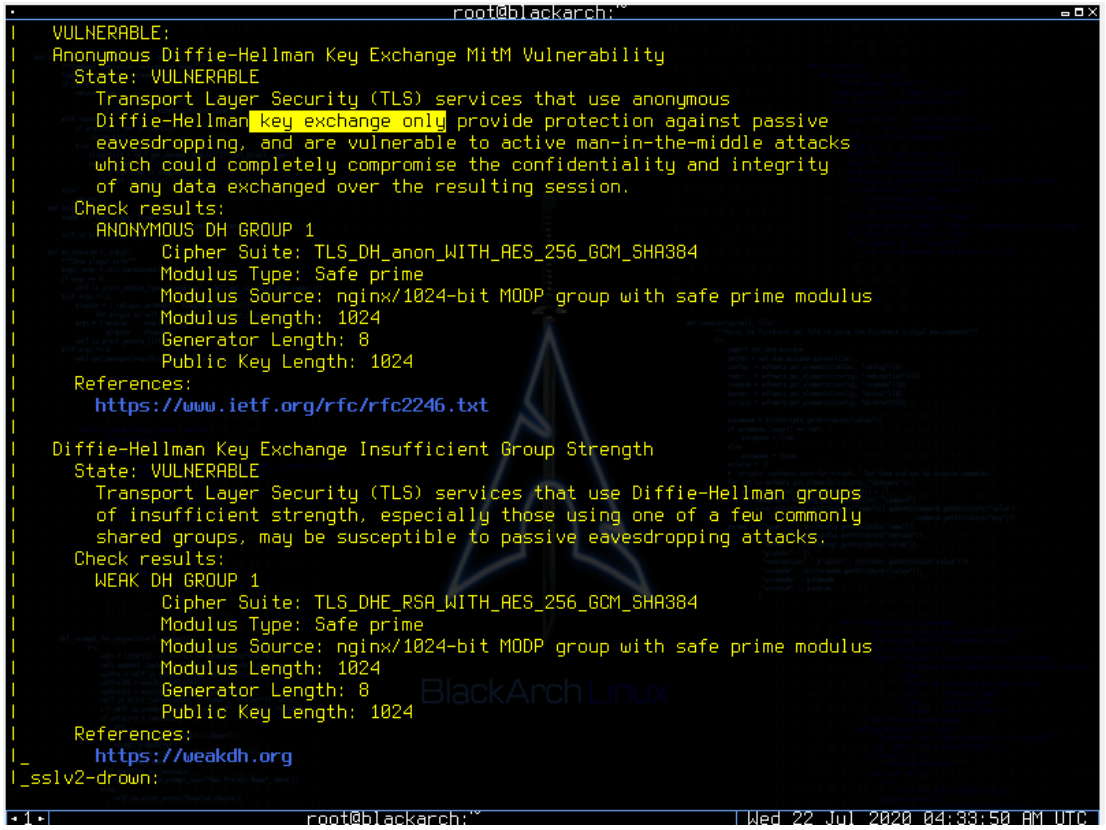

Ilustración 89. Nmap - Vuln - BlackArch (Yonfá, 2020)

Una vez finalizado el escaneo con el script Vuln podemos darnos cuenta de que existen algunas vulnerabilidades en los puertos abiertos de la red de la empresa, estas vulnerabilidades se explican más adelante en el trabajo, para poder conocer de qué se trata, su efecto y posible solución.

2.2.6.2.9. Exploit

El script Exploit es utilizada para explotar las vulnerabilidades que se encuentran en el sistema. (Leacock, 2019).

El script Exploit busca explotar las vulnerabilidades que detecta normalmente busca las vulnerabilidades que aparecen en la mayoría de las noticias de seguridad y aparecen varios cada día.

KALI LINUX – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Exploit.

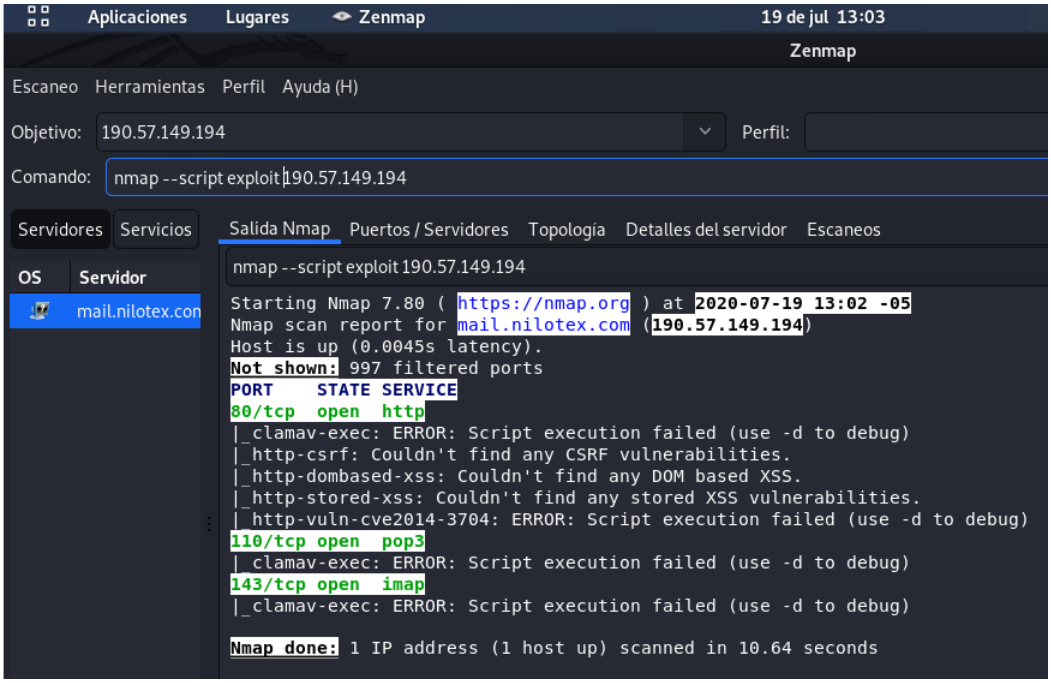

Ilustración 90. Zenmap - Exploit - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Exploit.

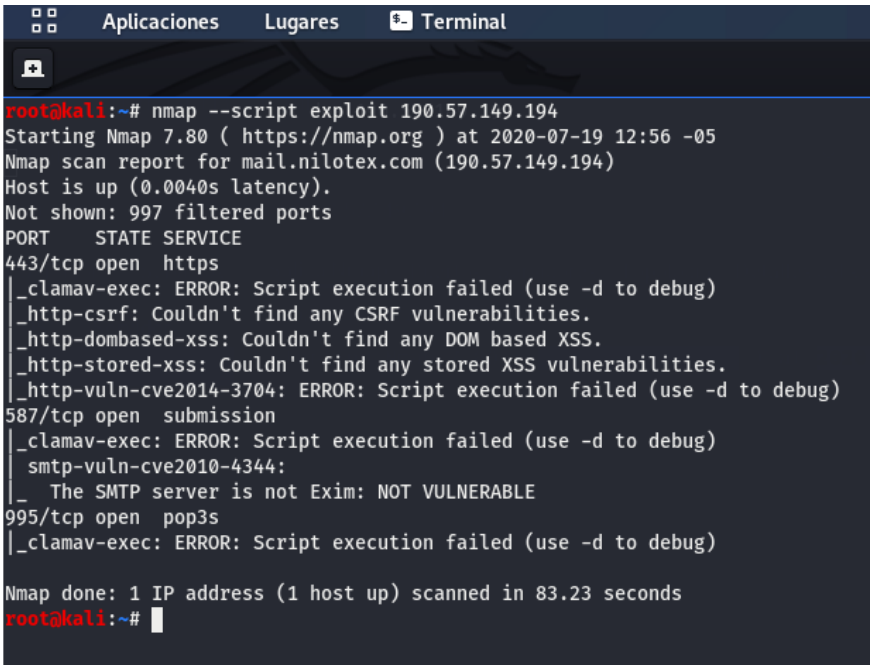

Ilustración 91. Nmap - Exploit - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Exploit, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas.

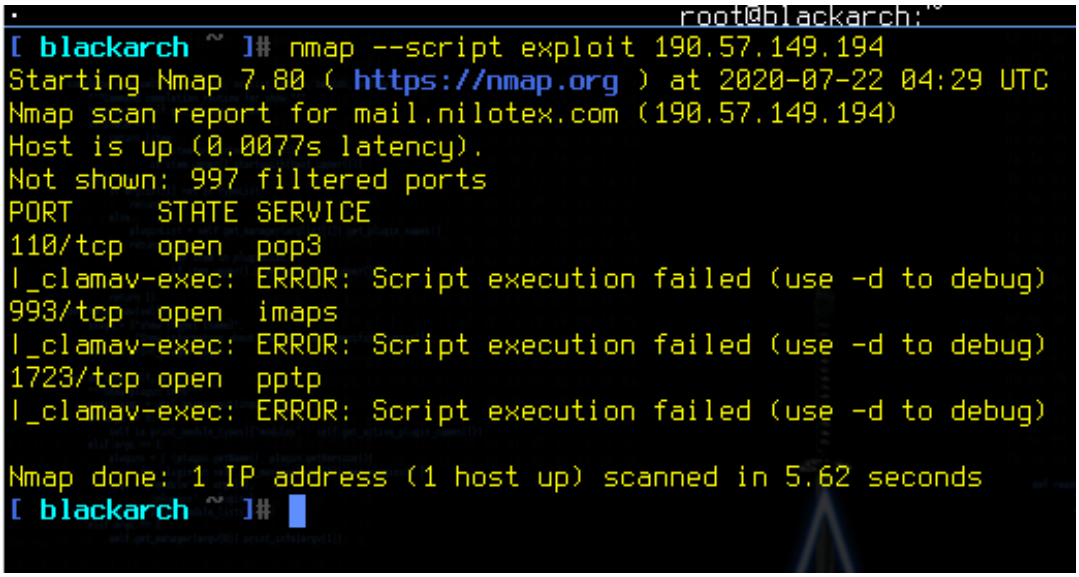

Ilustración 92. Nmap - Exploit - BlackArch (Yonfá, 2020)

Luego de finalizar el análisis con el script Exploit, los resultados arrojados indican que no se presentaron vulnerabilidades con la ejecución de dicho script.

2.2.6.2.10. Version

El script versión detecta versiones de los servicios con los que cuenta el sistema. (Leacock, 2019) (adastra, 2011).

El script Version como su nombre lo indica busca versiones en los sistemas de la red escanea, de esta forma podemos darnos cuenta si un sistema cuenta con una versión no actualizada y poder explotar esa falla en el sistema.

KALI LINUX – ZENMAP

Continuando con el uso de la herramienta Zenmap utilizamos el script Version.

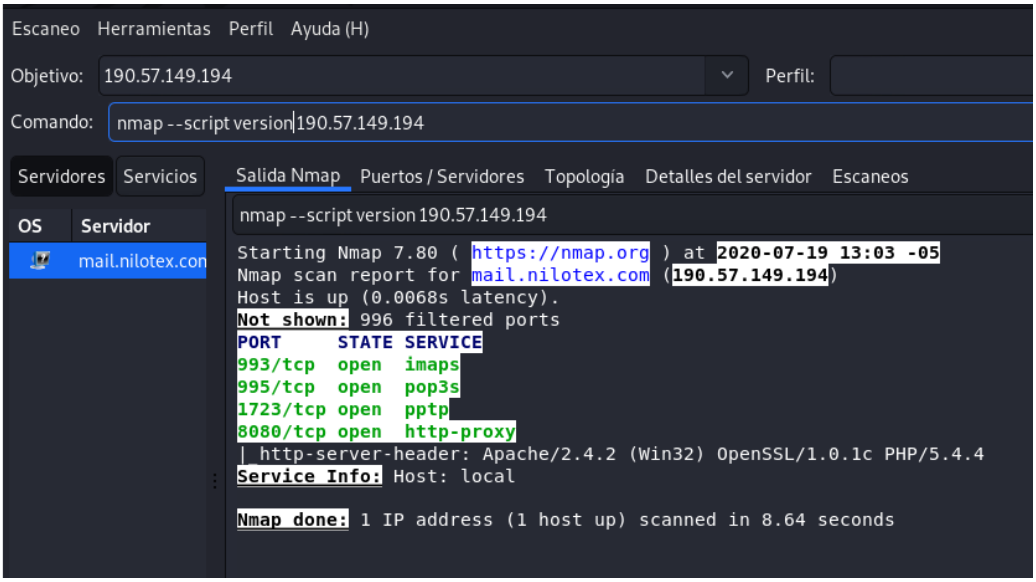

Ilustración 93. Zenmap - Version - Kali Linux (Yonfá, 2020)

KALI LINUX - TERMINAL – LINEA DE COMANDOS

Continuando con el análisis utilizaremos la terminal de Kali Linux para ver los resultados que me arroja el script Version.

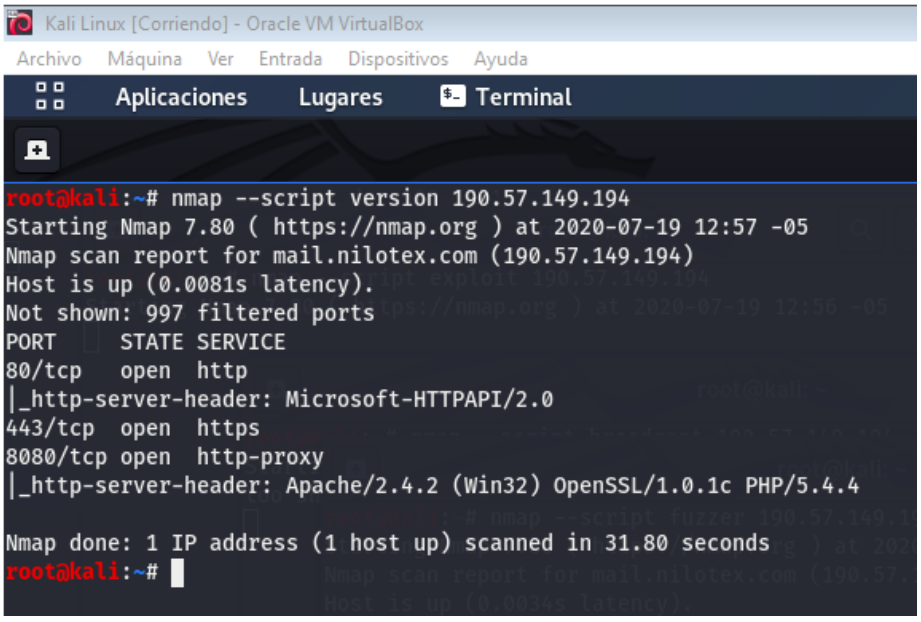

Ilustración 94. Nmap - Version - Kali Linux (Yonfá, 2020)

BLACKARCH - TERMINAL – LINEA DE COMANDOS

Para finalizar el uso del script Version, se usará la terminal de BlackArch para comparar con las otras dos herramientas usadas.

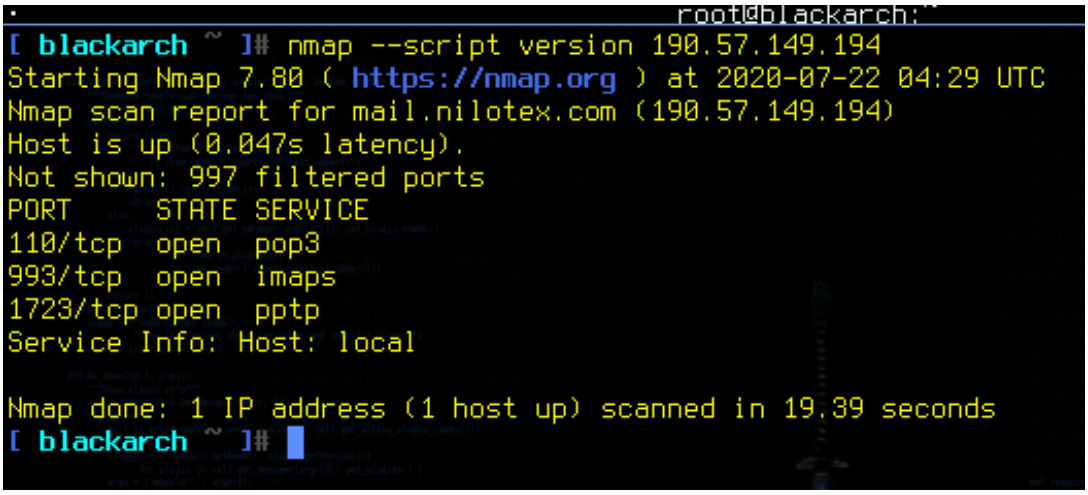

Ilustración 95. Nmap - Version - BlackArch (Yonfá, 2020)

Una vez finalizada la ejecución del script Version podemos darnos cuenta de que el script no presentó ninguna vulnerabilidad.

3. Capítulo 3. Análisis de Resultados e Implementación de guía

3.1. Análisis de Resultados

Una vez finalizado en escaneo a la red de la empresa con la ejecución de los distintos comandos, para identificar las vulnerabilidades, se va a realizar en este capítulo, el análisis de cada una de éstas, lo que permitirá indicar de manera detallada el puerto que presenta estas limitaciones de seguridad, y se explicará cuáles son las causas que provocan estas vulnerabilidades lo que servirá para la elaboración de la guía y la respectiva propuesta de solución.

Script: Discovery

Puerto: 433

- Ssl-enum-ciphers: Este script inicia repetidamente las conexiones SSLv3/TLS, cada vez que intenta un nuevo cifrado o compresor mientras se registra si un host lo acepta o lo rechaza. (NMAP.ORG, s.f.) (Kolybabi & Lawrence, s.f.).

  Haciendo referencia a la Ilustración 44 del análisis realizado presenta las siguientes vulnerabilidades.

  - **Warring: 64-bit block cipher 3DES vulnerable to SWEET32 attack**
  - **Warring: 64-bit block cipher DES vulnerable to SWEET32 attack**
  - **Warring: 64-bit block cipher DES40 vulnerable to SWEET32 attack**
  - **Warring: 64-bit block cipher IDEA vulnerable to SWEET32 attack**
  - **Warring: 64-bit block cipher RC2 vulnerable to SWEET32 attack**

  El firmware permite el uso de 3DES[1], DES[2], DES40[3], IDEA[4], RC2[5] para conexiones TLS y, por lo tanto, es vulnerable al ataque SWEET 32 (Es una manera de atacar conexiones web encriptados mediante la generación de grandes cantidades de tráfico web. (Ducklin, 2016)) (SONICWALL, 2020).

  Haciendo referencia a la Ilustración 44 del análisis realizado presenta la siguiente vulnerabilidad.

[1] Triple Data Encryption Standard
[2] Data Encryption Standard
[3] Data Encryption Standard con 40 bits
[4] International Data Encryption Algorithm
[5] Código de Ron o Cifrado de Rivest

- **Broken cipher RC4 is deprecated by RFC 7465**

Este problema afecta a los equipos que han confiado en el cifrado RC4 para conectarse con Windows Update. Windows Update ha cambiado sus protocolos de seguridad de conexión para finalizar la compatibilidad con el cifrado RC4. El cifrado RC4 ahora está deshabilitado de forma predeterminada y ya no se utiliza durante las negociaciones de reserva de TLS. (Microsoft, 2016).

Haciendo referencia a la Ilustración 44 del análisis realizado presenta la siguiente vulnerabilidad.

- **CBC-mode cipher in SSLv3 (CVE-2014-3566)**

SSL Versión 3.0 (RFC-6101) es un protocolo obsoleto e inseguro. Hay una vulnerabilidad en SSLv3 CVE-2014-3566 conocido como ataque de Padding Oracle On Downgraded Legacy Encryption (POODLE), ID de bug Cisco CSCur27131. La recomendación es deshabilitar SSL v3 mientras cambia los cifrados y solo utiliza TLS, y seleccionar la opción 3 (TLS v1). Revise el ID de bug Cisco proporcionado CSCur27131 para los detalles completos. (CISCO, 2019) (SSSL Shopper, 2008).

Haciendo referencia a la Ilustración 44 del análisis realizado presenta la siguiente vulnerabilidad.

- **Weak certificate signature: SHA1**

SHA-1 (Secure Hash Algorithm) es una función hash criptográfica que produce un valor hash de 160 bits y se considera débil. (Chandan, 2020).

Puerto: 993

- Ssl-enum-ciphers: Este script inicia repetidamente las conexiones SSLv3/TLS, cada vez que intenta un nuevo cifrado o compresor mientras se registra si un host lo acepta o lo rechaza. (Kolybabi & Lawrence, s.f.) (NMAP.ORG, s.f.).

Haciendo referencia a las Ilustraciones 37, 38, 39 del análisis realizado presenta la siguiente vulnerabilidad.

- **Warring: 64-bit block cipher 3DES vulnerable to SWEET32 attack**

El firmware permite el uso de 3DES (Triple Data Encryption Standard) para conexiones TLS y, por lo tanto, es vulnerable al ataque SWEET 32 (Es una manera de atacar conexiones web encriptados mediante la generación de grandes cantidades de tráfico web. (Ducklin, 2016)) (SONICWALL, 2020).

Puerto: 995

- Ssl-enum-ciphers: Este script inicia repetidamente las conexiones SSLv3/TLS, cada vez que intenta un nuevo cifrado o compresor mientras se registra si un host lo acepta o lo rechaza. (Kolybabi & Lawrence, s.f.) (NMAP.ORG, s.f.).

  Haciendo referencia a la Ilustración 41 del análisis realizado presenta la siguiente vulnerabilidad.

  - **Warring: 64-bit block cipher 3DES vulnerable to SWEET32 attack**

  El firmware permite el uso de 3DES (Triple Data Encryption Standard) para conexiones TLS y, por lo tanto, es vulnerable al ataque SWEET 32 (Es una manera de atacar conexiones web encriptados mediante la generación de grandes cantidades de tráfico web. (Ducklin, 2016)) (SONICWALL, 2020)

Script: Safe

Puerto: 110

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

  Haciendo referencia a la Ilustración 66 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan el intercambio anónimo de claves Diffie-Hellman solo proporcionan protección contra las escuchas pasivas y son vulnerables a ataques activos de tipo "man-in-the-middle" que podrían comprometer la confidencialidad y la integridad de los datos intercambiados a través de la sesión resultante.

  Haciendo referencia a la Ilustración 66 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva.

Puerto: 143

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

  Haciendo referencia a las Ilustraciones 60, 61 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan el intercambio anónimo de claves Diffie-Hellman solo proporcionan protección contra las escuchas pasivas y son vulnerables a ataques activos de tipo "man-in-the-middle" que podrían comprometer la confidencialidad y la integridad de los datos intercambiados a través de la sesión resultante.

  Haciendo referencia a la Ilustración 61 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva

Puerto: 443

- http-slowloris-check: Prueba un servidor web en busca de vulnerabilidad al ataque Slowloris DoS sin iniciar realmente un ataque DoS. (NMAP.ORG, s.f.) (Nikolic, s.f.).

  Haciendo referencia a la Ilustración 67 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Slowloris DOS attack**

    Slowloris intenta mantener abiertas muchas conexiones al servidor web de target y mantenerlas abiertas el mayor tiempo posible. Lo logra abriendo conexiones al servidor web de destino y enviando una solicitud parcial. Al hacerlo, priva a los recursos del servidor http y provoca la denegación de servicio.

- Ssl-ccs-injection: Detecta si un servidor es vulnerable a la vulnerabilidad SSL/TLS "CCS Injection" (CVE-2014-0224) (NMAP.ORG, s.f.) (Perta, s.f.).

Haciendo referencia a la Ilustración 68 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: OpenSSL antes de 0.9.8za, 1.0.0** antes de 1.0.0m, y 1.0.1 antes de 1.0.1h no restringe correctamente el procesamiento de los mensajes ChangeCipherSpec, lo que permite a los atacantes de man-in-the-mdlle activar el uso de una clave maestra de longitud cero en ciertas comunicaciones de OpenSSL a OpenSSL y, en consecuencia, sesiones de alta fidelidad u obtener información confidencial, a través de un protocolo de enlace TLS diseñado, también conocido como la vulnerabilidad de "Inyección CCS"

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

Haciendo referencia a la Ilustración 68 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Trasport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)**

  El protocolo de Seguridad de la capa de transporte (TLS) contiene una falla que se activa cuando se manejan intercambios de claves Diffie-Hellman definidos con el cifrado DHE_EXPORT. Esto puede permitir que un atacante hombre en el medio rebaje la seguridad de una sesión TLS a una criptografía de grado de exportación de 512 bits, que es significativamente más débil, lo que permite al atacante romper más fácilmente el cifrado y controlar o alterar el cifrado corriente.

Haciendo referencia a la Ilustración 69 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Los servicios de Seguridad de la capa de transporte (TLS) que usan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que usan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escuchas pasivas.

- Ssl-heartbleed: Detecta si un servidor es vulnerable al error OpenSSL Heartbleed (CVE-2014-0160). (NMAP.ORG, s.f.) (Karlsson, s.f.).

Haciendo referencia a la Ilustración 70 del análisis realizado presenta la siguiente vulnerabilidad.

- VULNERABLE: The Heartbleed Bug es una vulnerabilidad grave en la popular biblioteca de software criptográfico OpenSSL. Permite robar información destinada a ser protegida por encriptación SSL / TLS.

Haciendo referencia a la Ilustración 70 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Las versiones de OpenSSL 1.0.1** y 1.0.1-beta releases (incluidas 1.0.1f y 1.0.2-beta1) de OpenSSL se ven afectadas por el error Heartbleed. El error permite leer la memoria de los sistemas protegidos por las versiones vulnerables de OpenSSL y podría permitir la divulgación de información confidencial cifrada, así como las claves de cifrado en sí.

- Ssl-poodle: Comprueba si se permiten los cifrados SSLv3 CBC (POODLE). (NMAP.ORG, s.f.) (Miller, s.f.).

Haciendo referencia a la Ilustración 70 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: SSL POODLE information leak**

  El protocolo SSL 3.0, como se usa en OpenSSL a través de 1.01i y otros productos, utiliza un relleno CBC no determinista que facilita a los atacantes intermedios obtener datos en texto claro a través de un ataque de oráculo de relleno, también conocido como el problema "POODLE".

Puerto: 587

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

Haciendo referencia a la Ilustración 62 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

  Los servicios de seguridad de la capa de transporte (TLS) que utilizan el intercambio anónimo de claves Diffie-Hellman solo proporcionan protección contra las escuchas pasivas y son vulnerables a ataques activos de tipo "man-in-the-middle" que podrían comprometer la confidencialidad y la integridad de los datos intercambiados a través de la sesión resultante.

Haciendo referencia a la Ilustración 62 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade Mitm (Logjam)**

  El protocolo de Seguridad de la capa de transporte (TLS) contiene una falla que se activa cuando se manejan intercambios de claves Diffie-Hellman definidos con el cifrado DHE_EXPORT. Esto puede permitir que un atacante hombre en el medio rebaje la seguridad de una sesión TLS a una criptografía de grado de exportación de 512 bits, que es significativamente más débil, lo que permite al atacante romper más fácilmente el cifrado y controlar o alterar el cifrado corriente.

Haciendo referencia a la Ilustración 63 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva.

Puerto: 995

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

Haciendo referencia a las Ilustraciones 58, 59, 63, 64, 71 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

  Los servicios de seguridad de la capa de transporte (TLS) que utilizan el intercambio anónimo de claves Diffie-Hellman solo proporcionan protección contra las escuchas pasivas y son vulnerables a ataques activos de tipo "man-in-the-middle" que podrían comprometer la confidencialidad y la integridad de los datos intercambiados a través de la sesión resultante.

Haciendo referencia a las Ilustraciones 59, 61, 71 del análisis realizado presenta la siguiente vulnerabilidad.

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva

Script: Vuln

Puerto: 110

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

  Haciendo referencia a la Ilustración 73 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan el intercambio anónimo de claves Diffie-Hellman solo proporcionan protección contra las escuchas pasivas y son vulnerables a ataques activos de tipo "man-in-the-middle" que podrían comprometer la confidencialidad y la integridad de los datos intercambiados a través de la sesión resultante.

  Haciendo referencia a la Ilustración 74 del análisis realizado presenta la siguiente vulnerabilidad

  - **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva.

Puerto: 143

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (Gajek, s.f.) (NMAP.ORG, s.f.).

  Haciendo referencia a las Ilustraciones 80, 83 del análisis realizado presenta la siguiente vulnerabilidad

  - **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan el intercambio anónimo de claves Diffie-Hellman solo proporcionan protección contra las escuchas

pasivas y son vulnerables a ataques activos de tipo "man-in-the-middle" que podrían comprometer la confidencialidad y la integridad de los datos intercambiados a través de la sesión resultante.

Haciendo referencia a las Ilustraciones 80, 84 del análisis realizado presenta la siguiente vulnerabilidad

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva.

Puerto: 443

- Ssl-ccs-injection: Detecta si un servidor es vulnerable a la vulnerabilidad SSL/TLS "CCS Injection" (CVE-2014-0224) (NMAP.ORG, s.f.) (Perta, s.f.).

  Haciendo referencia a las Ilustraciones 81, 85, 86 del análisis realizado presenta la siguiente vulnerabilidad

  - **VULNERABLE: OpenSSL antes de 0.9.8za, 1.0.0** antes de 1.0.0m, y 1.0.1 antes de 1.0.1h no restringe correctamente el procesamiento de los mensajes ChangeCipherSpec, lo que permite a los atacantes de man-in-the-mdlle activar el uso de una clave maestra de longitud cero en ciertas comunicaciones de OpenSSL a OpenSSL y, en consecuencia, sesiones de alta fidelidad u obtener información confidencial, a través de un protocolo de enlace TLS diseñado, también conocido como la vulnerabilidad de "Inyección CCS"

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (Gajek, s.f.) (NMAP.ORG, s.f.)

  Haciendo referencia a las Ilustraciones 81, 86 del análisis realizado presenta la siguiente vulnerabilidad

  - **VULNERABLE: Trasport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)**

    El protocolo de Seguridad de la capa de transporte (TLS) contiene una falla que se activa cuando se manejan intercambios de claves Diffie-Hellman definidos con el cifrado DHE_EXPORT. Esto puede permitir que un atacante hombre en el medio rebaje la

seguridad de una sesión TLS a una criptografía de grado de exportación de 512 bits, que es significativamente más débil, lo que permite al atacante romper más fácilmente el cifrado y controlar o alterar el cifrado corriente.

Haciendo referencia a las Ilustraciones 81, 82, 87 del análisis realizado presenta la siguiente vulnerabilidad

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Los servicios de Seguridad de la capa de transporte (TLS) que usan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que usan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escuchas pasivas.

- Ssl-heartbleed: Detecta si un servidor es vulnerable al error OpenSSL Heartbleed (CVE-2014-0160). (NMAP.ORG, s.f.) (Karlsson, s.f.)

  Haciendo referencia a las Ilustraciones 82, 87 del análisis realizado presenta la siguiente vulnerabilidad

  - **VULNERABLE: El error Heartbleed** es una vulnerabilidad grave en la popular biblioteca de software criptográfico OpenSSL. Permite robar información destinada a ser protegida por encriptación SSL / TLS.

    Las versiones de OpenSSL 1.0.1 y 1.0.2-beta (incluidas 1.0.1f y 1.0.2-beta1) de OpenSSL se ven afectadas por el error de heartbleed. El error permite leer la memoria de los sistemas protegidos por las versiones vulnerables de OpenSSL y podría permitir la divulgación de información confidencial cifrada, así como las claves de cifrado.

- Ssl-poodle: Comprueba si se permiten los cifrados SSLv3 CBC (POODLE) (NMAP.ORG, s.f.) (Miller, s.f.).

  Haciendo referencia a las Ilustraciones 82, 88 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: SSL POODLE information leak**

    El protocolo SSL 3.0, como se usa en OpenSSL a través de 1.01i y otros productos, utiliza un relleno CBC no determinista que facilita a los atacantes intermedios obtener datos en texto claro a través de un ataque de oráculo de relleno, también conocido como el problema "POODLE”.

- http-slowloris-check: Prueba un servidor web en busca de vulnerabilidad al ataque Slowloris DoS sin iniciar realmente un ataque DoS. (NMAP.ORG, s.f.) (Nikolic, s.f.).

  Haciendo referencia a la Ilustración 85 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Slowloris DOS attack**

    Slowloris intenta mantener abiertas muchas conexiones al servidor web de target y mantenerlas abiertas el mayor tiempo posible. Esto se logra abriendo conexiones al servidor web target y enviando una solicitud parcial. Al hacerlo, priva de recursos al servidor http y provoca la denegación de servicio.

Puerto: 587

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (Gajek, s.f.) (NMAP.ORG, s.f.).

  Haciendo referencia a la Ilustración 78 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

    Los servicios de seguridad de la capa de transporte (TLS) que utilizan el intercambio anónimo de claves Diffie-Hellman solo proporcionan protección contra las escuchas pasivas y son vulnerables a ataques activos de tipo "man-in-the-middle" que podrían comprometer la confidencialidad y la integridad de los datos intercambiados a través de la sesión resultante.

  Haciendo referencia a la Ilustración 79 del análisis realizado presenta la siguiente vulnerabilidad.

  - **VULNERABLE: Trasport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)**

    El protocolo de Seguridad de la capa de transporte (TLS) contiene una falla que se activa cuando se manejan intercambios de claves Diffie-Hellman definidos con el cifrado DHE_EXPORT. Esto puede permitir que un atacante hombre en el medio rebaje la seguridad de una sesión TLS a una criptografía de grado de exportación de 512 bits, que es significativamente más débil, lo que permite al atacante romper más fácilmente el cifrado y controlar o alterar el cifrado corriente.

Haciendo referencia a la Ilustración 77 del análisis realizado presenta la siguiente vulnerabilidad

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva.

Puerto: 993

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

Haciendo referencia a la Ilustración 82 del análisis realizado presenta la siguiente vulnerabilidad

- **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

  Vulnerabilidad anónima de MitM de intercambio de claves Diffie-Hellman

  Los servicios de Seguridad de la capa de transporte (TLS) que utilizan el intercambio de claves anónimo Diffie-Hellman solo brindan protección contra escuchas pasivas y son vulnerables a ataques activos de intermediarios que podrían comprometer por completo la confidencialidad e integridad de cualquier información intercambiada sobre el resultado sesión.

Haciendo referencia a la Ilustración 83 del análisis realizado presenta la siguiente vulnerabilidad

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Diffie-Hellman Intercambio de claves Fuerza de grupo insuficiente

  Los servicios de Seguridad de la capa de transporte (TLS) que usan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que usan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques pasivos de espionaje.

Puerto: 995

- Ssl-dh-params: Detección de parámetros Diffie-Hellman efímera débil para servicios SSL/TLS. (NMAP.ORG, s.f.) (Gajek, s.f.).

Haciendo referencia a la Ilustración 89 del análisis realizado presenta la siguiente vulnerabilidad

- **VULNERABLE: Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

Vulnerabilidad anónima de MitM de intercambio de claves Diffie-Hellman

Los servicios de Seguridad de la capa de transporte (TLS) que utilizan el intercambio de claves anónimo Diffie-Hellman solo brindan protección contra escuchas pasivas y son vulnerables a ataques activos de intermediarios que podrían comprometer por completo la confidencialidad e integridad de cualquier información intercambiada sobre el resultado sesión.

Haciendo referencia a la Ilustración 89 del análisis realizado presenta la siguiente vulnerabilidad

- **VULNERABLE: Diffie-Hellman Key Exchange Insufficient Group Strength**

  Los servicios de Seguridad de la capa de transporte (TLS) que usan grupos Diffie-Hellman de fuerza insuficiente, especialmente aquellos que usan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques pasivos de espionaje.

3.2. Guía de Implementación

Para poder mitigar las vulnerabilidades detectadas en la red de la empresa, nos basaremos en la guía de control que la normativa ISO/IEC 27001 nos brinda.

A continuación, se describirán los apartados que se encuentran en la norma ISO que se tomarán para mitigar estas vulnerabilidades.

En el Anexo A de la norma ISO/IEC 27001, sección A.10 referente a Criptografía, apartado A10.1 Controles de criptografía, dice que el objetivo es" Asegurar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información". (ISO/IEC, 2017)

En cuanto a las vulnerabilidades el apartado A.12.6 referente a Gestión de la Vulnerabilidad técnica su principal objetivo es prevenir la explotación de vulnerabilidades técnicas. El punto A.12.6.1 sobre la Gestión de vulnerabilidades técnicas el control que sugiere la normativa dice: "Se debe Obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado." (ISO/IEC, 2017)

Vulnerabilidades

- **Warring: 64-bit block cipher 3DES vulnerable to SWEET32 attack**
- **Warring: 64-bit block cipher DES vulnerable to SWEET32 attack**
- **Warring: 64-bit block cipher DES40 vulnerable to SWEET32 attack**

- **Warring: 64-bit block cipher IDEA vulnerable to SWEET32 attack**
- **Warring: 64-bit block cipher RC2 vulnerable to SWEET32 attack**

Descripción:

El firmware permite el uso de 3DES[6], DES[7], DES40[8], IDEA[9], RC2[10] para conexiones TLS y, por lo tanto, es vulnerable al ataque SWEET 32 (Es una manera de atacar conexiones web encriptados mediante la generación de grandes cantidades de tráfico web. (Ducklin, 2016)) (SONICWALL, 2020)

Solución

Esta vulnerabilidad se corrige actualizando a la última versión el firmware que la empresa posee. (SONICWALL, 2020)

Vulnerabilidad

- **Broken cipher RC4 is deprecated by RFC 7465**

Descripción:

Este problema afecta a los equipos que han confiado en el cifrado RC4 para conectarse con Windows Update. Windows Update ha cambiado sus protocolos de seguridad de conexión para finalizar la compatibilidad con el cifrado RC4. El cifrado RC4 ahora está deshabilitado de forma predeterminada y ya no se utiliza durante las negociaciones de reserva de TLS. (Microsoft, 2016)

Solución

Microsoft recomienda habiliten TLS 1.2 en sus servicios y quiten la compatibilidad con RC4. Para mitigar este problema, habilite conjuntos de cifrado que usen cifrados alternativos compatibles con Windows Update. (Microsoft, 2016)

Vulnerabilidad

- **CBC-mode cipher in SSLv3 (CVE-2014-3566)**

[6] Triple Data Encryption Standard
[7] Data Encryption Standard
[8] Data Encryption Standard con 40 bits
[9] International Data Encryption Algorithm
[10] Código de Ron o Cifrado de Rivest

Descripción:

SSL Versión 3.0 es un protocolo obsoleto e inseguro. Hay una vulnerabilidad en SSLv3 CVE-2014-3566 conocido como ataque de Padding Oracle On Downgraded Legacy Encryption (POODLE). (CISCO, 2019) (SSSL Shopper, 2008)

Solución

La recomendación es deshabilitar SSL v3 mientras cambia los cifrados y solo utiliza TLS. (CISCO, 2019) (SSSL Shopper, 2008)

Vulnerabilidad

- **Weak certificate signature: SHA1**

Descripción:

SHA-1 (Secure Hash Algorithm) es una función hash criptográfica que produce un valor hash de 160 bits y se considera débil. (Chandan, 2020)

Solución

Para solucionar se necesita obtener un certificado SSL firmado con SHA-2.

Algunos proveedores de certificados SSL pueden proporcionarle un certificado firmado por SHA-2. (Chandan, 2020)

Vulnerabilidad

- **Anonymous Diffie-Hellman Key Exchange MitM Vulnerability**

Descripción:

Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Helman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva. (MinistroFang207, s.f.)

Solución

Se puede utilizar Elliptic-Curve Diffie-Hellman (ECDHE) o cambiar a un grupo Diffie-Hellman de 2048 bits y más fuerte. (MinistroFang207, s.f.)

Actualizar todas la aplicaciones y versiones de sistemas a la última versión, ya que se corrigen muchos errores de versiones anteriores.

Vulnerabilidad

- **Diffie-Hellman Key Exchange Insufficient Group Strength**

Descripción:

Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Helman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva. (MinistroFang207, s.f.)

Solución

Se puede utilizar Elliptic-Curve Diffie-Hellman (ECDHE) o cambiar a un grupo Diffie-Hellman de 2048 bits y más fuerte. (MinistroFang207, s.f.)

Vulnerabilidad

- **Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)**

Descripción:

Es un ataque al protocolo de intercambio de claves Diffie-Hellman utilizado en TLS, permite a un atacante man-in-the-middle degradar las conexiones TLS vulnerables a la criptografía de grado de exportación de 512 bits, dando como resultado el poder leer y modificar los datos pasados a través de la conexión. (weakdh.org, 2015) (Schneier en Seguridad, 2015).

Los servicios de seguridad de la capa de transporte (TLS) que utilizan grupos Diffie-Helman de fuerza insuficiente, especialmente aquellos que utilizan uno de los pocos grupos comúnmente compartidos, pueden ser susceptibles a ataques de escucha pasiva. (MinistroFang207, s.f.)

Solución

Se recomienda deshabilitar la compatibilidad con los conjuntos de cifrado de grado de exportación (DHE_EXPORT) que permiten degradar las conexiones Diffie-Hellman y generar un grupo Diffie-Hellman de 2048 bits nuevo y único, ya que el nuevo mínimo es 1024 bits., Es preferible usar Elliptic-Curve Diffie-Hellman Key Exchange. (Oweis, 2015) (weakdh.org, 2015)

Vulnerabilidad

- **Slowloris DOS attack**

Descripción:

Un ataque DDOS (denegación de servicio distribuida) es uno de los principales problemas de las compañías. Este tipo de ataques utiliza solicitudes HTTP parciales para abrir conexiones entre un único equipo y un servidor Web de destino. (NETSCOUT, 2020) (Pillai, 2013)

Solución

Para solucionar esta vulnerabilidad existen algunas posibilidades que nos brindaran una mayor seguridad en nuestros sistemas, estas son algunas sugerencias:

- Aumentar el número máximo de clientes que el servidor Web permitirá.
- Limite el número de conexiones que una sola dirección IP puede intentar.
- Poner restricciones a la velocidad mínima de transferencia se permite una conexión.
- Restringir la cantidad de tiempo que un cliente puede permanecer conectado.
- En el caso de los servidores web Apache, se pueden emplear varios módulos para evitar daños por un ataque Slowloris. Estos módulos incluyen: Mod_limitipconn, Mod_qos, Mod_evasive, Seguridad Mod, Mod_noloris, Mod_antiloris

  Apache 2.2.15 incluye el módulo mod_reqtimeout, que es la solución soportada por los desarrolladores. (NETSCOUT, 2020) (Pillai, 2013)

Vulnerabilidad

- **The Heartbleed Bug**

Descripción:

El error Heartbleed no es un defecto en los protocolos SSL o TLS; más bien, es un defecto en la implementación de OpenSSL, esta vulnerabilidad permite robar la información protegida. (Rowley, 2014) (The Heartbleed Bug, 2020)

Solución

Para poder mitigar estas vulnerabilidades es necesario actualizar a la última versión de OpenSSL, revocar todos los certificados utilizados con la versión vulnerable. (Rowley, 2014)

Vulnerabilidad

- **The “CCS Injection” vulnerability**

Descripción:

Esta es una vulnerabilidad grave. Es un ataque difícil de detectar ya que no deja rastro, en este ataque los nodos intermedios malintencionados interceptan datos cifrados y los descifran mientras obligan a clientes SSL a usar claves débiles. (lepidum, 2014)

Solución:

Para solucionar esta vulnerabilidad si se usa dispositivos Android o Linux es necesario aplicar las actualizaciones ya que en las versiones OpenSSL 1.0.1h, OpenSSL 1.0.0m, OpenSSL 0.9.8za, ya que estos dispositivos utilizan OpenSSL. Mientras que en dispositivos Windows, Mac o IPhone no existe un riesgo ante esta vulnerabilidad. (lepidum, 2014)

Vulnerabilidad

- **SSL POODLE information leak**

Descripción:

El ataque POODLE (Padding Oracle On Downgraded Legacy Encryption) usa la vulnerabilidad en el cifrado por bloques (CBC) en la versión 3.0 de SSL (Secure Socket Layer). Este ataque permite descifrar y extraer información desde una transacción cifrada, puede ser utilizado contra cualquier sistema o aplicación compatible con SSL 3.0 con cifrado de modo CBC. Mediante este ataque se puede obtener contraseñas, cuentas de usuario, cookies y otros tokens de autenticación. (ASI, 2014)

Solución

Se recomendable desactivar la compatibilidad SSL 3.0 en las configuraciones del sistema/aplicación, también utilizar una extensión TLS_FALLBACK_SCSV que permite evita atacantes MITM. OpenSSL ya ha agregado compatibilidad para TLS_FALLBACK_SCSV en sus versiones más recientes. (ASI, 2014).

4. Capítulo 4. Conclusiones y Recomendaciones

En el presente trabajo de titulación se detallan las posibles causas por las cuales se pudieron presentar dichas vulnerabilidades y su recomendación para corregirlas, de esta manera se pretende mantener el sistema de la empresa en las mejores condiciones de seguridad.

4.1. Conclusiones

- El objetivo del presente trabajo de disertación, fue encontrar las posibles vulnerabilidades en la red de la empresa, el cual nos presentó algunas fallas en la seguridad de las versiones de los protocolos que la empresa utiliza, afectando a la información que la empresa maneja en sus transacciones. Convirtiéndose en un riesgo para su seguridad.
- El mantener versiones no actualizadas en sistemas y aplicaciones es un descuido muy grande para la seguridad de cualquier empresa, ya que existen errores en estas versiones que no se controlan de otra manera más que actualizando o con los diferentes parches que surgen para corregir estos errores.
- La normativa ISO/IEC 27001 en todos sus apartados indica los controles que se deben utilizar para el manejo adecuado de la información de la empresa, tomando en cuenta a cada miembro y el rol que debe cumplir.
- El análisis realizado arrojo una serie de vulnerabilidades ocasionando un alto riesgo de inseguridad al momento de realizar procesos informáticos en el sistema de la empresa, utilizando herramientas como NMAP para poder detectar estas amenazas y vulnerabilidades. Entre las vulnerabilidades encontradas están: ataques SWEET32, ataques man-in-the-middle, intercambio de claves Diffie-Hellman, ataques Slowloris DOS, vulnerabilidades criptográficas.
- La falta de conocimiento o descuido por parte de los encargados del sistema se vuelve un riego de seguridad, ya que son ellos los responsables de mantener los sistemas seguros para el beneficio de la empresa. El mantenerse actualizado ante los nuevos riegos que surgen y de igual manera ante las soluciones a estos riegos brinda una ventaja amplia a la empresa, ya que puede reducir el impacto en la empresa y poder controlar y mitigar estas posibles vulnerabilidades.

4.2. Recomendaciones

- Como toda la tecnología avanza a pasos agigantados, el mantener nuestros sistemas y aplicaciones con las últimas versiones es lo más recomendable que los responsables del área de sistemas deben tener en cuanta. Esto brinda mayor seguridad en nuestros aplicativos, por el simple hecho que cada actualización que se realiza corrige errores que nuestros sistemas pueden poseer en versiones posteriores.
- Realizar un escaneo periódico de los sistemas de la compañía, para de esta manera tener control y tomar las acciones necesarias ante posibles fallos que se detecten en los escaneos.
- El mantenerse actualizado de versiones, errores, productos en el área de sistemas es muy importante por el avance tecnológico que el mundo vive. Así como la tecnología avanza, los ataques mejorar al igual que las seguridades que se deben implementar para controlar posibles ataques.
- Capacitar al personal constantemente en la adaptación del SGSI ayuda al correcto funcionamiento de los controles establecidos.
- Desarrollar un plan de seguridad informática tomando en cuenta el análisis realizado, para de esta manera proteger los datos y la información que la empresa maneja.

Bibliografía

adastra. (27 de Julio de 2011). *SEGURIDAD EN SISTEMAS Y TÉCNICAS DE HACKING. THEHACKERWAY (THW)*. Recuperado el 19 de Julio de 2020, de Técnicas de Recolección de Información – Scripting con NMAP: https://thehackerway.com/2011/07/27/tecnicas-de-recoleccion-de-informacion-%E2%80%93-scripting-con-nmap/

admin. (30 de Mayo de 2012). *sitiopractico*. Recuperado el 26 de Enero de 2020, de La Comisión Electrotécnica Internacional (IEC): http://sitiopractico.net/blog/la-comision-electrotecnica-internacional-iec/

ASI. (17 de Octubre de 2014). *ASI*. Recuperado el 28 de Julio de 2020, de Ataque POODLE a vulnerabilidad en SSL: https://blog.auditoria.com.mx/2014/10/ataques-poodle-en-vulnerabilidad-en-ssl/

Barr, D. (s.f.). *KALI TOOLS*. Recuperado el 15 de Junio de 2020, de dnswalk Package Description: https://tools.kali.org/information-gathering/dnswalk

BlackArch Linux. (2020). *BlackArch Linux*. Recuperado el 25 de Febrero de 2020, de Acerca de: https://blackarch.org/

BlackArch Linux. (2020). *BlackArch Linux*. Recuperado el 01 de Marzo de 2020, de Herramientas: https://blackarch.org/tools.html

Blog Calidad ISO. (30 de Diciembre de 2014). *Historia de la ISO*. Recuperado el 21 de Enero de 2020, de http://blogdecalidadiso.es/historia-de-la-iso/

Catoira, F. (24 de Julio de 2012). *Welivesecurity.comby by ESET*. Recuperado el 17 de Marzo de 2020, de Penetration Test, ¿en qué consiste?: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

ceos3c. (5 de Julio de 2019). *Ethical Hacking, Linux & Open Source*. Recuperado el 11 de Agosto de 2020, de Nmap Tutorial Series 4: Nmap Scripts (NSE): https://www.ceos3c.com/hacking/nmap-tutorial-series-4-nmap-scripts-nse/

Chandan, K. (3 de Junio de 2020). *GEEKFLARE*. Recuperado el 27 de Julio de 2020, de Análisis de vulnerabilidad de seguridad SHA-1 y cómo solucionar: https://geekflare.com/test-ssl-sha1-vulnerability-and-fix/

CISCO. (10 de Septiembre de 2019). *Apoyo*. Recuperado el 27 de Julio de 2020, de VULNERABILIDAD de modo CBC débil del protocolo SSL v3 y TLS v1: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118518-technote-esa-00.html

Disterer, G. (11 de Abril de 2013). *ISO/IEC 27000, 27001 and 27002 for Information Security Management*. Obtenido de Development of Standards: https://serwiss.bib.hs-

hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf

Disterer, G. (Abril de 2013). *Journal of Information Security*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27000, 27001 y 27002 para la gestión de seguridad de la información: https://www.scirp.org/pdf/JIS_2013042311130103.pdf

Ducklin, P. (25 de Agosto de 2016). *naked Security by Sophos*. Recuperado el 24 de Julio de 2020, de Anatomía de una colisión criptográfica – el ataque "Sweet32": https://nakedsecurity.sophos.com/es/2016/08/25/anatomy-of-a-cryptographic-collision-the-sweet32-attack/#:~:text=Sweet32%20es%20una%20manera%20de%20atacar%20conexiones%20web,de%20informaci%C3%B3n%20sobre%20el%20tr%C3%A1fico%20que%20est%C3%A1%20cifrando.

ESET. (12 de Febrero de 2015). *Welivesecurity*. Recuperado el 19 de Julio de 2020, de Auditando con Nmap y sus scripts para escanear vulnerabilidades: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

Filip Waeytens, e. t. (s.f.). *KALI TOOLS*. Recuperado el 15 de Junio de 2020, de Descripción del paquete dnsenum: https://tools.kali.org/information-gathering/dnsenum

Gajek, J. (s.f.). *NMAP.ORG*. Recuperado el 24 de Julio de 2020, de Archivo ssl-dh-params: https://nmap.org/nsedoc/scripts/ssl-dh-params.html

Gómez, O., Aguileta, A., Góme, G., & Aguilar, R. (Mayo de 2014). *Computacion e Informatica.* Recuperado el 03 de Marzo de 2020, de Estudio del Proceso Software Personal (PSP) en un entorno académico: http://redi.uady.mx/bitstream/handle/123456789/428/25-45-1-SM.pdf?sequence=1&isAllowed=y

Groothuis, E. (s.f.). *KALI LINUX*. Recuperado el 15 de Junio de 2020, de dnstracer Package Description: https://tools.kali.org/information-gathering/dnstracer

Grupo CFI. (s.f.). *Análisis de vulnerabilidades*. Recuperado el 19 de Julio de 2020, de ¿Qué es un análisis de vulnerabilidades?: https://grupocfi.es/analisis-de-vulnerabilidades/

Guijarro, H. (22 de Mayo de 2018). *IT Governance Europe*. Recuperado el 10 de Marzo de 2020, de Qué es un test de penetración y para qué sirve: https://www.itgovernance.eu/blog/es/que-es-un-test-de-penetracion-y-para-que-sirve

GUILENIA S.A. (s.f.). *Normas IEC*. Recuperado el 30 de Enero de 2020, de Comisión Electrotécnica Internacional (IEC): http://www.guilenia.com/interup_4J.asp

H1RD. (30 de Junio de 2017). *H1RD SECURITY*. Recuperado el 17 de Marzo de 2020, de Fases de un test de penetración: http://www.h1rd.com/hacking/Fases-de-un-ataque

Horton, A. (s.f.). *KALI TOOLS*. Recuperado el 15 de Junio de 2020, de urlcrazy Package Description: https://tools.kali.org/information-gathering/urlcrazy

IEC. (2020). *Internacional Electrotécnico Comisión*. Recuperado el 26 de Enero de 2020, de Who we are: https://www.iec.ch/about/profile/

IEC. (2020). *International Electrotechnical Commission*. Recuperado el 26 de Enero de 2020, de Who we are: https://www.iec.ch/dyn/www/f?p=103:5:0

iSECPartners. (s.f.). *KaliTools*. Recuperado el 20 de Julio de 2020, de SSLyze Package Description: https://tools.kali.org/information-gathering/sslyze

IsecT. (s.f.). *ISO/IEC 27002*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27002: 2013: https://www.iso27001security.com/html/27002.html

Isect. (s.f.). *ISO/IEC 27003*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27003:2017: https://www.iso27001security.com/html/27003.html

Isect. (s.f.). *ISO/IEC 27004*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27004:2016: https://www.iso27001security.com/html/27004.html

Isect. (s.f.). *ISO/IEC 27005*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27005: 2018: https://www.iso27001security.com/html/27005.html

Isect. (s.f.). *ISO/IEC 27006*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27006:2015: https://www.iso27001security.com/html/27006.html

Isect. (s.f.). *ISO/IEC 27007*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27007:2020: https://www.iso27001security.com/html/27007.html

Isect. (s.f.). *ISO/IEC 27010*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27010:2015: https://www.iso27001security.com/html/27010.html

Isect. (s.f.). *ISO/IEC 27011*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27011:2016: https://www.iso27001security.com/html/27011.html

Isect. (s.f.). *ISO/IEC 27011*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27011:2015: https://www.iso27001security.com/html/27013.html

Isect. (s.f.). *ISO/IEC 27014*. Recuperado el 20 de Febrero de 2020, de ISO / CEI 27014:2013: https://www.iso27001security.com/html/27014.html

Isect. (s.f.). *ISO/IEC 27018*. Recuperado el 20 de Febrero de 2020, de ISO/IEC 27018:2019: https://www.iso27001security.com/html/27018.html

Isect. (s.f.). *ISO/IEC 27019*. Recuperado el 20 de Febrero de 2020, de ISO/IEC 27019:2017: https://www.iso27001security.com/html/27019.html

Isect. (s.f.). *ISO/IEC 27021*. Recuperado el 20 de Febrero de 2020, de ISO/IEC 27021:2017: https://www.iso27001security.com/html/27021.html

Isect. (s.f.). *ISO/IEC 27030*. Recuperado el 20 de Febrero de 2020, de ISO/IEC 27030: https://www.iso27001security.com/html/27030.html

Isect. (s.f.). *ISO/IEC 27032*. Recuperado el 21 de Febrero de 2020, de ISO/IEC 27032: 2012: https://www.iso27001security.com/html/27032.html

Isect. (s.f.). *ISO/IEC 27033*. Recuperado el 21 de Febrero de 2020, de ISO/IEC 27033: 2010+: https://www.iso27001security.com/html/27033.html

Isect. (s.f.). *ISO/IEC TR 27016*. Recuperado el 20 de Febrero de 2020, de ISO /IEC TR 27016:2014: https://www.iso27001security.com/html/27016.html

ISO 27000.es. (s.f.). *El portal de ISO 27001 en Español*. Recuperado el 01 de Febrero de 2020, de DestacaDos ISO 27000: http://www.iso27000.es/iso27000.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO/IEC 27000:2018 [ISO/IEC 27000:2018]: https://www.iso.org/standard/73906.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27002: 2013 [ISO / IEC 27002: 2013]: https://www.iso.org/standard/54533.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27003: 2017 [ISO / IEC 27003: 2017]: https://www.iso.org/standard/63417.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27004: 2016 [ISO / IEC 27004: 2016]: https://www.iso.org/standard/64120.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27005: 2018 [ISO / IEC 27005: 2018]: https://www.iso.org/standard/75281.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27006: 2015 [ISO / IEC 27006: 2015]: https://www.iso.org/standard/62313.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27007: 2017 [ISO / IEC 27007: 2017]: https://www.iso.org/standard/67398.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC TS 27008: 2019 [ISO / IEC TS 27008: 2019]: https://www.iso.org/standard/67397.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27009: 2016 [ISO / IEC 27009: 2016]: https://www.iso.org/standard/42508.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27010: 2015 [ISO / IEC 27010: 2015]: https://www.iso.org/standard/68427.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27011: 2016 [ISO / IEC 27011: 2016]: https://www.iso.org/standard/64143.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27013: 2015 [ISO / IEC 27013: 2015]: https://www.iso.org/standard/64138.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27014: 2013 [ISO / IEC 27014: 2013]: https://www.iso.org/standard/43754.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC TR 27015: 2012 [ISO / IEC TR 27015: 2012]: https://www.iso.org/standard/43755.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC TR 27016: 2014 [ISO / IEC TR 27016: 2014]: https://www.iso.org/standard/43756.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27017: 2015 [ISO / IEC 27017: 2015]: https://www.iso.org/standard/43757.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27018: 2019 [ISO / IEC 27018: 2019]: https://www.iso.org/standard/76559.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27019: 2017 [ISO / IEC 27019: 2017]: https://www.iso.org/standard/68091.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27021: 2017 [ISO / IEC 27021: 2017]: https://www.iso.org/standard/61003.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC CD 27022 [ISO / IEC CD 27022]: https://www.iso.org/standard/61004.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC TR 27023: 2015 [ISO / IEC TR 27023: 2015]: https://www.iso.org/standard/61005.html

ISO. (s.f.). *ISO*. Recuperado el 20 de Febrero de 2020, de ISO / IEC 27031: 2011 [ISO / IEC 27031: 2011]: https://www.iso.org/standard/44374.html

ISO. (s.f.). *ISO*. Recuperado el 21 de Febrero de 2020, de ISO / IEC 27032: 2012 [ISO / IEC 27032: 2012]: https://www.iso.org/standard/44375.html

ISO. (s.f.). *ISO*. Recuperado el 21 de Febrero de 2020, de ISO / IEC 27033-1: 2015 [ISO / IEC 27033-1: 2015]: https://www.iso.org/standard/63461.html

ISO. (s.f.). *ISO / IEC 27001 GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*. Recuperado el 01 de Febrero de 2020, de https://www.iso.org/isoiec-27001-information-security.html

ISO. (s.f.). *Sobre Nosotros*. Recuperado el 14 de Enero de 2020, de ISO: https://www.iso.org/about-us.html

ISO/IEC. (2017). NORMA TÉCNICA ECUATORIANA. *TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – REQUISITOS (ISO/IEC 27001:2013+Cor.1:2014+ Cor. 2:2015, IDT), Segunda*, 19. Ecuador. Recuperado el 27 de Julio de 2020

ISO/IEC. (2017). NORMA TÉCNICA ECUATORIANA. *TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE , Segunda*, 16. (INEN, Trad.) Ecuador. Recuperado el 27 de Julio de 2020

ISO27000.ES. (2005). *ISO27000.ES*. Recuperado el 20 de Febrero de 2020, de Serie "27000": http://www.iso27000.es/page8.html

ISO27K information segurity. (16 de Febrero de 2020). *ISO27K information segurity*. Recuperado el 20 de Febero de 2020, de ISO / IEC 27000: 2018: https://www.iso27001security.com/html/27000.html

ISOTools. (20 de Junio de 2013). *ISO, Organización Internacional de Normalización: Historia, Funciones y Estructura.* Recuperado el 21 de Enero de 2020, de Historia de la ISO: https://www.isotools.org/2013/06/20/iso-organizacion-internacional-de-normalizacion-historia-funciones-y-estructura/

ISOTools. (26 de Julio de 2015). *Origen de las normas ISO*. Recuperado el 21 de Enero de 2020, de https://www.isotools.org/2015/07/26/origen-normas-iso/

Ivan. (4 de Septiembre de 2017). *Hacking para novatos*. Recuperado el 10 de Marzo de 2020, de Fases de una auditoría (pentesting): https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/

KaliTools. (s.f.). *Listado de herramientas de Kali Linux*. Recuperado el 02 de Marzo de 2020, de https://tools.kali.org/tools-listing

Karlsson, P. (s.f.). *NMAP.ORG*. Recuperado el 25 de Julio de 2020, de File ssl-heartbleed: https://nmap.org/nsedoc/scripts/ssl-heartbleed.html

Kolybabi, M., & Lawrence, G. (s.f.). *NMAP.ORG*. Recuperado el 24 de Julio de 2020, de Discovery: https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html

Leacock, S. (12 de Mayo de 2019). *Backtrack Academy*. Recuperado el 19 de Julio de 2020, de Introducción al escaneo de red y vulnerabilidades con Nmap: https://backtrackacademy.com/articulo/introduccion-al-escaneo-de-red-y-vulnerabilidades-con-nmap

lepidum. (16 de Junio de 2014). *lepidum*. Recuperado el 28 de Julio de 2020, de CCS Injection Vulnerability: http://ccsinjection.lepidum.co.jp/

Lowe, M. (s.f.). *KaliTools*. Recuperado el 20 de Julio de 2020, de enum4linux Package Description: https://tools.kali.org/information-gathering/enum4linux

Mak Kolybabi, G. L. (s.f.). *NMAP.ORG*. Recuperado el 24 de Julio de 2020, de File ssl-enum-ciphers: https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html

Martorella, C. (s.f.). *KaliTools*. Recuperado el 19 de Julio de 2020, de theharvester Package Description: https://tools.kali.org/information-gathering/theharvester

Microsoft. (18 de Agosto de 2016). *Apoyo*. Recuperado el 27 de Julio de 2020, de Windows Update ha dejado de ser compatible con el cifrado RC4: https://support.microsoft.com/en-us/help/3186695/windows-update-has-deprecated-support-for-the-rc4-cipher

Miller, D. (s.f.). *NMAP.ORG*. Recuperado el 25 de Julio de 2020, de File ssl-poodle: https://nmap.org/nsedoc/scripts/ssl-poodle.html

MinistroFang207. (s.f.). *Course Hero*. Recuperado el 29 de Julio de 2020, de 3 name transport layer security tls protocol: https://www.coursehero.com/file/pc3ags1/3-Name-Transport-Layer-Security-TLS-Protocol-DHEEXPORT-Ciphers-Downgrade-MitM/

NETSCOUT. (2020). *Ataques DDoS de Slowloris*. Recuperado el 27 de Julio de 2020, de ¿Qué es un ataque Slowloris?: https://es.netscout.com/what-is-ddos/slowloris-

attacks#:~:text=Slowloris%20is%20an%20application%20layer%20DDoS%20attack%20which,Slowloris%20Attack%3F%20%7C%20NETSCOUT%20Saltar%20al%20contenido%20principal

Nikolic, A. (s.f.). *NMAP.ORG*. Recuperado el 25 de Julio de 2020, de File http-slowloris-check: https://nmap.org/nsedoc/scripts/http-slowloris-check.html

Nilotex. (2020). *Conócenos*. Recuperado el 09 de Marzo de 2020, de http://www.nilotex.com/conocenos.html

NMAP.ORG. (s.f.). *Nmap Network Scanning*. Recuperado el 11 de Agosto de 2020, de Chapter 9. Nmap Scripting Engine: https://nmap.org/book/nse-usage.html

NMAP.ORG. (s.f.). *NMAP.ORG*. Recuperado el 24 de Julio de 2020, de Script Discovery: https://nmap.org/nsedoc/categories/discovery.html

NMAP.ORG. (s.f.). *Script Safe*. Recuperado el 24 de Julio de 2020, de https://nmap.org/nsedoc/categories/safe.html

NMAP.ORG. (s.f.). *Script Safe*. Recuperado el 24 de Julio de 2020, de https://nmap.org/nsedoc/categories/safe.html

NMAP.ORG. (s.f.). *Script Vuln*. Recuperado el 25 de Julio de 2020, de https://nmap.org/nsedoc/categories/vuln.html

OffSec Services Limited. (s.f.). *KALI*. Recuperado el 02 de Marzo de 2020, de ¿Qué es Kali Linux?: https://www.kali.org/docs/introduction/what-is-kali-linux/

Orcero, D. S. (2018). Kali Linux. En D. S. Orcero, *Kali Linux* (pág. 15). Madrid, España: Ra-Ma. Recuperado el 02 de Marzo de 2020

Ostec. (s.f.). *Pentest: ¿qué es y cuáles son los principales tipos?* Recuperado el 10 de Marzo de 2020, de ¿Qué es el Pentest?: https://ostec.blog/es/seguridad-perimetral/pentest-concepto-tipos

Oweis, M. (20 de Mayo de 2015). *HubPages*. Recuperado el 29 de Julio de 2020, de Another SSL major flow – LOGJAM attack: https://hubpages.com/technology/Another-SSL-major-flow-LOGJAM-attack

P. Eronen, E. (Febrero de 2009). *DES and IDEA Cipher Suites for Transport Layer Security (TLS)*. Recuperado el 24 de Julio de 2020, de IDEA Cipher Suite: https://tools.ietf.org/html/rfc5469

pagvac. (s.f.). *KALI TOOLS*. Recuperado el 15 de Junio de 2020, de dnsmap Package Description: https://tools.kali.org/information-gathering/dnsmap

pentestmonkey. (s.f.). *KaliTools*. Recuperado el 20 de Julio de 2020, de smtp-user-enum Package Description: https://tools.kali.org/information-gathering/smtp-user-enum

Perez, C. (18 de Febrero de 2014). *KALI TOOLS*. Recuperado el 15 de Junio de 2020, de DNSRecon Package Description: https://tools.kali.org/information-gathering/dnsrecon

Perta, C. (s.f.). *NMAP.ORG*. Recuperado el 25 de Julio de 2020, de File ssl-ccs-injection: https://nmap.org/nsedoc/scripts/ssl-ccs-injection.html

Pillai, S. (24 de Febrero de 2013). */ROOT.IN~*. Recuperado el 27 de Julio de 2020, de SLOWLORIS: HTTP DOS(Denial Of Service)attack and prevention: https://www.slashroot.in/slowloris-http-dosdenial-serviceattack-and-prevention

Prenafeta, J. (23 de Agosto de 2018). *Hiberus Tecnologia*. Recuperado el 11 de Marzo de 2020, de Qué es pentesting y cómo detectar y prevenir ciberataques: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/

q-bo. (23 de Julio de 2018). *Origen de las normas ISO*. Recuperado el 21 de Enero de 2020, de Historia y antecedentes de las normas ISO: https://q-bo.org/origen-de-las-normas-iso/

Raul Siles, T. S. (s.f.). *KaliTools*. Recuperado el 20 de Julio de 2020, de TLSSLed Package Description: https://tools.kali.org/information-gathering/tlssled

Rowley, J. (9 de Abril de 2014). *CA Security COUNCIL*. Recuperado el 29 de Julio de 2020, de Heartbleed Bug Vulnerability: Discovery, Impact and Solution: https://casecurity.org/2014/04/09/heartbleed-bug-vulnerability-discovery-impact-and-solution/#:~:text=%20The%20features%20of%20the%20Heartbleed%20bug%20that,not%20rely%20on%20other%20vulnerabilities%20to...%20More%20

RSnake. (s.f.). *KALI TOOLS*. Recuperado el 15 de Junio de 2020, de Fierce Package Description: https://tools.kali.org/information-gathering/fierce

Schneier en Seguridad. (21 de Mayo de 2015). *Schneier en Seguridad*. Recuperado el 29 de Julio de 2020, de The Logjam (and Another) Vulnerability against Diffie-Hellman Key Exchange: https://www.schneier.com/blog/archives/2015/05/the_logjam_and_.html

SONICWALL. (26 de Marzo de 2020). *APOYO*. Recuperado el 24 de Julio de 2020, de SWEET32 Vulnerabilidad De Cifrados De 64 Bits (3DES/Blowfish) - CVE-2016-2183: https://www.sonicwall.com/support/knowledge-base/sweet32-vulnerability-of-64-bit-ciphers-3des-blowfish-cve-2016-2183/170505312196945/

SONICWALL. (26 de Marzo de 2020). *APOYO*. Recuperado el 27 de Julio de 2020, de SWEET32 Vulnerability Of 64 Bit Ciphers (3DES/Blowfish) - CVE-2016-2183: https://www.sonicwall.com/support/knowledge-base/sweet32-vulnerability-of-64-bit-ciphers-3des-blowfish-cve-2016-2183/170505312196945/

SSL247. (2020). *Tests de penetración realizados por nuestros expertos certificados*. Recuperado el 10 de Marzo de 2020, de ¿Qué es un test de penetración?: https://www.ssl247.es/test-penetracion

SSSL Shopper. (19 de Octubre de 2008). Obtenido de Cómo deshabilitar SSL 2.0 y SSL 3.0 en IIS 7: https://www.sslshopper.com/article-how-to-disable-ssl-2.0-in-iis-7.html

The Heartbleed Bug. (03 de Junio de 2020). *The Heartbleed Bug*. Recuperado el 29 de Julio de 2020, de The Heartbleed Bug: https://heartbleed.com/

Upgrade hub TECH & JOB. (11 de Septiembre de 2019). *Blog*. Recuperado el 11 de Marzo de 2020, de El pentest como método de protección para las empresas: https://upgrade-hub.com/pentest-metodo-proteccion-empresas/

Velasco, R. (13 de Enero de 2014). *RZ redes zone*. Recuperado el 20 de Julio de 2020, de Comprueba la seguridad de una conexión SSL con SSLScan: https://www.redeszone.net/2014/01/13/comprueba-la-seguridad-de-una-conexion-ssl-con-sslscan/

weakdh.org. (15 de Mayo de 2015). *weakdh.org*. Recuperado el 29 de Julio de 2020, de Diffie-Hellman débil y el ataque de Logjam: https://weakdh.org/

welivesecurity by ESET. (9 de Octubre de 2014). *¿Sabes qué es un exploit y cómo funciona?* Recuperado el 11 de Agosto de 2020, de Tipos de exploits: https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/

Yonfá, J. A. (01 de 05 de 2020). PenTesting. Quito, Pichincha, Ecuador.