

DESCUBRIMIENTO Y ANALISIS DE VULNERABILIDADES INFORMÁTICAS SOBRE LOS  
SERVIDORES DE UNA EMPRESA PRIVADA EN BOGOTÁ

PRESENTADO POR:

DIANA MARCELA BARRERA FLÓREZ

DIANA ISABEL MUNAR GUERRERO

CARLOS ENRIQUE MOGOLLÓN CAMARGO

ASESOR TÉCNICO DE PROYECTO:

Ingeniero Eduardo Chavarro Ovalle

UNIVERSIDAD EL BOSQUE

FACULTAD DE INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMÁTICAS

BOGOTÁ, COLOMBIA

5 DE JULIO DE 2019

## DEDICATORIA

A Dios por darnos la fuerza y voluntad para lograr esta meta, a nuestras familias por compartir los momentos de dedicación de estudio para nuestro crecimiento profesional

## AGRADECIMIENTOS

A Dios, a nuestras familias por su constante apoyo y motivación para el desarrollo de este proyecto.

A la empresa privada que nos brindó la oportunidad de desarrollar este proyecto sobre un entorno real y nos apoyó durante todo el proceso.

A nuestro asesor externo que nos guio durante todo el trayecto del trabajo.

A nuestro tutor de la Universidad quien siempre estuvo dispuesto a orientarnos para el desarrollo de este proyecto.

A todos por ellos porque desempeñaron un papel fundamental y permitieron que finalizáramos exitosamente este proyecto lo cual contribuyó a nuestra formación profesional a lo largo de este año.

## RESUMEN

A través de este proyecto se busca identificar vulnerabilidades con Nessus, sobre los servidores de una empresa privada en Bogotá, analizar los resultados y realizar pruebas manuales de las vulnerabilidades obtenidas de los servidores evaluados para certificar que estas no sean falsos positivos. A partir de ello diseñar un plan de remediación para la compañía que responda a los resultados obtenidos.

Con lo anterior se busca contribuir a la empresa en el proceso de certificación de la norma ISO 27001 para que los resultados obtenidos de este proyecto sean el insumo que permita cumplir con el control de gestión de vulnerabilidades técnicas (A12.6).

El objetivo principal de este proyecto es poder efectuar recomendaciones generales referentes al análisis de vulnerabilidades informáticas sobre los servidores de una empresa, utilizando herramientas Open Source. La metodología propuesta consiste en realizar una investigación inicial referente a las herramientas adecuadas para la evaluación de las vulnerabilidades informáticas, posteriormente realizar un análisis de resultados obtenidos en pruebas realizadas sobre los servidores con varias herramientas Open Source, así como proponer soluciones que permitan gestionar las vulnerabilidades informáticas y lograr diseñar un plan de remediación para la empresa. Se llega a la conclusión que la metodología adoptada y las herramientas utilizadas entregan información valiosa y verídica, lo que permite lograr un mejor punto de vista para tomar decisiones y reducir en gran parte los riesgos de la seguridad informática.

## PALABRAS CLAVE

Vulnerabilidad, seguridad informática, Open Source, amenaza, seguridad de la información, ciberataque, remediación, Nessus.

## **ABSTRACT**

Through this project the main objective is to identify vulnerabilities with Nessus Tool for the servers of a private company in Bogotá, analyze this results and perform manual tests of the vulnerabilities obtained to verify that these are not false positives. Based on this it will be designed a remediation plan for the company that responds to the results. The purpose with the above is to contribute to the company in the process of certification of the ISO 27001 standard for the results of this project is due to a management control of technical vulnerabilities (A12.6).

The main objective of this work is to make general recommendations concerning the analysis of computer vulnerabilities on the servers of a company, using Open Source tools. The proposed methodology consists of making an initial enquiry concerning the appropriate tools for the assessment of computer vulnerabilities, then an analysis of results obtained in tests performed on servers, as well as propose solutions that enable managing computer vulnerabilities and to design a remediation plan for the company. It is concluded that the methodology adopted, and the tools used provide valuable and truthful information, which allows for a better perspective for to make decisions and reduce the risks of computer security.

## **KEYWORDS**

Vulnerability, computer security, Open Source, threat, information security, cyberattack, remediation, Nessus.

## Tabla de Contenido

RESUMEN .....	1
PALABRAS CLAVE .....	1
ABSTRACT .....	2
KEYWORDS .....	2
1. Título.....	10
2. Introducción.....	10
3. Descripción general del proyecto.....	10
3.1 Definición del problema.....	11
3.1.1 Manifestación.....	11
3.1.2 Contexto.....	12
3.1.3 Causas .....	13
3.1.4 Efectos .....	13
3.2 Aspectos a solucionar .....	13
3.3 Solución propuesta .....	13
4. Estado del arte .....	14
4.1 Marco de referencia teórico .....	14
4.1.1 Procedimiento de gestión de vulnerabilidades .....	15
4.1.2 Vulnerabilidad .....	16
4.1.3 Análisis de riesgos .....	16
4.1.4 CVSS (Common vulnerability score system) .....	17
4.1.5 OWASP.....	21
4.2 Marco de referencia tecnológico.....	24
4.2.1 OSSTM .....	24
4.2.2 Nessus .....	25
4.2.3 Nmap .....	26
4.2.4 Zenmap.....	27
4.2.5 Retina .....	27
5. Glosario de términos .....	28
6. Justificación .....	33

7.	Objetivos .....	34
7.1.	General .....	34
7.2.	Específicos .....	34
8.	Requerimientos .....	34
8.1	Requerimientos funcionales .....	34
8.2	Requerimientos no funcionales .....	35
9.	Metodología .....	36
9.1	Aprobación para la evaluación de vulnerabilidades .....	37
9.2	Generar un inventario de activos.....	37
9.3	Recopilación de información .....	37
9.3.1	Fase escaneos en prueba .....	38
9.3.2	Fase escaneos en producción .....	39
9.4	Definir el alcance de la evaluación .....	39
9.5	Ejecución de las pruebas.....	40
9.6	Generar un informe de resultados.....	40
9.7	Generar un plan de remediación .....	41
9.8	Ejecución de plan de acción .....	41
9.9	Verificación de la efectividad .....	41
9.10	Socialización de resultados con los interesados.....	41
10.	Capítulos de desarrollo .....	42
10.1	Acuerdos para la evaluación de las vulnerabilidades.....	42
10.2	Escaneos sobre los servidores en fase de prueba.....	44
10.2.1	Pruebas realizadas el 15 de febrero de 2019 .....	47
10.2.2	Pruebas realizadas semana 25 febrero - 3 marzo de 2019 .....	48
10.2.3	Pruebas realizadas semana 4 marzo-10 marzo de 2019.....	50
10.2.4	Pruebas realizadas 3semana 11 marzo-17 marzo de 2019 .....	52
10.3	Escaneos sobre los servidores en producción .....	53
10.3.1	Pruebas realizadas semana 1 de Abril de 2019 .....	58
10.3.2	Ejecución de las pruebas .....	60
10.3.3	Revisión conexiones activas .....	63

10.3.4 Revisión de puertos abiertos/cerrados(nmap/zenmap) .....	64
10.3.5 Pruebas de conectividad (ping) .....	65
10.3.6 Escaneo con Nessus.....	66
10.3.7 Pruebas manuales .....	70
11. Resultados .....	81
11.1 Criticidad de vulnerabilidades.....	82
11.2 Vulnerabilidades de acuerdo a criticidad .....	83
11.2 Vulnerabilidades en cada servidor .....	84
11.3 Vulnerabilidades en servidor por criticidad .....	85
11.4 Vulnerabilidades según la familia.....	86
11.5 Vulnerabilidades según sistema operativo .....	87
12. Discusión .....	88
13. Conclusiones .....	90
14. Documentación de Referencia .....	92
15. Glosario .....	95
16. Anexos .....	101

## Índice de Figuras

Figura 1. Nivel gráfico grupo de métricas.....	20
Figura 2. Métricas de puntuación base (base score metrics) .....	20
Figura 3. OWASP Top 10 en 2017 .....	22
Figura 4. Tiempo vs. Costo en testeo de seguridad de Internet .....	25
Figura 5. Diagrama general de servidores a escanear fase de pruebas .....	38
Figura 6. Diagrama general de servidores a escanear fase de desarrollo .....	39
Figura 7. Acceso conexión VPN.....	42
Figura 8. Revisión con Netstat IP: *.*.110.2 .....	44
Figura 9. Revisión con netstat IP: *.*.200.50.....	44
Figura 10. Revisión con netstat IP: *.*.110.3.....	44
Figura 11. Revisión con netstat IP: *.*.200.51 .....	45
Figura 12. Escaneo con Zenmap - IP *.*.110.2 y *.*.200.51 (Anexo 8 - Escaneo Zenmap) .....	45
Figura 13. Tabla de enrutamiento e interfaces (Anexo 9 - Enrutamiento de la red).....	46
Figura 14. Escaneo con herramienta Nessus ( Anexo 11 - Escaneo Nessus 15Feb) .....	47
Figura 15. Escaneo múltiple con herramienta Nessus ( Anexo 12 - Pruebas Feb25 Mar03 ) .....	48
Figura 16. Escaneo múltiple con herramienta Nessus ( Anexo 13 - Escaneo Múltiple ) .....	49
Figura 17. Escaneo múltiple con herramienta Retina ( Anexo 14 - Escaneo Retina ) .....	50
Figura 18. Escaneo simple con herramienta Nessus ( Anexo 15 - Pruebas Mar04) .....	51
Figura 19. Escaneo simple con herramienta Nessus – Kali Linux .....	51
Figura 20. Escaneo simple con herramienta Retina (Anexo 16- Pruebas Mar11-17 Retina) .....	52
Figura 21. Escaneo simple con herramienta Nessus – Service Discovery.....	54
Figura 22. Escaneo simple con herramienta Nessus – Host Discovery.....	54
Figura 23. Escaneo simple con herramienta Nessus – Service Discovery.....	55
Figura 24. Escaneo simple con herramienta Nessus – Fuerza bruta.....	55
Figura 25. Escaneo simple con herramienta Nessus – Aplicaciones Web .....	56
Figura 26. Escaneo simple con herramienta Nessus – Service Discovery .....	56
Figura 27. Escaneo simple con herramienta Nessus – Windows .....	57
Figura 28. Escaneo simple con herramienta Nessus .....	57
Figura 29. Evidencia vulnerabilidad CVE-2007-6750 sobre todos servidores rango .100 .....	58
Figura 30. Evidencia vulnerabilidad CVE-2012-2122 sobre todos servidores rango .200 .....	58
Figura 31. Evidencia falla escaneos en Linux.....	59

Figura 32. Evidencia 28 Abril .....	59
Figura 33. Nmap Windows 7 .....	59
Figura 34. Nessus Windows 7 .....	59
Figura 35. Conexión a la VPN establecida .....	60
Figura 36. Verificación de conexión a la VPN.....	61
Figura 37. Desconexión de la VPN.....	61
Figura 38. Evidencia conexión IP *.*.100.10 del rango de IPs .100.....	62
Figura 39. Evidencia conexión IP *.*.110.3 del rango de IPs .110.....	62
Figura 40. Prueba conexión IP *.*.200.10 del rango de IPs .200 .....	62
Figura 41. Revisión conexiones activas (Nestat) .....	63
Figura 42. Revisión conexiones activas (Nestat) .....	64
Figura 43. Revisión conexiones activas (Nestat) .....	64
Figura 44. Prueba de conectividad respuesta por ping rango .100.....	65
Figura 45. Prueba de conectividad respuesta por ping rango .110 .....	65
Figura 46. Prueba de conectividad respuesta por ping rango .200 .....	65
Figura 47. Tabla de enrutamiento e interfaces .....	66
Figura 48. Escaneo sobre Nessus rango .100 .....	67
Figura 49. Escaneo sobre Nessus rango .100 .....	67
Figura 50. Escaneo sobre Nessus rango .100 .....	68
Figura 51. Prueba manual – Ingreso a Intranet de la empresa .....	70
Figura 52. Prueba manual - Plugin 49067 .....	71
Figura 53. Prueba manual - Plugin 46803 .....	71
Figura 54. Prueba manual - Puerto 443 Index.....	72
Figura 55. Prueba manual - Puerto 443 Index.....	74
Figura 56. Prueba manual - Plugin 106375 .....	74
Figura 57. Prueba manual - Puerto 9080 pasa a 9443.....	75
Figura 58. Prueba manual - Puerto 9080 pasa a 9443.....	76
Figura 59. Prueba manual - Puerto 9080 pasa a 9443.....	76
Figura 60. Prueba manual – Plugin 106375 .....	77
Figura 61. Prueba manual – Puerto 9943.....	77
Figura 62. Plugin 117665 .....	77
Figura 63. Plugin 117665 – Puerto 9200 .....	78

Figura 64. Pluggin 85582 .....	78
Figura 65. Prueba manual - Pluggin 85582 - *.*.100.15/install/ .....	79
Figura 66. Prueba manual – Puerto 8083.....	79
Figura 67. Prueba manual - Plugin10662 .....	80
Figura 68. Plugin 12479 .....	80
Figura 69. Plugin 50344 .....	80
Figura 70. Plugin 50344 Puerto 8080 .....	81
Figura 71. Vulnerabilidades detectadas.....	82
Figura 72. Vulnerabilidades por criticidad.....	83
Figura 73. Vulnerabilidades en servidores .....	84
Figura 74. Vulnerabilidades en servidores por criticidad .....	85
Figura 75. Vulnerabilidades según familia .....	86
Figura 76. Vulnerabilidades según sistema operativo por criticidad .....	87

## Índice de Tablas

Tabla 1. Control 12.6 de la Norma ISO 27001 [4].....	16
Tabla 2. Criticidad y Score CVSS .....	18
Tabla 3. Características equipos de trabajo para realizar los escaneos de vulnerabilidades .....	35
Tabla 4. Herramientas de escaneo seleccionadas .....	43
Tabla 5. Resultados Zenmap sobre los 4 servidores.....	46
Tabla 6. Resultados herramienta Nessus consolidado en tabla Excel .....	48
Tabla 7. Resultados consolidados herramienta Nessus .....	49
Tabla 8. Resultados herramienta Retina .....	50
Tabla 9. Resultados herramienta Nessus .....	51
Tabla 10. Resultados herramienta Nessus – Kali Linux.....	52
Tabla 11. Resultados herramienta Retina .....	53
Tabla 12. Inventario de Activos ( Anexo 17 - Inventario de activos).....	69
Tabla 13. Escaneos consolidados sobre Excel (Anexo 18 - Registro fase producción).....	70
Tabla 14. Tabla consolidada para Plan de Remediación ( Anexo 22 - Remediación).....	89

## **1. Título**

DESCUBRIMIENTO Y ANALISIS DE VULNERABILIDADES INFORMÁTICAS SOBRE LOS SERVIDORES DE UNA EMPRESA PRIVADA EN BOGOTÁ

## **2. Introducción**

En los últimos años se ha visto un auge/crecimiento en la evolución y sofisticación de las amenazas a los sistemas informáticos y su impacto negativo en los activos de información de las diferentes organizaciones que sin importar el sector son objetivo de los ciberdelincuentes que buscan comprometer los 3 pilares de seguridad de la información: Disponibilidad, Integridad y Confidencialidad, a través de buscar fallas en los sistemas o explotar vulnerabilidades que no han sido identificadas o parchadas. Así pueden surgir interrogantes para las organizaciones tales como: ¿Se está protegido ante ataques maliciosos?; Es la red segura para el envío de información? ¿Se cuenta con planes de continuidad en caso de que ocurra algún incidente que afecte la operación? Hoy en día, las vulnerabilidades y el riesgo que corre la información a aumentado a gran escala y según las estadísticas o estimaciones cada día se generan más ataques a la operatividad de los negocios en cuanto a la información se refiere. [1]

Teniendo en cuenta lo anterior el objetivo de este proyecto es apoyar a una empresa privada en Bogotá en el descubrimiento y análisis de vulnerabilidades sobre servidores críticos con el fin de generar un plan de remediación que les permita atender lo anterior y de esta manera contribuir en el proceso de certificación de la norma ISO 27001 para que los resultados obtenidos de este proyecto sean el insumo que permita cumplir con el control de gestión de vulnerabilidades técnicas (A12.6).

## **3. Descripción general del proyecto**

Las empresas hoy en día priorizan la seguridad de la información, debido a que se considera el activo más valioso, el cual debe ser protegido para garantizar la continuidad del negocio. No existe un sistema completamente seguro, cada día aparecen nuevas amenazas y riesgos de seguridad que se pueden volver eventos críticos que afecten los activos que custodia la organización y así comprometer la confidencialidad, integridad y disponibilidad de los datos.

Ejercer supervisión sobre las vulnerabilidades informáticas que se puedan presentar es fundamental para cumplir con lo anterior. Por ello es muy importante contar con procedimientos que se puedan aplicar ante cualquier evento de seguridad que se presente y que pueda disminuir la probabilidad de ocurrencia de las vulnerabilidades.

El desarrollo de este proyecto se basa en el análisis de vulnerabilidades informáticas sobre 30 servidores de una empresa privada de la ciudad de Bogotá, los cuales se escogieron por la empresa a desarrollar el proyecto junto con los estudiantes con el fin de cumplir la necesidad actual, para ello se emplearan algunas herramientas Open Source para identificar estas vulnerabilidades y así plasmar en el documento, un procedimiento (detección, análisis y plan de remediación de vulnerabilidades identificadas sobre los servidores) que pueda ser gestionado correctamente por parte de la compañía según los elementos encontrados para el desarrollo del proyecto y que sea la base para atender futuras amenazas.

### **3.1 Definición del problema**

Se han superado distintas fases de madurez corporativa, pero nunca se ha logrado consolidar el proyecto de la implementación de la norma ISO 27001 al 100%, enfocado en el control de gestión de vulnerabilidades. Existe incertidumbre/preocupación sobre el estado de seguridad de algunos servidores ya que se desconoce si pueden tener alguna vulnerabilidad que afecten la continuidad del negocio. Así mismo no existe un procedimiento técnico que oriente en cómo se debería realizar las pruebas de vulnerabilidades y bajo qué criterios. Es por ello que con este proyecto se busca atender esta situación y que la información obtenida sea el insumo correspondiente del control de gestión de vulnerabilidades técnicas (A12.6) requerido en la norma.

#### **3.1.1 Manifestación**

Desde el año 2007 la empresa inicio los esfuerzos en materia de seguridad de la información hacia la norma ISO 27001. Se han presentado incidentes que afectan la compañía y algunos de ellos se han materializado (se encuentra en los registros de monitoreo/seguridad; tecnológicos de la compañía los cuales son protegidos bajo) desde el área de TI de la compañía se ha manifestado la necesidad de tener un procedimiento técnico sobre evaluación de vulnerabilidades informáticas, el cual pueda ser aplicado por los Ingenieros encargados para

conocer el estado de seguridad de algunos servidores de la empresa y así identificar si son o no vulnerables ante alguna amenaza de seguridad.

La organización cuenta con un proceso de gestión de riesgos y esto ha permitido llevar a cabo planes de tratamiento de los mismos para su disminución, entre los más relevantes que nos mencionaron está la manipulación no autorizada de información, ataques de denegación de servicio, ataques de web defacement (modificación de una página web sin autorización del propietario).

Además, en la compañía existen procesos que definen el ciclo de seguridad de la información enmarcado dentro de la norma, lo cual permite controlar y detectar a tiempo los riesgos que puedan presentarse para mitigarlos o eliminarlos, así como el uso de herramientas para la identificación y priorización de vulnerabilidades.

### **3.1.2 Contexto**

La Empresa en la cual se desarrollará este proyecto ofrece servicios de desarrollo de software, gestión de riesgos y monitoreo de vehículos, al sector logístico y transporte. A través de la prestación de servicios en soluciones en gerencia de riesgos, soluciones digitales y asistencia logística para el seguro de transporte y cadena de suministros. Tiene una compleja infraestructura, con red certificada, cuenta con Firewall Perimetral, Antivirus y plataformas de seguridad integrada, así como herramientas de monitoreo de la infraestructura. La Empresa está certificada en IT Mark que consiste en un capítulo de seguridad de la información, donde se garantizan controles de clasificación de seguridad de los activos de información. La empresa tiene dos (2) sedes y cada una cuenta con protección perimetral. En cada sede existen aproximadamente entre cincuenta (50) y setenta (70) estaciones de trabajo. Cuenta con servicios VoIP, Directorio Activo, servicio de impresión y correo electrónico web. Los servidores en la nube que serán objetos de evaluación, cuenta con medidas de protección de un DataCenter TIER 3.

### **3.1.3 Causas**

La metodología para el proceso de gestión de amenazas y vulnerabilidades en los servidores y en las aplicaciones web, está pendiente por organizar. La Empresa actualmente está vinculada a varios procesos de implementación tanto de la norma ISO 27001 como de una herramienta de seguridad integrada para atender varios procesos que aún no está desplegada completamente. Teniendo en cuenta lo anterior hay varias actividades en curso que requieren bastante personal para atenderlas, lo cual demanda una gran quitar cantidad de tiempo, que excede la capacidad operativa con la que cuenta actualmente la Empresa, por tanto se requiere mano de obra (estudiantes del proyecto a desarrollar) que contribuya a cumplir con estos objetivos en mejora de la unidad del negocio.

### **3.1.4 Efectos**

Hay incertidumbre sobre el estado de seguridad de los servidores mencionados en el contexto, ya que pueden tener vulnerabilidades que afecten la seguridad de la organización y repercutan negativamente en la implementación que se está ejecutando paralelamente en la organización. Existe la posibilidad de que se materialicen riesgos identificados por la compañía, impactando la credibilidad de la organización y la confianza en los servicios que afecte a la credibilidad de la organización. Podría también existir pérdidas económicas o podría generar demandas por incumplimientos de contratos.

## **3.2 Aspectos a solucionar**

La seguridad se incluye en un proceso cíclico y de mejora continua, por tanto, es importante enmarcar la empresa en un proceso estructurado y organizado para la implementación de la norma ISO 27001 que permita gestionar riesgos de forma sistematizada y controlada, creando para la empresa un procedimiento técnico para la evaluación de vulnerabilidades informáticas.

## **3.3 Solución propuesta**

Con el fin de atender la problemática manifestada por la empresa, se utilizarán herramientas para identificar vulnerabilidades sobre algunos servidores de la empresa, se realizará un análisis y se definirá un plan de remediación de acuerdo a lo encontrado, el cual quedará

enmarcado bajo un procedimiento como guía a seguir para futuros usos. Con lo anterior la Empresa podrá mejorar la postura de seguridad en la organización, organizar las metodologías existentes de procesos e ir en concordancia con los controles de seguridad de la cláusula gestión de vulnerabilidades a aplicar de la norma ISO 27001.

Se trabajará el escaneo de vulnerabilidades en dos fases, la primera consiste en escaneos de prueba sobre 4 servidores con el fin de identificar cual es el perfil de escaneo adecuado y realizar una exploración. Posteriormente se realizar de forma periódica escaneos de vulnerabilidades en los servidores de la Empresa, por medio de algunas herramientas OpenSource, para identificar cuáles son críticas y recurrentes y que esta sea la base para el procedimiento a implementar. Del resultado de estos escaneos se podrá conocer en detalle el estado de la seguridad del entorno a evaluar, el alcance e impacto de posibles intrusiones y así poder validar la correlación existente entre y vulnerabilidades identificadas.

## **4. Estado del arte**

### **4.1 Marco de referencia teórico**

La seguridad de la información digital para una organización es importante tratarla desde varios aspectos: físico, donde se encuentra alojada la información; el social, relacionado con la sensibilización que tiene el personal que manipula la información, y el lógico, que se refiere a la configuración de sus niveles de disponibilidad. Justo así se intenta crear un esquema seguro el cual se debe ajustar a los niveles de confidencialidad, integridad y disponibilidad de la información, según la norma ISO 27001.

En la actualidad, la determinación del nivel de inseguridad (visto desde la óptica de vulnerabilidad y riesgo) de la información trasciende los niveles de su uso u operatividad, de forma que es necesario interpretar sus unidades de portabilidad y los medios por los que se transmite, donde se abren nuevas configuraciones al fraude, a la alteración y al uso indebido; esto ha guiado al asentamiento de áreas forenses, cibercrimen e inteligencia sobre la información.

Toda organización ha presentado o presenta actualmente inconvenientes en la seguridad de la información, la falta de protección, falta de conocimiento de herramientas y lograr la mejor

forma de salvaguardar la información es de forma redundante o repetitiva, lo cual puede afectar al sistema económico y hasta generar pérdida de tiempo en la recuperación de la información. Es importante trabajar sobre los tres pilares de la seguridad de la información confidencialidad, integridad y disponibilidad de los sistemas informáticos necesarios para mantener las operaciones y que se acople con la norma ISO 27001.

"El informe anual de Symantec (ISTR), que analiza 157 países, reveló que en 2017 Colombia fue el sexto país de Latinoamérica con el mayor número de ataques cibernéticos detectados, bajando dos posiciones en comparación al 2016, cuando ocupó el cuarto lugar". [2] Hoy en día, las vulnerabilidades y el riesgo que corre la información a aumentado a gran escala y según las estadísticas o estimaciones cada día se generan más ataques a la operatividad de los negocios en cuanto a la información se refiere, y de acuerdo a estos resultados se ha incrementado y evolucionado el campo de la seguridad en todas las distintas áreas (forenses, cibercriminal, administración de sistemas de gestión de seguridad).

[3]"En Colombia, gracias a las estrategias desarrolladas por el Min TIC, durante el primer trimestre de 2017, se cuenta con una cifra de veintiocho millones de conexiones a internet de banda ancha, lo que evidencia un aumento considerable en la economía digital del país". La seguridad de la información digital para una organización es importante tratarla desde varios aspectos: físico, donde se encuentra alojada la información; el social, relacionado con la sensibilización que tiene el personal que manipula la información, y el lógico, que se refiere a la configuración de sus niveles de disponibilidad. Justo así se intenta crear un esquema seguro el cual se debe ajustar a los niveles de confidencialidad, integridad y disponibilidad de la información, según la norma ISO 27001.

#### **4.1.1 Procedimiento de gestión de vulnerabilidades**

Es un documento que incluye las fases para la realización de la evaluación (análisis) de vulnerabilidades de activos de una infraestructura tecnológica, en el cual se encuentran las debilidades de las plataformas de software o hardware para solucionar las fallas, antes de que puedan generar un impacto negativo o las materializaciones de eventos indeseados e inesperados.

En la norma ISO 27001 existe un control sobre la gestión de vulnerabilidades técnicas como se describe a continuación:

Tabla 1. Control 12.6 de la Norma ISO 27001 [4]

A.12.6	Gestión de la vulnerabilidad técnica	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.

#### 4.1.2 Vulnerabilidad

Punto débil en la seguridad de un sistema informático que permiten que un atacante comprometa la integridad, disponibilidad, confidencialidad de la información.

- Defecto en el desarrollo del software o mala configuración en un sistema que podría ser explotada por una potencial fuente de amenaza para ocasionar algún tipo de daño.
- Materialización de una amenaza en un sistema informático, que puede provocar pérdida o daño de la información.
- Debilidad que se encuentra en un activo o control y que puede ser explotada por una o más amenazas lo que deriva en un riesgo de seguridad.

Se encuentran organizados por códigos universales (CVE,CVSS). En general las vulnerabilidades pueden encontrarse en los sistemas porque pueden contener agujeros de seguridad conocidos y desconocidos (vulnerabilidades *0-day*), cuentan con configuraciones por defecto o son el resultado de errores de configuración. [5]

#### 4.1.3 Análisis de riesgos

Es parte del SGSI, que permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la

medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información. Son muchas las metodologías utilizadas para la gestión de riesgos, pero todas parten de un punto común: la identificación de activos de información Sobre estos activos de información es que hace la identificación de las amenazas o riesgos y las vulnerabilidades valoración para determinar cuáles son los más críticos para la empresa. Esta valoración suele hacerse en términos de la posibilidad de ocurrencia del riesgo y del impacto que tenga la materialización del riesgo. La valoración del impacto puede medirse en función de varios factores: la pérdida económica si es posible cuantificar la cantidad de dinero que se pierde, la reputación de la empresa dependiendo si el riesgo pueda afectar la imagen de la empresa en el mercado o de acuerdo al nivel de afectación por la pérdida o daño de la información. Una vez identificadas las amenazas, lo más importante del análisis de riesgos es la identificación de controles ya sea para mitigar la posibilidad de ocurrencia de la amenaza o para mitigar su impacto. Las medidas de control que puede asumir una empresa van a estar relacionadas con el tipo de amenaza y el nivel de exposición que represente para la información corporativa. Una empresa puede afrontar un riesgo de cuatro formas diferentes: aceptarlo, transferirlo, mitigarlo o evitarlo. Si un riesgo no es lo suficientemente crítico para la empresa la medida de control puede ser Aceptarlo, es decir, ser consciente de que el riesgo existe y hacer un monitoreo sobre él. Si el riesgo representa una amenaza importante para la seguridad de la información se puede tomar la decisión de Transferir o Mitigar el riesgo. Finalmente, si el nivel de riesgo es demasiado alto para que la empresa lo asuma, puede optar por Evitar el riesgo, eliminando los activos de información o la actividad asociada. a gestión de riesgos debe garantizarle a la empresa la tranquilidad de tener identificados sus riesgos y los controles que le van a permitir actuar ante una eventual materialización o simplemente evitar que se presenten. Esta gestión debe mantener el equilibrio entre el costo que tiene una actividad de control, la importancia del activo de información para los procesos de la empresa y el nivel de criticidad del riesgo. [6]

#### **4.1.4 CVSS (Common vulnerability score system)**

[7] El Sistema de puntuación de vulnerabilidad común (CVSS) proporciona una manera de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad. La puntuación numérica se puede traducir a una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar

adecuadamente sus procesos de gestión de vulnerabilidades. CVSS es un estándar publicado utilizado por organizaciones de todo el mundo, se encuentra actualmente en la versión 3.0.

Está bajo la custodia de FIRST (fórum of incident response and security teams) pero es un estándar abierto que se puede utilizar libremente. [8]

Luego de asignar valores a las métricas base, la fórmula puede tener como resultado una puntuación que oscila entre 0.0 y 10.0, mismo que representa la severidad de la vulnerabilidad en cuestión. La severidad puede ser baja, media, alta, crítica si el puntaje obtenido luego de aplicar la formula CVSS está en la escala(score) de la siguiente tabla.

Tabla 2. Criticidad y Score CVSS

Severidad	CVSS Score
Nula	0
Bajo	0,1 a 3,9
Medio	4,0 a 6,9
Alto	7,0 a 8,9
Critica	9,0 a 10

Aunque se trata de una guía oficial, las organizaciones pueden modificarla y aplicar su propia escala, pero siempre manteniendo la misma escala para todas las evaluaciones.

Es importante mencionar que la correspondencia entre las categorías cualitativas y cuantitativas solo se aplica si son evaluadas solo las métricas base, o en caso contrario si se consideran todas las métricas de los tres grupos: base, temporal y de entorno.

[9]Para calcular un puntaje asociado a una vulnerabilidad, CVSS utiliza métricas: base, temporal y de entorno, cada una se conforma a su vez de un conjunto de otras métricas, como lo veremos a continuación (sin embargo, este valor de Score sale en el reporte de escaneos)

La severidad de las tres métricas mide la manera en la que una vulnerabilidad, si se

explota, afecta de forma directa a los activos de TI. Los impactos se determinan de manera independiente, como el grado de pérdida de confidencialidad, integridad y disponibilidad, ya que una vulnerabilidad podría causar pérdida parcial de integridad y disponibilidad, pero tal vez no afecte la confidencialidad.

**Métricas Base:** Representan las características intrínsecas a la vulnerabilidad, que son constantes en el tiempo y en el entorno del usuario. Incluyen las métricas de vector de acceso, complejidad de acceso y autenticación, de manera que permiten definir cómo se puede acceder a una vulnerabilidad y si se cumplen las condiciones para ser explotada.

**Métricas Temporales.:** Representan las características de una vulnerabilidad que pueden cambiar en el tiempo, pero que son constantes en el ambiente de un usuario. Debido a que los riesgos planteados por una vulnerabilidad pueden cambiar a lo largo del tiempo, se consideran tres factores que influyen en ello: confirmación de los detalles técnicos de la vulnerabilidad (explotabilidad), el nivel de remediación y el reporte de confianza, referido a la disponibilidad del código o técnicas que permitan la explotación. Estas métricas son opcionales e incluyen un valor que no afecta a la evaluación cuando un usuario cree que la métrica en particular no existe y quiere omitirla.

**Métricas de entorno:** considera características de una vulnerabilidad que son únicas para el contexto del usuario que lleva a cabo la evaluación. Se definen debido a los distintos ambientes que pueden denotar una gran influencia sobre el riesgo que representa una vulnerabilidad para una organización. Este grupo de métricas se enfoca en las características de una vulnerabilidad asociadas al entorno del usuario. Incluyen el daño potencial colateral, distribución de objetivos y los requisitos de confidencialidad, integridad y disponibilidad. Al igual que las métricas temporales, son opcionales y cada una tiene un valor sin efecto en la evaluación, el cual es utilizado cuando un usuario considera que la métrica en particular no existe y la omite.

**Métricas de alcance:** a que existen vulnerabilidades que pueden identificarse en un componente específico (componente vulnerable), pero que sin embargo pueden afectar a otros elementos (componente impactado).

Las ventajas de utilizar el método definido con CVSS son diversas, principalmente, se utilizan puntuaciones de vulnerabilidad estandarizadas, lo que permite crear criterios consistentes para la gestión de vulnerabilidades. También, al utilizar un marco abierto es posible conocer las características individuales de la vulnerabilidad, mismas que son utilizadas para obtener la puntuación. Finalmente, cuando se calcula la puntuación, la vulnerabilidad se vuelve representativa del riesgo en una organización, por lo que los usuarios conocen la importancia de una vulnerabilidad con relación a otras. A continuación, se presenta a nivel grafico lo descrito anteriormente:

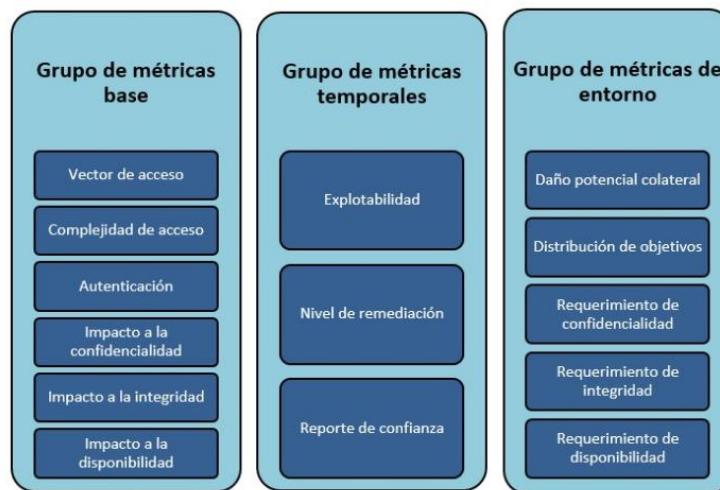


Figura 1. Nivel gráfico grupo de métricas

Base Score Metrics		
<b>Exploitability Metrics</b>		
<b>Attack Vector (AV)*</b>		
Local (AV:L)	Adjacent Network (AV:A)	Network (AV:N)
<b>Access Complexity (AC)*</b>		
High (AC:H)	Medium (AC:M)	Low (AC:L)
<b>Authentication (Au)*</b>		
Multiple (Au:M)	Single (Au:S)	None (Au:N)
<b>Impact Metrics</b>		
<b>Confidentiality Impact (C)*</b>		
None (C:N)	Partial (C:P)	Complete (C:C)
<b>Integrity Impact (I)*</b>		
None (I:N)	Partial (I:P)	Complete (I:C)
<b>Availability Impact (A)*</b>		
None (A:N)	Partial (A:P)	Complete (A:C)

Figura 2. Métricas de puntuación base (base score metrics)

#### 4.1.5 OWASP

Es una comunidad abierta/proyecto abierto para todas las personas y organizaciones que desarrollen, conserven y adquieran aplicaciones. Contiene herramientas, estándares, publicaciones, metodologías. Genera un top 10 de vulnerabilidades (riesgos seguridad) a nivel mundial de aplicaciones web.

[10]Uno de los principales objetivos del OWASP es educar a los desarrolladores, diseñadores, arquitectos, gerentes y organizaciones sobre las consecuencias de las debilidades más comunes y más importantes de la seguridad de las aplicaciones web. La organización trata de cómo incrementar la seguridad en aplicaciones y se enfoca en mejorar todas las áreas, basándose en personas, procesos y tecnología. OWASP comparte material abierto, para colaborar y hacer que las aplicaciones sean seguro, es una entidad sin lucro, su fin es que las aplicaciones sean seguras y que tengan éxito.

OWASP genera gradualmente un Top 10 de las vulnerabilidades que se presentan en las aplicaciones a nivel mundial, las ultimas fueron el 2017, estas se generan de las opiniones de la comunidad que hace parte de OWASP. El objetivo del Top 10 es concientizar a los desarrolladores y gerentes como de convertirse en un standard de seguridad.

OWASP apoya a las grandes organizaciones a utilizar el Estándar de Verificación de Seguridad en Aplicaciones, a las casas de software también en el aseguramiento de las aplicaciones. se incita a todo el equipo y organizaciones de desarrollo de software a crear un programa de seguridad de aplicaciones que sea compatible con su cultura y tecnología, cultiva las fortalezas existentes para medir y mejorar el programa de seguridad en sus aplicaciones, usa el Modelo de Madurez de Aseguramiento del Software.

El Top 10 de OWASP, provee técnicas básicas para protegerse contra estas áreas con problemas de riesgo alto, y suministra orientación sobre cómo continuar desde allí.

<b>OWASP Top 10 2017</b>	
A1:2017 – Inyección	
A2:2017 – Pérdida de Autenticación y Gestión de Sesiones	
A3:2017 – Exposición de Datos Sensibles	
A4:2017 – Entidad Externa de XML (XXE) [NUEVO]	
A5:2017 – Pérdida de Control de Acceso [Unido]	→
A6:2017 – Configuración de Seguridad Incorrecta	
A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)	
A8:2017 – Deserialización Insegura [NUEVO, Comunidad]	
A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas	
A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]	

Figura 3. OWASP Top 10 en 2017

**A1:2017 Inyección:** Las fallas de inyección, como SQL, NoSQL, OS o LDAP se presenta al enviar datos no confiables, por un comando o consulta. Los datos dañinos ejecutan comandos involuntarios o acceda a los datos sin la autorización.

**A2:2017 Pérdida de Autenticación:** Las funciones de la aplicación de autenticación y gestión de sesiones no son implementadas correctamente, los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para tomar la identidad de otros usuarios.

**A3:2017 Exposición de datos sensibles:** las aplicaciones web y APIs no protegen apropiadamente datos sensibles, ejemplo la información financiera, la información de salud Información Personal. Los atacantes roban o modifican datos no muy bien protegidos y con ello realizar fraudes, robos de identidad u otros delitos. Por tal motivo estos datos sensibles se le deben crear métodos de protección adicionales, tales como el cifrado en almacenamiento y tránsito.

A4:2017 Entidades Externas XML (XXE): los procesadores XML anteriores o sin configurar correctamente, calculan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para dejar ver archivos internos mediante la URI o archivos insertados en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio llamados DoS.

A5:2017 Pérdida de Control de Acceso: Las opciones que se le dan en los perfiles a los usuarios autenticados pueden hacer usan incorrectamente. Los atacantes explotan esos defectos para entrar, sin autorización, a opciones y/o datos, entrar a cuentas de otros usuarios, observación de archivos sensibles, modificar datos, cambiar acceso, roles, etc.

A6:2017 Configuración de Seguridad Incorrecta: La configuración de seguridad incorrecta es común y por configuración manual, ad hoc o por omisión (o por la falta de configuración). buckets abiertos, cabeceras HTTP configuradas erróneamente, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc.

A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS): Los XSS se presenta cuando la aplicación toma datos no confiables y los envía al navegador web sin validación y codificación apropiada; o actualiza una página web con datos provistos por el usuario utilizando una API que ejecuta JavaScript en el navegador. Ejecuta comandos en el navegador de la víctima y el atacante puede secuestrar la sesión, modificar (defacement) los sitios web, o redireccionar al usuario hacia un sitio malicioso.

A8:2017 Deserialización Insegura: Se presenta cuando una aplicación recibe objetos serializados dañinos y estos objetos son manipulados o son borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

A9:2017 Componentes con vulnerabilidades conocidas: Estos componentes pueden ser bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, se puede provocar una pérdida de datos o tomar el

control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas debilitan las defensas de las aplicaciones y permitir diversos ataques.

A10:2017 Registro y Monitoreo Insuficientes: El registro y monitoreo insuficiente permite a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. [11]

## **4.2 Marco de referencia tecnológico**

Existen metodologías o estándares que permiten seguir un lineamiento para realizar pruebas de penetración las cuales localizan y explotan los sistemas de cómputo con la finalidad de hacerlos más seguros, el procedimiento en sí permite probar vulnerabilidades, generar pruebas de concepto de los ataques y demostrar que las vulnerabilidades son reales y el sistema está expuesto, algunas de las metodologías más completas y en trabajo continuo para mejora y actualización son Open Source Security Testing Methodology Manual (OSSTM), OWASP Testing Guide, PTES Technical Guidelines.

Para esta investigación nos hemos basado en el Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM) que es uno de los estándares profesionales más completos y más utilizados en auditorías de seguridad de los sistemas, es un esquema que se encuentra en constante evolución de acuerdo a los aportes de los expertos que trabajan sobre el tema, este manual incluye varias fases como un marco de trabajo a seguir para la ejecución de auditorías y pruebas a realizar para así verificar la seguridad en nuestros sistemas. OSSTMM puede ser una referencia de ISO 27001, que permite probar bajo un marco la seguridad operativa de ubicaciones físicas, flujo de trabajo, seguridad inalámbrica, de telecomunicaciones, de redes de datos y cumplimiento para finalmente lograr desarrollar un informe de auditoría con las pruebas de seguridad realizadas.

### **4.2.1 OSSTM**

Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). Actualmente se encuentra en desarrollo la versión 3. Es uno de los estándares profesionales más completos y comúnmente utilizados en Auditorías de Seguridad para revisar la Seguridad de los Sistemas desde

Internet. Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Se ha logrado gracias a un consenso entre más de 150 expertos internacionales sobre el tema, que colaboran entre sí mediante Internet. Está compuesto por diversas fases; que permite probar bajo un marco la seguridad operativa de ubicaciones físicas, flujo de trabajo, seguridad inalámbrica, de telecomunicaciones, de redes de datos y cumplimiento para finalmente lograr desarrollar un informe de auditoría con las pruebas de seguridad realizadas.

Define la búsqueda de vulnerabilidades como a las comprobaciones automáticas de un sistema o sistemas dentro de una red.

ISECOM (institute for security and open methodologies) quien genero la metodología OSSTM aplica los siguientes términos a los diferentes tipos de sistemas y de testeos de seguridad de red, basados en tiempo y costo para el testeo de seguridad de internet. [12]

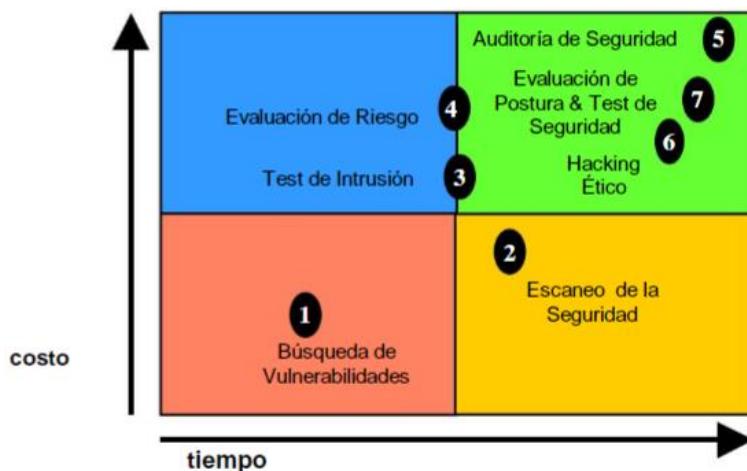


Figura 4. Tiempo vs. Costo en testeo de seguridad de Internet

A continuación, se describen las herramientas de escaneo que se investigaron y se utilizarán en el desarrollo del proyecto.

#### 4.2.2 Nessus

Permite identificar y corregir vulnerabilidades de manera rápida y sencilla, incluidos fallas de software, parches faltantes, malware y configuraciones erróneas, en una variedad de sistemas operativos, dispositivos y aplicaciones.

[13]Nessus es el analizador de vulnerabilidades más completo en el mercado actual. Nessus Professional le ayudará a automatizar el proceso de análisis de vulnerabilidades, ahorrará tiempo en ciclos de cumplimiento. Anteriormente, hasta el 2016, era de código abierto, se puede bajar completa la versión para pruebas 7 días, presentando todas las características. disponible para su descarga gratuita desde <https://es-la.tenable.com/downloads/nessus>. Trabaja en ambiente cliente servidor, se puede desplegar para sus escaneos de los clientes de la red y a los mismos servidores, monitorea los datos de escaneo. Puede exportar los resultados del escaneo a unos pocos formatos básicos, incluyendo ASCII y HTML. El cliente y el servidor se ejecutan en plataformas UNIX como Linux, Solaris de Sun Microsystems y FreeBSD. Nessus también proporciona clientes para plataformas Win32 y Java. Las acciones que se pueden realizar con este escáner son:

- Escanear IPs ilimitadas
- Funciones ilimitadas, incluyendo resultados en vivo y auditoría de configuración
- Detección precisa de activos a alta velocidad y amplia cobertura y perfiles
- La biblioteca de vulnerabilidades y comprobaciones de configuración más grande del mundo, continuamente actualizada
- Correo electrónico y soporte comunitario
- Formación gratuita y orientación

#### **4.2.3 Nmap**

Network Mapper, es un código libre y abierto (OpenSource), para el descubrimiento de redes y auditorías de seguridad. Se puede usar para tareas como el inventario de redes, la administración de programas de actualización de servicios y la supervisión del tiempo de actividad del host o del servidor. Nmap utiliza paquetes de IP sin procesar en formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre de aplicación y versión) ofrecen, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de filtros de paquetes / cortafuegos están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente redes grandes, pero funciona bien contra hosts individuales. Nmap corre

en ambiente, Linux, Windows y Mac OS X. Una herramienta flexible de transferencia, redirección y depuración de datos (Ncat), una utilidad para comparar resultados de escaneo (Ndiff) y una herramienta de análisis de generación de paquetes y respuesta (Nping). Es compatible con todos los sistemas, aunque no tiene garantía, está respaldado por toda la comunidad de desarrolladores. Este está inmerso en Kali Linux en sus últimas versiones, viene como una utilidad preinstalada.

[14]

#### **4.2.4 Zenmap**

Herramienta similar a Nmap pero en ambiente gráfico, el cual permite observar el estado de los puertos personalizando los tipos o perfiles de escaneo. Herramienta similar a Nmap pero en ambiente gráfico, el cual permite observar el estado de los puertos personalizando los tipos o perfiles de escaneo. Corre en ambiente Windows, en el proyecto se usó a través de Windows 10, ejecutando en óptimas condiciones, admite docenas de técnicas avanzadas para trazar redes llenas de filtros IP, firewalls, enruteadores y otros obstáculos. Esto incluye muchos mecanismos de escaneo de puertos (tanto TCP como UDP), detección de SO, detección de versiones, barridos de ping y más. Zenmap y Nmap se ha utilizado para escanear enormes redes de literalmente cientos de miles de máquinas. El objetivo de Zenmap es hacer que Nmap sea fácil de usar ya que es en ambiente gráfico, también ofrece funciones avanzadas para usuarios con experiencia en Nmap.

[15]

#### **4.2.5 Retina**

Es uno del escáner más potente de vulnerabilidades que existen en el mercado, proporciona pruebas de vulnerabilidad para múltiples plataformas, evaluación de vulnerabilidades y la capacidad de crear sus propias auditorías. Además, Retina permite proteger de forma proactiva las redes contra las vulnerabilidades más críticas incorporando la base de datos de vulnerabilidades más actualizada. Dado que las auditorías de vulnerabilidad se agregan continuamente, esta base de datos se actualiza al comienzo de cada sesión. Retina permite, escanear en paralelo con el sistema de colas Retina para realizar 30 auditorías únicas de una máquina. Realiza la mayoría de las exploraciones sin derechos administrativos. Esto le permite asegurar rápida y fácilmente sus redes distribuidas globalmente. Se puede crear análisis de auditoría personalizados para aplicar sus políticas de seguridad internas, como implementaciones y configuraciones de máquinas. Retina utiliza Access o cualquier almacén de datos ODBC para el

almacenamiento y un servidor de administración y agregación para controlar los escáneres remotos. Además, están disponibles las capacidades de autenticación multiusuario. [16]

## 5. Glosario de términos

**Activo:** Algo que tiene valor para la organización (ISO/IEC 13335-1:2004). Compuesto por información, procesos, personas, infraestructura y aplicaciones.

**Amenaza:** Posibilidad de violar la seguridad que existe si se da una circunstancia, capacidad, acción o evento que puede infringir la seguridad y causar daño. Esto es, una amenaza es el posible riesgo de que una vulnerabilidad sea explotada. Evento que puede provocar un incidente en la organización produciendo daños o pérdidas materiales/inmateriales. Situación o evento que puede generar un incidente o afectar un recurso. Posibilidad de violar la seguridad. [17]

**Análisis de riesgos:** Permite conocer cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades, para establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

**Ataque:** Asalto a la seguridad del sistema derivada de una amenaza inteligente, es decir, un acto deliberado que intenta evadir los servicios de seguridad y violar las políticas de seguridad de un sistema. Puede ser pasivo o activo:

**Ataque Activo:** Interfiere con el tráfico legítimo de la red, entre los tipos se encuentra: suplantación de identidad, modificación del mensaje, denegación, repetición, retransmisión. [17]

**Ataque Pasivo:** Monitoreo no autorizado por un intruso el tráfico en la red para capturar información; escucha y analiza el tráfico; no afecta recursos.

**Ciberataque:** Es la explotación de forma deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Estos ataques utilizan código malicioso para alertar la lógica

o los datos del ordenador, lo que puede comprometer la información y provocar delitos cibernéticos.

**Confidencialidad:** Los componentes del sistema serán accesibles solo por aquellos usuarios autorizados, impedir el acceso no autorizado.

**CPE (Common platform enumeration):** es un esquema de nombres estructurado para sistemas, software y paquetes de tecnología de la información. Basado en la sintaxis genérica para los Identificadores Uniformes de Recursos (URI), el CPE incluye un formato de nombre formal, un método para verificar nombres contra un sistema y un formato de descripción para unir texto y pruebas a un nombre.

**CVE (Common vulnerabilities and exposures):** Lista de entradas que contiene un número de identificación, una descripción y al menos una referencia pública, para vulnerabilidades de seguridad informática conocidas públicamente. Se utilizan en numerosos productos y servicios de ciberseguridad de todo el mundo.

**CVSS (Common vulnerability score system):** El Sistema de puntuación de vulnerabilidad común (CVSS) proporciona una manera de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad. La puntuación numérica se puede traducir a una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades. CVSS es un estándar publicado utilizado por organizaciones de todo el mundo, se encuentra actualmente en la versión 3.0.

**CWE (Common weakness enumeration specification):** Proporciona un lenguaje común (lista desarrollada por la comunidad) para encontrar, tratar las causas de las vulnerabilidades de seguridad del software tal como se encuentran en el código, diseño, o arquitectura del sistema. Sirve como línea base para la identificación de debilidades, mitigación y esfuerzo de prevención. Cada Id individual representa un tipo de vulnerabilidad individual. Mantainded por Corporacion MITRE que proporciona una lista en detalle para cada CWE individual.

**Disponibilidad:** Propiedad de un sistema o recurso de estar disponible, utilizable, operacional; los servicios deben estar siempre activos (24x7x365) es decir los componentes del sistema y/o datos a solicitud de usuarios cuando así lo deseen.

**Integridad:** Componentes del sistema solo pueden ser creados y modificados por los usuarios autorizados, impedir la manipulación de la información.

**NVD (National vulnerability database):** Repositorio del gobierno de los Estados Unidos de donde se toman los datos de vulnerabilidades CVE. Incluye bases de datos de referencias de listas de verificación de seguridad, fallas de software relacionadas con la seguridad, configuraciones erróneas, nombres de producto y métricas de impacto.

**Nessus:** Analizador de vulnerabilidades más completo en el mercado actual.

**Nmap:** Network Mapper, es un código libre y abierto (OpenSource), es la utilidad por excelencia, para el descubrimiento de redes y auditorías de seguridad.

**Norma ISO/IEC 27000:** Familia de estándares ISO orientados a la seguridad de la información. Incluye conceptos y definiciones que soportan a la familia. Algunos integrantes importantes son:

- **ISO 27001:** Norma principal, requisitos del SGSI. Indica que se debe hacer.
- **ISO 27002:** Controles recomendados de la norma ISO 27001. Indica cómo se hace.
- **ISO 27003:** Guía implementación siguiendo PHVA
- **ISO 27005:** Estándar de gestión de riesgos de seguridad de la información.

**Open Source:** Código Abierto; Expresión con la que se conoce al software distribuido y desarrollado libremente

**Openvas:** es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. Permite la actualización continua de la base de Pruebas de

Vulnerabilidades de Red. Es una herramienta principal de OSSIM, todos los productos que la componen son software libre y la mayoría de ellos son distribuidos bajo licencia GPL.

**OSSTM:** Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Está compuesto por diversas fases; que permite probar bajo un marco la seguridad operativa de ubicaciones físicas, flujo de trabajo, seguridad inalámbrica, de telecomunicaciones, de redes de datos y cumplimiento para finalmente lograr desarrollar un informe de auditoría con las pruebas de seguridad realizadas.

**OVAL (Open vulnerability and assessment language):** Es una comunidad/estándar de seguridad de la información internacional para promover contenido de seguridad abierto al público. Son definiciones de diversas fuentes, en donde se puede verificar información de vulnerabilidades o parches. Va integrado con el sitio web de cvedetails.com para navegar entre CVE, productos y detalles de definiciones OVAL.

**OWASP:** Proyecto abierto de seguridad de aplicaciones web. Genera un top 10 de vulnerabilidades (riesgos seguridad) a nivel mundial de aplicaciones web.

**Plan de remediación:** Documento que permita corregir las fallas identificadas y evaluadas, en conformidad con los resultados de la priorización. En general, la corrección de estas fallas se relaciona con la aplicación de actualizaciones o parches de seguridad o ajustes a la configuración o eliminación de software.

**Procedimiento de gestión de vulnerabilidades:** Es un documento que incluye las fases para la realización de la evaluación de vulnerabilidades de activos de una infraestructura tecnológica, en el cual se encuentran las debilidades de las plataformas de software o hardware para solucionar las fallas, antes de que puedan generar un impacto negativo o la materialización de eventos indeseados e inesperados. Por normatividad se debe definir la frecuencia de ejecución de las pruebas el cual depende del sector.

**PTES Technical Guidelines:** El Estándar de Ejecución de Pruebas de Penetración fue creado por algunas de las mentes más brillantes y expertos definitivos en la industria de pruebas de penetración. Consta de siete fases de prueba de penetración y puede usarse para realizar una prueba de penetración efectiva en cualquier entorno.

**Remediación:** Acciones aplicadas para cerrar o eliminar una vulnerabilidad tales como: cierre de puertos, aplicación de parches, actualización de software ajustes a la configuración o eliminación del software afectado.

**Retina:** Es uno de los escáneres más potente de vulnerabilidades que existen en el mercado, proporciona pruebas de vulnerabilidad para múltiples plataformas, evaluación de vulnerabilidades y la capacidad de crear sus propias auditorías

**Riesgo:** Estimación del grado de exposición de 1 o más activos de información ante la materialización de una amenaza que pueda impactar negativamente o causar daños en una organización. Se puede aceptar, mitigar, o transferir. Se busca reducir a un nivel que resulte aceptable.

**Seguridad de la información:** Proteger la información de una organización, independientemente del lugar en el que se localice: impresos en papel, discos duros de las computadoras, etc. Tiene 3 principios fundamentales: Confidencialidad, Integridad, Disponibilidad. Su radio de acción cubre análisis de riesgos, seguridad personal/física, gestión de comunicaciones, control acceso, gestión de incidentes, gestión continuidad del negocio, entre otros.

**Seguridad informática:** Proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización(hardware,software) y que estas sean utilizadas de la manera indicada por la organización. Su radio de acción cubre pruebas de evaluación de vulnerabilidades, test de penetración, hacking ético, entre otros.

**SGSI (Sistema de gestión de seguridad de la información):** Orientado a gestionar riesgos del negocio. Es el concepto central sobre el que se construye la norma ISO 27001. Debe

ser realizado mediante un proceso sistemático, documentado, conocido por toda la organización. Ayuda a establecer las políticas y procedimientos en relación a los objetivos de negocio de la organización con el objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

**VPN:** Una red privada virtual (RPV), es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

**Vulnerabilidad:** Punto débil en la seguridad de un sistema informático que permiten que un atacante comprometa la integridad, disponibilidad, confidencialidad de la información.

**Zenmap:** Herramienta similar a Nmap pero en ambiente gráfico, el cual permite observar el estado de los puertos personalizando los tipos o perfiles de escaneo.

## 6. Justificación

En la actualidad, todos los activos de la empresa deben ser monitoreados y gestionados con la misma importancia dentro de un período de tiempo regular para garantizar la confidencialidad, integridad y disponibilidad de los mismos. De esta manera evitar que se materialicen amenazas de seguridad que surjan de vulnerabilidades informáticas no atendidas en el tiempo correcto, las cuales deben ser incluidas en un plan de remediación de vulnerabilidades y tratamiento de riesgos con la finalidad de llevar una gestión periódica que garantice los procesos y servicios de la empresa. Debido a que la empresa actualmente no cuenta con herramientas que permitan identificar vulnerabilidades que afecten la seguridad de la información, es importante y oportuno el objeto de este trabajo para presentar un plan de gestión/procedimiento gestión de vulnerabilidades que permita ayudar a futuras investigaciones a la selección de herramientas para el monitoreo y gestión de vulnerabilidades.

## 7. Objetivos

### 7.1. General

Descubrir y analizar las vulnerabilidades informáticas sobre un grupo de servidores de una empresa privada en la ciudad de Bogotá.

### 7.2. Específicos

- Realizar una investigación sobre el estado del arte acerca de metodologías y herramientas Open Source para evaluación de vulnerabilidades informáticas.
- Proponer soluciones que se encarguen de gestionar las vulnerabilidades informáticas sobre los servidores a través de herramientas Opensource.
- Analizar los resultados y realizar pruebas manuales de las vulnerabilidades obtenidas de los servidores evaluados para certificar que estas no sean falsos positivos.
- Diseñar un plan de remediación para la compañía que responda a los resultados obtenidos.

## 8. Requerimientos

### 8.1 Requerimientos funcionales

El proyecto propuesto reúne una serie de requerimientos identificados y necesarios para llevar a cabo las actividades propuestas en el documento para el análisis y gestión de vulnerabilidades que pueden afectar directamente el sistema de información de la empresa.

Entre los requerimientos funcionales detectados se mencionan los siguientes:

- Obtener permisos de acceso a los recursos de la empresa.
- Autorización para realizar pruebas sobre los servidores
- Determinar el tiempo que tomará la ejecución de las pruebas a realizar

sobre los servidores y la cantidad de pruebas a realizar con cada herramienta de escaneo.

- Direcciones IP de los hosts a los cuales se les realizarán los escaneos de vulnerabilidades.
- Acceso a conexión por VPN entregada por la empresa para realizar conexión remota y así generar los escaneos a cada host dentro de la misma red.
- Conexión de banda ancha a Internet para el acceso a la red por VPN.
- Herramientas de evaluación de vulnerabilidades Open Source (Nmap, Retina, Nessus)
- Tabla de seguimiento de escaneos de vulnerabilidades con las herramientas Open Source.
- Equipos de trabajo:
- 

Tabla 3. Características equipos de trabajo para realizar los escaneos de vulnerabilidades

EQUIPO	CARACTERÍSTICAS
COMPUTADOR PORTATIL	PROCESADOR: CORE INTEL I5 1,7 GHz MEMORIA RAM: 6GB A 64 bits DISCO DURO: 500GB
COMPUTADOR PORTATIL	PROCESADOR: CORE INTEL I7 2,7 GHz MEMORIA RAM: 12GB A 64 bits DISCO DURO: 1TB
COMPUTADOR PORTATIL	PROCESADOR: CORE XEON 2,8 GHz MEMORIA RAM: 16GB A 64 bits DISCO DURO: 250GB

## 8.2 Requerimientos no funcionales

En cuanto a los requerimientos no funcionales se detectan como principales generar una documentación periódica del proyecto que brindará a la empresa información clara y actualizada del resultado de la evaluación de análisis de vulnerabilidades detectadas:

- Contar con los respaldos de la información de cada servidor antes de la ejecución de las pruebas sobre los servidores.
- Acuerdo de confidencialidad entre la Empresa a desarrollar el proyecto y los estudiantes del mismo. (Firmado y entregado a la empresa en octubre de 2018)

- Reuniones periódicas entre la empresa y estudiantes con la finalidad de registrar los avances realizados, generar discusiones y resolver inquietudes.
- Realizar documentos gerenciales y técnicos.
- Firma de acuerdo de confidencialidad entre empresa y proveedor que ejecutara las pruebas.
- Carta dirigida al proveedor encargado de las pruebas donde se indicará que no se le informará al proveedor sobre las pruebas a realizar sobre el objetivo con el fin de evaluar su respuesta.
- Documentos enviados por la empresa a la Universidad donde se definen las condiciones de las pruebas.

## **9. Metodología**

[18] Se toma como base la metodología OSSTM, basada en las buenas prácticas de la norma ISO 27001 enfocadas a la seguridad de la información para identificar las vulnerabilidades del sistema sobre los servidores de una empresa privada en Bogotá.

El objetivo es la identificación, comprensión y verificación de las debilidades, errores de configuración y vulnerabilidades en un servidor o red. La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheo de sistemas. Se requiere la verificación manual para eliminar falsos positivos, descubrir el flujo de datos de entrada y salida de la red. Entre los resultados esperados se tiene: tipo de aplicación o servicio por vulnerabilidad, niveles de parches de los sistemas y aplicaciones, listado de vulnerabilidades, mapa de red.

A continuación se muestra las fases que recomienda la metodología OSSTM en el ítem 7 para búsqueda y verificación de vulnerabilidades:

- Integrar en las pruebas realizadas los escáneres, herramientas de hacking y exploits utilizados actualmente.
- Medir la organización objetivo utilizando herramientas de escaneo habituales.
- Lograr determinar vulnerabilidades por tipo de aplicación y sistema.

- Lograr ajustar vulnerabilidades a servicios
- Lograr determinar el tipo de aplicación y servicio por vulnerabilidad
- Realizar pruebas redundantes al menos con 2 escáneres automáticos de vulnerabilidades
  - Identificar todas las vulnerabilidades relativas a las aplicaciones
  - Identificar todas las vulnerabilidades relativas a los sistemas operativos
  - Identificar todas las vulnerabilidades de sistemas parecidos o semejantes que podrían también afectar a los sistemas objetivos
    - Verificar todas las vulnerabilidades encontradas durante la fase de búsqueda de exploits con el objetivo de descartar falsos positivos y falsos negativos
    - Verificar todos los positivos

En el documento de Procedimiento de gestión de vulnerabilidades el cual se diseñó para la empresa se encuentra detallado el desarrollo este proyecto. A continuación, se detallan algunos ítems de este: (Anexo 6 - Procedimiento gestión de vulnerabilidades)

### **9.1 Aprobación para la evaluación de vulnerabilidades**

Debido a que las actividades relacionadas con la identificación de vulnerabilidades pueden catalogarse como intrusivas por las herramientas de seguridad que se encuentren instaladas dentro la infraestructura de la organización, es necesario que se tenga la aprobación para ejecutar el escáner, programar la actividad y notificar a las partes interesadas, es decir aquellas que pueden afectar o verse afectadas por esta actividad.

### **9.2 Generar un inventario de activos**

Referente a la lista de inventario de activos entregada por la empresa, se requiere generar listado complementario asociado con la información y sistemas, utilizados para procesar, almacenar o transmitir esa información, y sobre los cuales se llevará a cabo la evaluación.

### **9.3 Recopilación de información**

En esta fase se realizará la recolección de información para el desarrollo del proyecto, basado en documentos, videos, imágenes, también se realizará la recolección de la información

de las tecnologías para el objetivo del trabajo.

Se realizará el escaneo en dos fases, una fase de escaneos en prueba sobre 4 servidores en desarrollo con el fin de identificar cual es el perfil de escaneo adecuado y realizar una exploración inicia(Febrero/Marzo). Posteriormente la segunda fase de escaneos sobre los 30 servidores en producción utilizando Nessus en horario no hábil durante 2 meses (Abril-Mayo) con el fin de reunir información para después entrar a la etapa de correlacionar estos resultados, y poder a partir de allí generar el plan de remediación, informes ejecutivo/técnico y el procedimiento objetivo del proyecto.

### 9.3.1 Fase escaneos en prueba

Cantidad: 4 Servidores

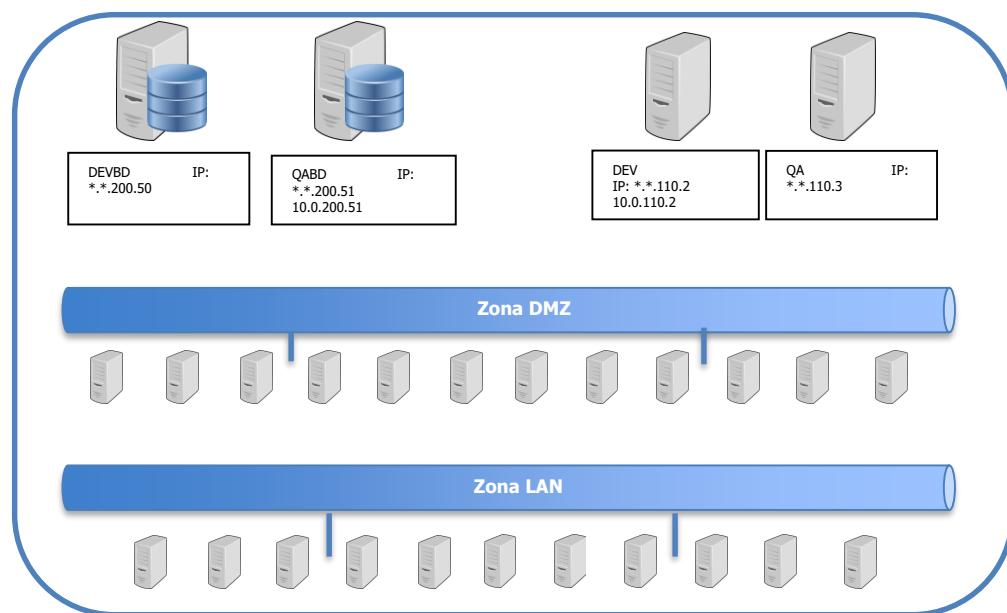


Figura 5. Diagrama general de servidores a escanear fase de pruebas

### 9.3.2 Fase escaneos en producción

Cantidad: 30 Servidores

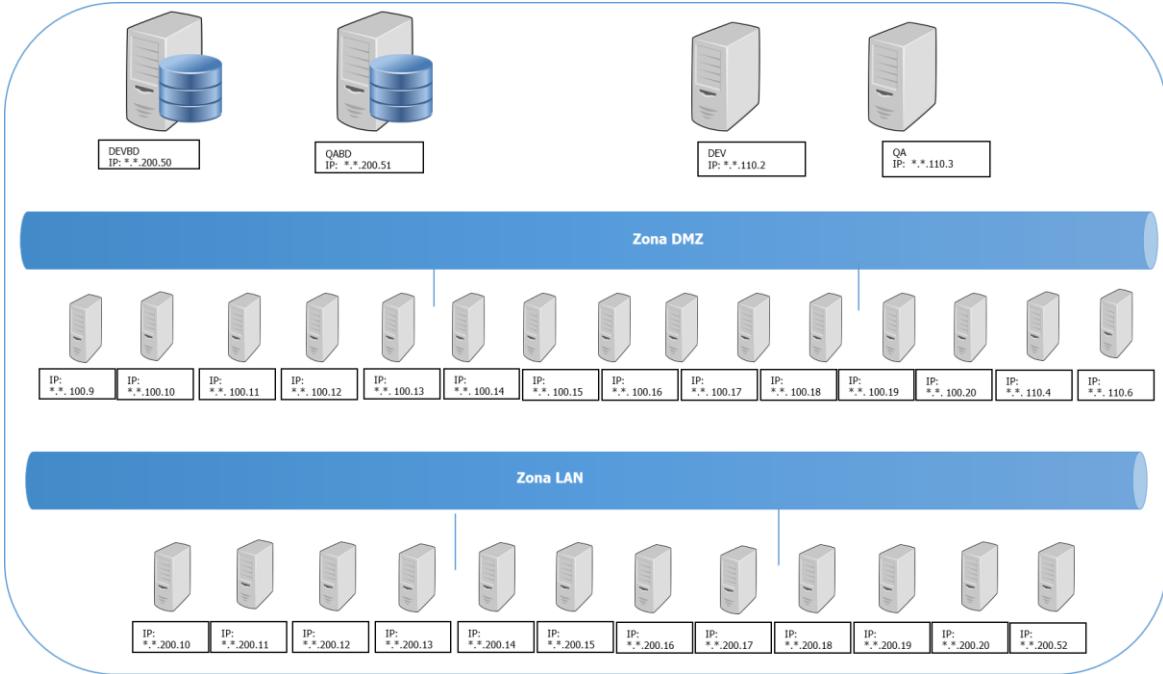


Figura 6. Diagrama general de servidores a escanear fase de desarrollo

### 9.4 Definir el alcance de la evaluación

La evaluación puede ejecutarse de dos modos: interno y externo. Desde la perspectiva interna se realizará el escaneo desde la infraestructura de la organización, con acceso a los recursos de forma directa. La evaluación externa implica lidiar con la protección perimetral que se tiene en la red corporativa y se adopta la posición que tendría un atacante en busca de alguna vulnerabilidad. Se deben definir métodos de conexión, horario de pruebas, herramientas a utilizar, perfil de escaneo, definir medidas preventivas previas a la realización de las pruebas.

Las pruebas se harían a través de VPN, horario no hábil, herramientas fase pruebas (Retina, Nmap, Nessus, Openvas, Zenmap), fase producción (Nessus, Nmap). Evaluación del perfil de escaneo de acuerdo a las pruebas en la fase de pruebas. Las medidas de contingencia son responsabilidad de la empresa.

Como parte de la planeación de las pruebas se acordó con la empresa que ellos realizarán backups a los servidores previa ejecución de las pruebas, monitoreo constante a los servidores con el fin de prevenir efectos adversos sobre los servicios involucrados en los servidores.

La definición de la herramienta a utilizar debe considerar si era licenciada o libre, que incluya una base de datos actualizada aceptada por la industria (CERT, SANS, NIST), con métricas tipo CVSSS y con criterio común de clasificación como el CVE. En la fase de pruebas se permite la utilización de diversas herramientas con el fin de elegir la mejor para la fase de producción, definir el perfil de escaneo, revisar los tiempos de ejecución entre otros.

## **9.5 Ejecución de las pruebas**

De acuerdo al alcance definido ejecutar los escaneos en horario no hábil para no afectar la operación de la organización, registrar la información obtenida para un posterior análisis de resultados.

Posterior a la identificación de las debilidades y la obtención de información relacionada con las mismas, resulta necesario llevar a cabo un proceso de valoración que permita conocer su impacto. Para ello es posible utilizar algún sistema de puntaje como CVSS. Es importante mencionar que herramientas especializadas permiten automatizar estas actividades.

## **9.6 Generar un informe de resultados**

De acuerdo a la fase anterior se deben registrar los escaneos obtenidos en un documento con el fin de consolidar la información en un único documento para después categorizar de acuerdo al CVSS, facilitar el análisis posterior; esto permitirá conocer el estado de la seguridad en los sistemas a partir de los hallazgos. También busca mostrar los resultados a través de la priorización de las vulnerabilidades, con el objetivo de atender primero las debilidades de mayor impacto sobre los activos.

Se pueden realizar pruebas manuales para descartar falsos positivos, análisis de los reportes obtenidos, clasificación y valoración de las vulnerabilidades de acuerdo a su criticidad, creación de la matriz de riesgo (Análisis y evaluación del riesgo, identificación de brechas, determinar el impacto de brechas sobre sistemas y operación del negocio, priorización de las vulnerabilidades

de acuerdo a la criticidad del negocio para evaluar el impacto de vulnerabilidades identificadas que permita evaluar el impacto y probabilidad de una posible explotación de la vulnerabilidad encontrada para posteriormente priorizar su remediación y diseñar el plan de remediación con base al documento que consolida los escaneos realizados

### **9.7 Generar un plan de remediación**

Como última actividad asociada a la evaluación de vulnerabilidades es necesario desarrollar un plan de remediación que es un documento que brinde las recomendaciones necesarias para poder dar solución a las vulnerabilidades encontradas. En general, la corrección de estas fallas se relaciona con la aplicación de actualizaciones o parches de seguridad. O ajustes a la configuración o eliminación de software.

### **9.8 Ejecución de plan de acción**

Las acciones de remediación planeadas deben ser ejecutadas en los tiempos establecidos por el personal de Tecnología encargado de la organización asignado para esta función con el fin de reducir los tiempos de exposiciones y reducir los riesgos de incumplimiento.

### **9.9 Verificación de la efectividad**

Las acciones de tratamiento deben ser evaluadas para verificar que el plan de remediación haya sido implementado y las brechas cerradas. Repetir técnicas y procesos de escaneo de vulnerabilidades (re test) si es necesario.

### **9.10 Socialización de resultados con los interesados**

Realizar una reunión técnica para informar de los resultados, realizar revisión general de las vulnerabilidades encontradas y la clasificación realizada por la herramienta que incluya el área de TI de la organización y los encargados de realización de las pruebas.

Se realizará una sesión presencial con la empresa en semanas posteriores a la radicación de este documento en facultad, como fase previa a la sustentación oficial de la universidad, y con el objetivo de tener la aceptación por parte de la empresa.

## 10. Capítulos de desarrollo

### 10.1 Acuerdos para la evaluación de las vulnerabilidades

Se obtuvo la aprobación por parte de la empresa privada en Bogotá a través de un acuerdo de confidencialidad, 2 documentos enviados por la empresa asesora Assure It a la Universidad El Bosque (pdf) en donde se indican las condiciones de las pruebas y que no se informará al proveedor de las mismas con el objetivo de verificar la respuesta de este.

La empresa autorizo a los estudiantes a que las conexiones para los escaneos se hicieran en horario no hábil (después de las 6 pm hasta las 7 am) se hiciera de manera remota, externa vía VPN SSL cuyas credenciales fueron brindadas por correo electrónico. El cliente VPN se descargó de acuerdo a la indicación de la empresa y el acceso era de este modo:



Figura 7. Acceso conexión VPN

Este proyecto se realizó en Windows 10 y Kali Linux hacia servidores Linux y Windows.

Como parte de la planeación de las pruebas se acordó con la empresa que ellos harían backup a los servidores previa ejecución de las pruebas, monitoreo constante a los servidores con el fin de prevenir efectos adversos sobre los servicios involucrados en los servidores.

Se realizó investigación de herramientas y metodologías aplicadas al estudio para escaneo y análisis de vulnerabilidades, como se registran en el (Anexo 7 - Herramientas de escaneo). Con

el objetivo de poder decidir cuál era la mejor opción se realizó una sesión de demos en la empresa en donde cada uno de los estudiantes del grupo socializó las herramientas open source para realizar el escaneo de vulnerabilidades.

A continuación, se presentan las herramientas revisadas durante la fase inicial de pruebas, para definir y seleccionar las herramientas a utilizar en la fase de producción:

Tabla 4. Herramientas de escaneo seleccionadas

HERRAMIENTAS	NMAP	ZENMAP	NESSUS	OPENVAS	RETINA
Tipo	Opensource	Opensource	Free Alternatives	Opensource	Opensource
Descripción	Herramienta de código abierto que escanea puertos.	Herramienta de código abierto que escanea puertos.	Herramienta de escaneo de seguridad remoto	Identifica vulnerabilidades y dispone la evaluación de riesgos de seguridad	Evaluación de vulnerabilidades
Tipo de prueba	Sondeo Ping Básico Avanzado	Intense Scan	Escaneo y análisis de vulnerabilidades a Direcciones IP  Básico default Avanzado default	Escaneo y análisis de vulnerabilidades a Direcciones IP	Escaneo y análisis de vulnerabilidades a Direcciones IP Perfil y auditprías personalizadas
Objetivo	Escanear puertos de los host y verificar en qué estado se encuentran (abiertos, cerrados)	Escanear los servidores de forma externa a través de una VPN habilitada para tal fin y realizar comparativa con las otras herramientas seleccionadas a través de una VPN habilitada para tal fin y realizar comparativa con las otras herramientas seleccionadas	Escanear los servidores de forma externa a través de una VPN habilitada para tal fin y realizar comparativa con las otras herramientas seleccionadas	Escanear los servidores de forma externa a través de una VPN habilitada para tal fin y realizar comparativa con las otras herramientas seleccionadas	Escanear los servidores de forma externa a través de una VPN habilitada y permite crear sus propias auditorías, permite escaneo en paralelo

## 10.2 Escaneos sobre los servidores en fase de prueba

Se inicia realizando revisión de las conexiones activas sobre los cuatro servidores por medio de Netstat

TCP	192.168.0.2:51925	ec2-18-211-211-204:https	CLOSE_WAIT
TCP	192.168.0.2:53539	104.46.118.81:https	ESTABLISHED
TCP	192.168.0.2:54265	host131:https	ESTABLISHED
TCP	192.168.0.2:54287	65.52.108.76:https	ESTABLISHED
TCP	192.168.0.2:55601	whatsapp-cdn-shv-02-mia3:https	ESTABLISHED
TCP	192.168.0.2:55730	bog02s07-in-f5:https	ESTABLISHED
TCP	192.168.0.2:55864	bog02s07-in-f5:https	ESTABLISHED
TCP	192.168.0.2:55892	8.18.25.27:https	ESTABLISHED
TCP	192.168.0.2:55914	do-20:https	SYN_SENT

Figura 8. Revisión con Netstat IP: \*.\*.110.2

C:\Users\LENOVO>netstat *.*.200.50			
Conexiones activas			
Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:50000	LENOVO-PC:52940	ESTABLISHED
TCP	127.0.0.1:50001	LENOVO-PC:52941	ESTABLISHED
TCP	127.0.0.1:50002	LENOVO-PC:52959	ESTABLISHED
TCP	127.0.0.1:50003	LENOVO-PC:52960	ESTABLISHED
TCP	127.0.0.1:51725	LENOVO-PC:51726	ESTABLISHED
TCP	127.0.0.1:51726	LENOVO-PC:51725	ESTABLISHED
TCP	127.0.0.1:51729	LENOVO-PC:51730	ESTABLISHED
TCP	127.0.0.1:51730	LENOVO-PC:51729	ESTABLISHED
TCP	127.0.0.1:52940	LENOVO-PC:50000	ESTABLISHED
TCP	127.0.0.1:52941	LENOVO-PC:50001	ESTABLISHED
TCP	127.0.0.1:52959	LENOVO-PC:50002	ESTABLISHED
TCP	127.0.0.1:52960	LENOVO-PC:50003	ESTABLISHED
TCP	192.168.0.2:51925	ec2-18-211-211-204:https	CLOSE_WAIT
TCP	192.168.0.2:53539	104.46.118.81:https	ESTABLISHED
TCP	192.168.0.2:54265	host131:https	ESTABLISHED

Figura 9. Revisión con netstat IP: \*.\*.200.50

C:\Users\LENOVO>netstat *.*.110.3			
Conexiones activas			
Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:50000	LENOVO-PC:52940	ESTABLISHED
TCP	127.0.0.1:50001	LENOVO-PC:52941	ESTABLISHED
TCP	127.0.0.1:50002	LENOVO-PC:52959	ESTABLISHED
TCP	127.0.0.1:50003	LENOVO-PC:52960	ESTABLISHED
TCP	127.0.0.1:51725	LENOVO-PC:51726	ESTABLISHED
TCP	127.0.0.1:51726	LENOVO-PC:51725	ESTABLISHED
TCP	127.0.0.1:51729	LENOVO-PC:51730	ESTABLISHED
TCP	127.0.0.1:51730	LENOVO-PC:51729	ESTABLISHED
TCP	127.0.0.1:52940	LENOVO-PC:50000	ESTABLISHED
TCP	127.0.0.1:52941	LENOVO-PC:50001	ESTABLISHED
TCP	127.0.0.1:52959	LENOVO-PC:50002	ESTABLISHED
TCP	127.0.0.1:52960	LENOVO-PC:50003	ESTABLISHED
TCP	192.168.0.2:51925	ec2-18-211-211-204:https	CLOSE_WAIT
TCP	192.168.0.2:53539	104.46.118.81:https	ESTABLISHED
TCP	192.168.0.2:54265	host131:https	ESTABLISHED

Figura 10. Revisión con netstat IP: \*.\*.110.3

```
C:\Users\LENOVO\netstat -a | find "10.0.200.51"
Conexiones activas

Proto  Dirección local *.*.    Dirección remota      Estado
TCP    127.0.0.1:50006      LENOVO-PC:52940      ESTABLISHED
TCP    127.0.0.1:50001      LENOVO-PC:52941      ESTABLISHED
TCP    127.0.0.1:50002      LENOVO-PC:52959      ESTABLISHED
TCP    127.0.0.1:50003      LENOVO-PC:52960      ESTABLISHED
TCP    127.0.0.1:51725      LENOVO-PC:51726      ESTABLISHED
TCP    127.0.0.1:51726      LENOVO-PC:51725      ESTABLISHED
TCP    127.0.0.1:51729      LENOVO-PC:51730      ESTABLISHED
TCP    127.0.0.1:51730      LENOVO-PC:51729      ESTABLISHED
TCP    127.0.0.1:52940      LENOVO-PC:50000      ESTABLISHED
TCP    127.0.0.1:52941      LENOVO-PC:50001      ESTABLISHED
TCP    127.0.0.1:52959      LENOVO-PC:50002      ESTABLISHED
TCP    127.0.0.1:52960      LENOVO-PC:50003      ESTABLISHED
TCP    192.168.0.2:51925      ec2-18-211-211-204:https  CLOSE_WAIT
TCP    192.168.0.2:53539      104.46.118.81:https  ESTABLISHED
TCP    192.168.0.2:54265      host131:https   ESTABLISHED
TCP    192.168.0.2:54287      65.52.108.76:https  ESTABLISHED
TCP    192.168.0.2:55601      whatsapp-cdn-shv-02-mia3:https ESTABLISHED
TCP    192.168.0.2:55730      bog02s07-in-f5:https ESTABLISHED
```

Figura 11. Revisión con netstat IP: \*.\*.200.51

Se procede a realizar la revisión de puertos abiertos y cerrados con las herramientas

### Nmap y Zenmap

```
Zenmap
Escaneo Herramientas Perfil Ayuda (H)
Objetivo: *.*.10.2
Comando: nmap -T4 -A -v *.*.110.2
Servidores Servicios Salida Nmap Puerto/Servidores Topología Detalles del servidor Escaneos
nmap -T4 -A -v *.*.110.2
[+] Valid after: 2019-11-21T12:00:00
[+] NDS: 0f62 016d ecd7 8818 b592 f7df 78de 4045
[_]SHA-1: 6ad0 c597 9453 9ad9 752c 3783 21b8 c21f 4bed b0b6
[_]ssl-date: TLS randomness does not represent time
8084/tcp open  ssl/http Apache httpd/2.4.23 ((Linux) OpenSSL/1.0.2e-fips PHP/5.6.26)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.23 (Ubuntu) OpenSSL/1.0.2e-fips PHP/5.6.26
|_http-title: Site not found. Wrong URL?
|_ssl-cert: Subject: commonName=*.infrared.net
|_Subject Alternative Name: DNS=*.infrared.net, DNS=infrared.net
|Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
|Public Key type: rsa
|Public Key bits: 2048
|Signature Algorithm: sha256WithRSAEncryption
|Not valid before: 2017-11-21T00:00:00
|Not valid after: 2019-11-21T12:00:00
|NDS: 0f62 016d ecd7 8818 b592 f7df 78de 4045
[_]SHA-1: 6ad0 c597 9453 9ad9 752c 3783 21b8 c21f 4bed b0b6
[_]ssl-date: TLS randomness does not represent time
9080/tcp open  http  nginx 1.15.3
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.15.3
|_http-title: Did not follow redirect to https://*.*.110.2:9443/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running on: Linux 4.X
OS_CPE: cpe:/o:linux:linux_kernel:4.0
OS_details: Linux 4.0, Linux 4.4
Uptime guess: 14.251 days (since Thu Jan 31 17:42:13 2019)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

Figura 12. Escaneo con Zenmap - IP \*.\*.110.2 y \*.\*.200.51 (Anexo 8 - Escaneo Zenmap)

Tabla 5. Resultados Zenmap sobre los 4 servidores

SERVIDOR	PERFIL SCAN	TIEMPO SCAN(SEG)	PUERTOS ABIERTOS	DNS	SISTEMA OPERATIVO
1	INTENSE	60.23	9080/TCP HTTP NGINX 1.15.3 22/TCP SSH OPENSSH 7.4 80/TCP HTTP APACHE HTTPD 443/TCP HTTP APACHE HTTPD 8080/TCP HTTPD APACHE HTTPD 2.4.6(CENTOS) OPENSSL 1.0.2K-FIPS PHP/5.4.45 8081 /TCP HTTPD APACHE HTTPD 2.4.23(UNIX) OPENSSL 1.0.1E-FIPS PHP/5.6.26 8083/TCP HTTPD APACHE HTTPD 2.4.6(CENTOS) OPENSSL 1.0.2K-FIPS PHP/5.4.45 8084/TCP :SSL/HTTP Apache HTTPD 2.4.23(Unix) OpenSSL/1.0.1e-fips PHP/5.6.26	intrared.net	LINUX 4.0
	QUICK	16.66	22/TCP SSH 80/TCP HTTP 443/TCP HTTPS 8080/TCP HTTP-PROXY 8081/TCP BLACKICE-ICECAP	N/A	N/A
	REGULAR	27.65	22/TCP SSH 80/TCP HTTP 443/TCP HTTPS 8080/TCP HTTP-PROXY 8081/TCP BLACKICE-ICECAP 8083/TCP US-SRV 8084/TCP UNKNOWN	N/A	N/A
	COMPREHENSIVE SLOW	N/A-NO TERMINO	SE DEBE VOLVER A PROBAR PORQUE NO TERMINO		
2	INTENSE	49.03	22/TCP SSH SSH 6.6.1 3306/TCP TCPWRAPPED	N/A	LINUX 4.4
	QUICK	18.20	22/TCP SSH 3306/TCP MYSQL	N/A	N/A
	REGULAR	16.34	N/A	N/A	N/A
	COMPREHENSIVE SLOW	NO TERMINO	N/A	N/A	N/A
3	INTENSE	62.39	8084/TCP SSL/HTTP APACHE HTTPD 2.4.23 UNIX OPENSSL/1.0.1E-FIPS PHP/5.6.26	intrared.net	LINUX 4.0/4.4
	QUICK	19.25	22/TCP SSH 80/TCP HTTP 443/TCP HTTPS 8080 /TCP HTTP-PROXY 8081/TCP BLACKICE-ICECAP	N/A	N/A
	REGULAR	29.26	22/TCP SSH 80/TCP HTTP 443/TCP HTTPS 8080 /TCP HTTP-PROXY 8081/TCP BLACKICE-ICECAP	N/A	N/A
	COMPREHENSIVE SLOW	NO TERMINO	N/A	N/A	N/A
4	INTENSE	36.86	22/TCP SSG OPENSSH 6.6.1 3306/TCP TCPWRAPPED	N/A	LINUX 4.4
	QUICK	24.83	22/TCP SSG OPENSSH 6.6.1 3306/TCP MYSQL	N/A	N/A
	REGULAR	16.15	N/A	N/A	N/A
	COMPREHENSIVE SLOW	NO TERMINO	N/A	N/A	N/A

```
C:\Users\LENOVO>route print
=====
ILista de interfaces
57...02 00 4c 4f f0 50 ....Adaptador de bucle invertido de Microsoft
29...00 ff a3 8a 8f b5 ....VMware SSL VPN-Plus Client Adapter
18...5c 51 4f f6 b6 a6 ....Dispositivo Bluetooth <Red de área personal> #2
16...5e 51 4f f6 b6 a2 ....Microsoft Virtual WiFi Miniport Adapter #2
15...5e 51 4f f6 b6 a3 ....Microsoft Virtual WiFi Miniport Adapter
14...5c 51 4f f6 b6 a2 ....Intel(R) Dual Band Wireless-AC 7260
13...28 d2 44 3f f2 29 ....Intel(R) Ethernet Connection I217-LM
19...00 50 56 c0 00 01 ....VMware Virtual Ethernet Adapter for VMnet1
20...00 50 56 c0 00 08 ....VMware Virtual Ethernet Adapter for VMnet8
22...0a 00 27 00 00 16 ....VirtualBox Host-Only Ethernet Adapter
1...00 00 00 00 00 00 ....Software Loopback Interface 1
23...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft
24...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #2
27...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #3
28...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #4
26...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #6
21...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #7
25...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #8
31...00 00 00 00 00 e0 Adaptador 6to4 de Microsoft
56...00 00 00 00 00 e0 Adaptador ISATAP de Microsoft #9
=====
```

Figura 13. Tabla de enrutamiento e interfaces (Anexo 9 - Enrutamiento de la red)

Se realizan escaneos de vulnerabilidades con las herramientas con perfil básico y avanzado, también la generación de reportes de cada una de las herramientas para registro en una base consolidada y realizar seguimiento de resultados.

En esta fase de pruebas se realizaron los escaneos sobre la herramienta Nessus y Retina, se ha realizado el registro de cada escaneo en una tabla de Excel para consolidación y organización de la información y posterior entrega técnica y gerencial para el análisis. (Anexo 10 - Registro Fase de Pruebas)

Así se presentan a continuación las pruebas realizadas sobre la fecha correspondiente y descripción asociada:

#### **10.2.1 Pruebas realizadas el 15 de febrero de 2019**

Se inician los escaneos de vulnerabilidades sobre las IPs de cada host reportado por medio de conexión VPN con la herramienta Nessus y perfil básico en estaciones de trabajo diferentes desde sistema operativo Windows 10.

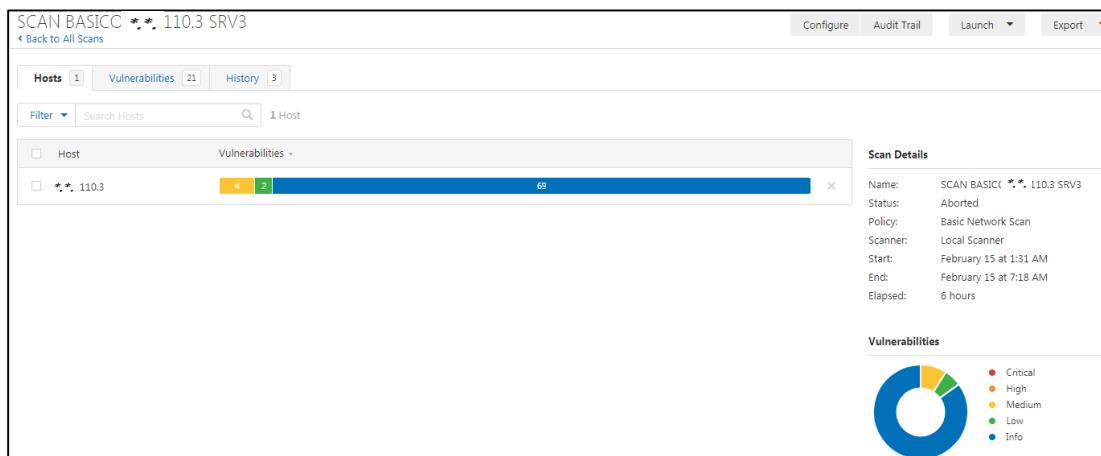


Figura 14. Escaneo con herramienta Nessus ( Anexo 11 - Escaneo Nessus 15Feb)

Tabla 6. Resultados herramienta Nessus consolidado en tabla Excel

FECHA	RESPONSABLE	HERRAMIENTA	DURACION	PERFIL ESCANEADO	CANTIDAD VULNERABILIDADES	CRITICIDAD	NOMBRE VULNERABILIDADES	FAMILIA VULNERABILIDADES	CONTEO VULNERABILIDADES	EVIDENCIA
14/2/2019	DIANA BARRERA	NESSUS-W7	9 MINUTOS	NETWORK BASIC (all ports)	11	1.0	NESSUS STOLEN SCANNER SSH Multiple issues Service detection Service detection(help request) Common platform enumeration(CPE) MySQL server detection Nessus scan information SSH server type and version information TCP/IP timestamps supported Traceroute information	Port scanners General Service detection Service detection Service detection General Databases Settings Service detection General	1 2 2 2 1 1 1 1 1 1	REPORTE 4

### 10.2.2 Pruebas realizadas semana 25 febrero - 3 marzo de 2019

De acuerdo con las conversaciones realizadas con la empresa por temas legales que no generen implicaciones al realizar los escaneos, se suspende la actividad por una semana, hasta que la empresa reporte por medio escrito que el proveedor IFX no será notificado sobre las pruebas a realizar.

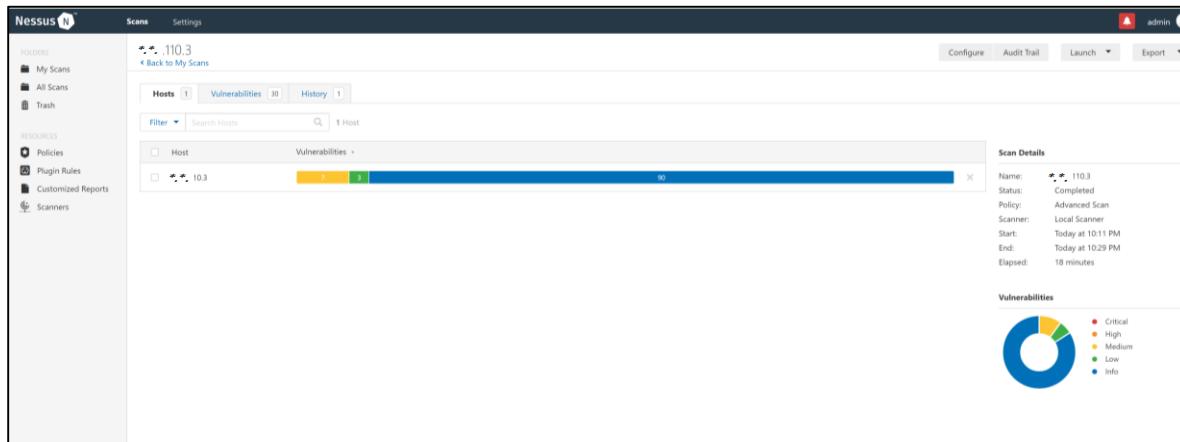


Figura 15. Escaneo con herramienta Nessus ( Anexo 12 - Pruebas Feb25 Mar03 )

Tabla 7. Resultados consolidados herramienta Nessus

FECHA	RESPONSABLE	HERRAMIENTA	DURACION	PERFIL ESCANEO	CANTIDAD VULNERABILIDADES	CRITICIDAD	NOMBRE VULNERABILIDADES	FAMILIA VULNERABILIDADES	CONTEO VULNERABILIDADES	EVIDENCIA
14/2/2019	DIANA BARRERA	NESSUS-W7	6 HORAS	NETWORK	9	1 4 2	HTTP Multiple Issues Redis Server Unprotected by Password Authentication SSL Certificate Cannot Be Trusted Apache Server Logging Mechanism Disclosure HTTP TRACE / FRAMES Method Allowed SSL Medium Strength Cipher Suites Supported SSH Server CBC Mode Ciphers Enabled SSL Anonymous Cipher Suites Supported Apache Banner Linux Distribution Disclosure Apache HTTP Server Version Backported Security Patch Detection (PHP) Backported Security Patch Detection (SSH) Local Checks Not Enabled (Info) Microsoft Windows SMB2 Dialects Supported (remote check) Nessus STM scanner Service Detection TCP/IP Timestamps Supported TLS ALPN Supported Protocol Enumeration TLS NPN Supported Protocol Enumeration Traceroute Information Web Server No 404 Error Code Check nginx HTTP Server Detection	Web servers Misc	18	Reporte 1
25/2/2019	DIANA MUNAR	NESSUS-W7	6 MINUTOS	ADVANCED SCAN	49	42				*.*.*.10_2_Ejecutivo

Se realiza en Nessus la personalización de perfiles para los escaneos, a continuación, se muestra un ejemplo de escaneo múltiple a los 4 hosts

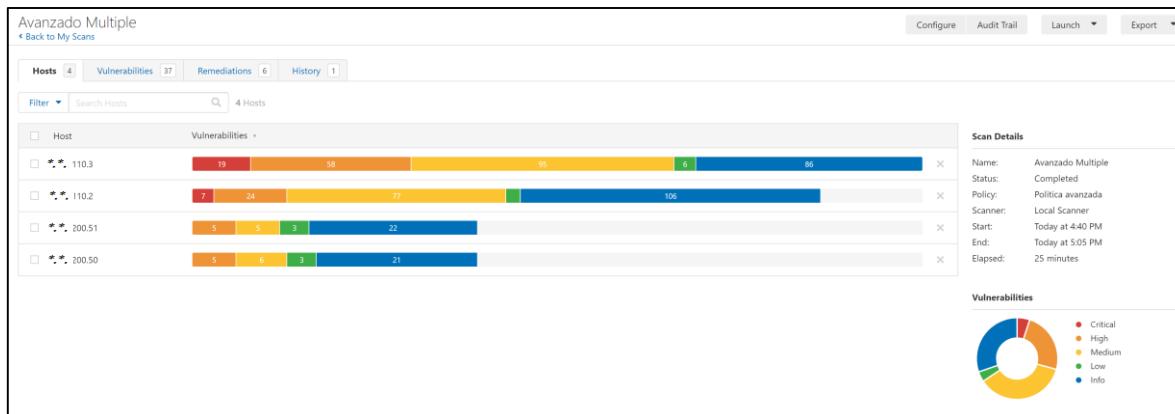


Figura 16. Escaneo múltiple con herramienta Nessus ( Anexo 13 - Escaneo Múltiple )

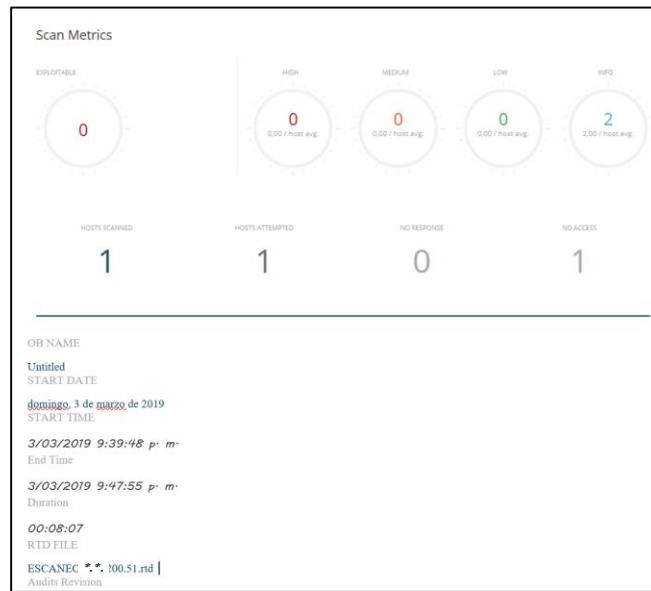


Figura 17. Escaneo múltiple con herramienta Retina ( Anexo 14 - Escaneo Retina )

Tabla 8. Resultados herramienta Retina

FECHA	RESPONSABLE	HERRAMIENTA	DURACION	PERFIL ESCANEO	CANTIDAD VULNERABILIDADES	CRITICIDAD	NOMBRE VULNERABILIDADES	FAMILIA VULNERABILIDADES	CONTEO VULNERABILIDADES	EVIDENCIA
3/3/2019	CARLOS MOGOLLON	RETINA	8 MINUTOS	NETWORK BASIC (all ports)	2	informativa	Acceso local SSH no disponible	Se encontraron los puertos abiertos TCP: 20001 Millennium	1	
						informativa	Servidor SSH detectado	TCP: 22 SSH - SSH (Secure Shell) Remote Login Protocol	1	REPORTE *.*, 100.51
								TCP: 3306 MySQL	1	

### 10.2.3 Pruebas realizadas semana 4 marzo-10 marzo de 2019

Durante la realización de las pruebas en este periodo de tiempo, se presentaron inconvenientes con la conexión, no estaba muy estable la VPN, adicionalmente al lanzar los escaneos no duraba más de un minuto la prueba y los resultados estaban en ceros, adicionalmente se logra realizar la instalación de la herramienta Nessus sobre Kali Linux, se ejecuta el escaneo en básico, sin embargo solo permite encontrar registro de vulnerabilidades en una IP de las 4 de pruebas, como se puede observar en las imágenes a continuación.

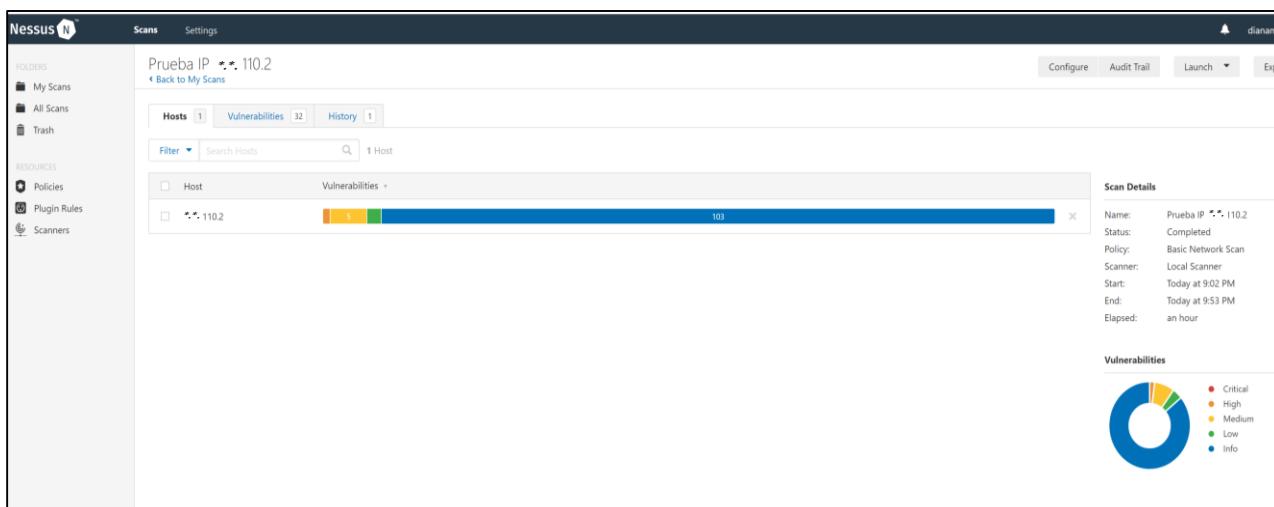


Figura 18. Escaneo simple con herramienta Nessus ( Anexo 15 - Pruebas Mar04)

Tabla 9. Resultados herramienta Nessus

FECHA	RESPONSABLE	HERRAMIENTA	DURACION	PERFIL ESCANEO	CANTIDAD VULNERABILIDADES	CRITICIDAD	NOMBRE VULNERABILIDADES
7/3/2019	DIANA MUNAR	NESSUS W10	1 HORA	BASIC NETWORK SCAN	49	1 4 2	Redis Server Unprotected by Password Authentication SSL Certificate Cannot Be Trusted Apache Server ETag Header Information Disclosure HTTP TRACE / TRACK Methods Allowed SSL Medium Strength Cipher Suites Supported (SWEET32) SSH Server CBC Mode Ciphers Enabled SSL Anonymous Cipher Suites Supported Apache Banner Linux Distribution Disclosure

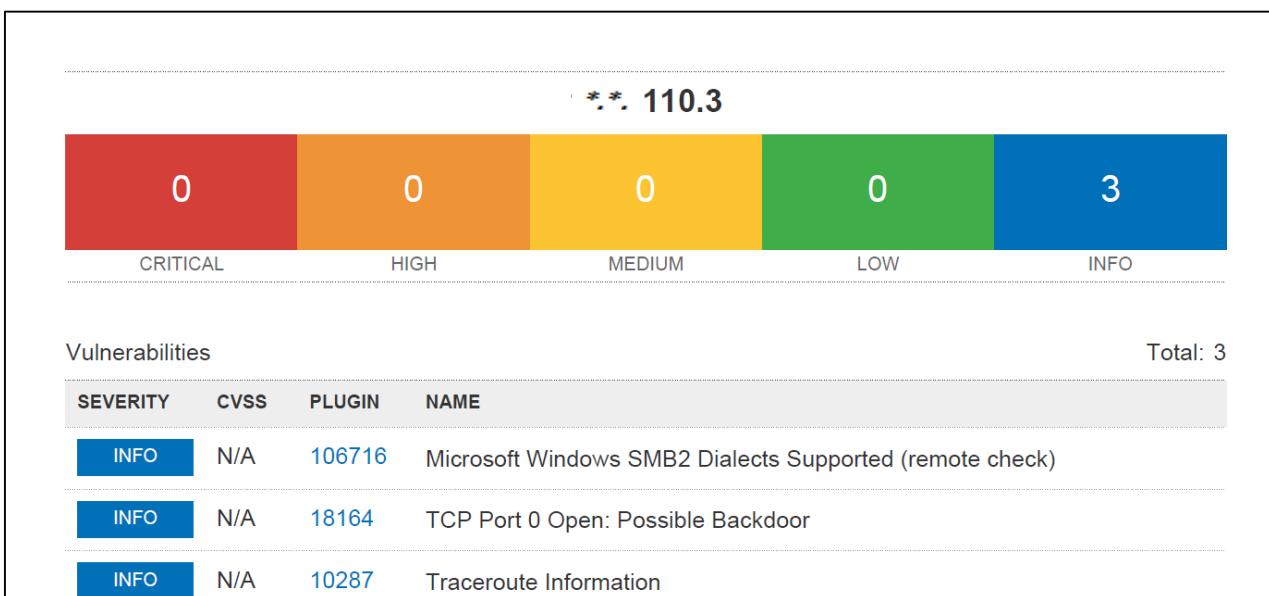


Figura 19. Escaneo simple con herramienta Nessus – Kali Linux

Tabla 10. Resultados herramienta Nessus – Kali Linux

FECHA	RESPONSABLE	HERRAMIENTA	DURACION	PERFIL ESCANEC	CANTIDAD VULNERABILIDADES	CRITICIDAD	NOMBRE VULNERABILIDADES
7/3/2019	DIANA MUNAR	NESSUS-KALI LINUX	40 MINUTOS	NETWORK BASIC (all ports)	3	1	Microsoft Windows SMB2 Dialects Supported (remote check)
7/3/2019	DIANA MUNAR	NESSUS-KALI LINUX	40 MINUTOS	NETWORK BASIC (all ports)	3	1	TCP Port 0 Open: Possible Backdoor
7/3/2019	DIANA MUNAR	NESSUS-KALI LINUX	40 MINUTOS	NETWORK BASIC (all ports)	3	1	Traceroute Information

### 10.3.4 Pruebas realizadas 3semana 11 marzo-17 marzo de 2019

Las pruebas realizadas esta semana se hicieron sobre Retina en donde se obtuvo buena información como se describe a continuación:

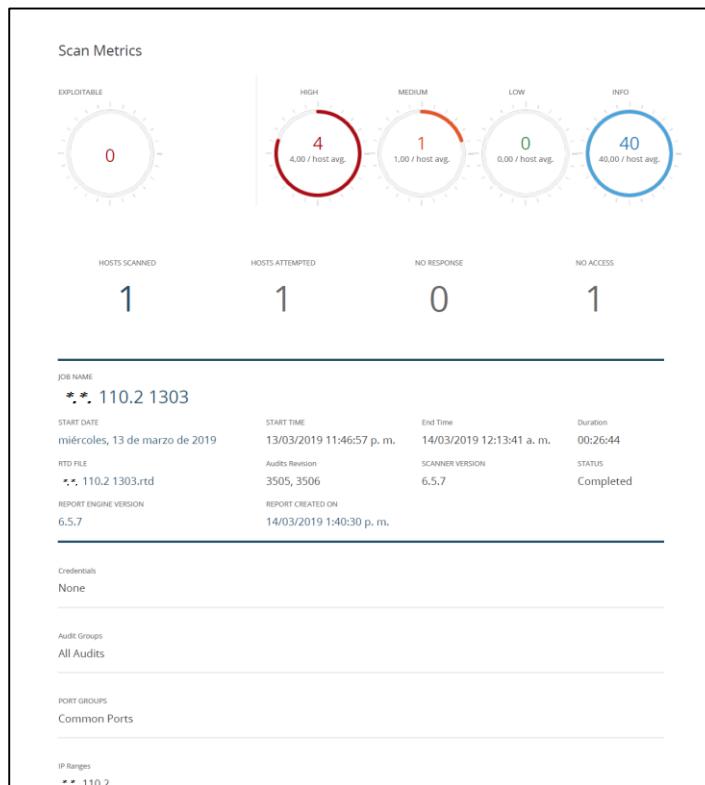


Figura 20. Escaneo simple con herramienta Retina (Anexo 16- Pruebas Mar11-17 Retina)

Tabla 11. Resultados herramienta Retina

FECHA	RESPONSABLE	HERRAMIENTA	DURACION	PERFIL ESCANEO	CANTIDAD VULNERABILIDADES	CRITICIDAD	NOMBRE VULNERABILIDADES	FAMILIA VULNERABILIDADES
28/2/2019	CARLOS MOGOLLON	RETINA	19.02 MINUTOS	NETWORK BASIC (all ports)	3	3	Servidor HTTP Nginx detectado	TCP: 22 SSH - SSH (Secure Shell) Remote Login Protocol TCP: 443 WWW-HTTP - World Wide Web Hyper Text Transfer Protocol TCP: 53 DNS - Domain Service TCP: 80 WWW-HTTP - World Wide Web Hyper Text Transfer Protocol TCP: 8080 WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
28/2/2019	CARLOS MOGOLLON	RETINA	19.02 MINUTOS	NETWORK BASIC (all ports)	3	3	Acceso local SSH no disponible	Web HTTP (Hyper Text Transfer Protocol) TCP: 8081 WWW-HTTP - World Wide Web Hyper Text Transfer Protocol TCP: 9080 WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
28/2/2019	CARLOS MOGOLLON	RETINA	19.02 MINUTOS	NETWORK BASIC (all ports)	3	3	Servidor SSH detectado	Web HTTP (Hyper Text Transfer Protocol) TCP: 8081 WWW-HTTP - World Wide Web Hyper Text Transfer Protocol TCP: 9080 WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
12/3/2019	CARLOS MOGOLLON	RETINA	22:01 MINUTOS	NETWORK BASIC (all ports)	45	4	3 Vulnerabilidad de ataque de cumpleaños triple DES (Sweet32) 1 Autenticación Redis desactivada	
12/3/2019	CARLOS MOGOLLON	RETINA	22:01 MINUTOS	NETWORK BASIC (all ports)	45	1	Versión de protocolo débil TLS / SSL compatible	
12/3/2019	CARLOS MOGOLLON	RETINA	22:01 MINUTOS	NETWORK BASIC (all ports)	45		SSL/TLS Cipher Suites Supported	
12/3/2019	CARLOS MOGOLLON	RETINA	22:01 MINUTOS	NETWORK BASIC (all ports)	45		CBC Symmetric Encryption Security Feature Bypass	
12/3/2019	CARLOS MOGOLLON	RETINA	22:01 MINUTOS	NETWORK BASIC (all ports)	45		HTTP 1.1 Protocol Detected	
12/3/2019	CARLOS MOGOLLON	RETINA	22:01 MINUTOS	NETWORK BASIC (all ports)	45		SSL/TLS Cipher Block Chaining Cipher Suites Supported	
12/3/2019	CARLOS MOGOLLON	RETINA	22:01 MINUTOS	NETWORK BASIC (all ports)	45		SSL Certificate Public Key Algorithm	TCP: 22 SSH - SSH (Secure Shell) Remote Login Protocol TCP: 443 WWW-HTTP - World Wide Web Hyper Text Transfer Protocol

### 10.3 Escaneos sobre los servidores en producción

En esta fase de escaneo en servidores en producción se realizaron las pruebas sobre Nessus y Nmap. Para este trabajo se ha realizado una documentación de cada escaneo en tabla de Excel que se relacionará más adelante en este documento para organización de la información y posterior entrega técnica y gerencial para el análisis.

Para el caso de Nessus el perfil seleccionado es avanzado opción múltiple con todas las opciones de escaneo:

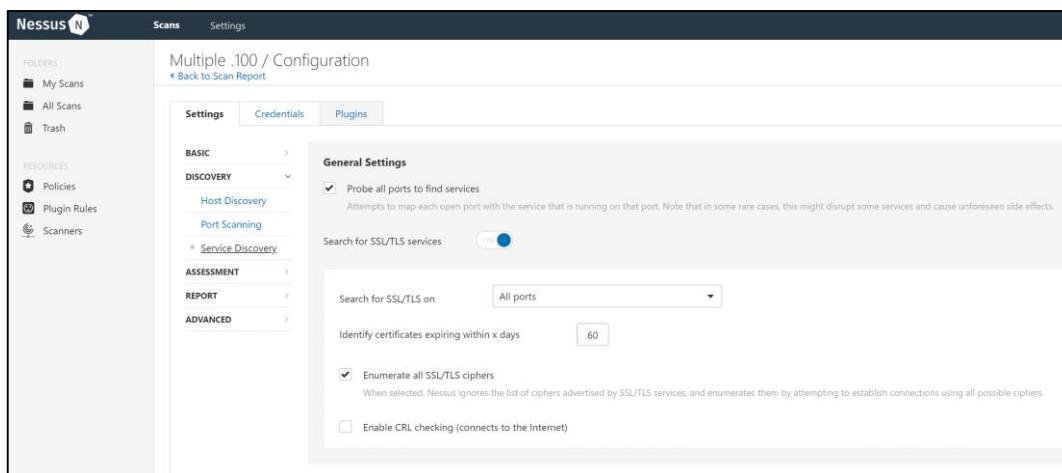


Figura 21. Escaneo simple con herramienta Nessus – Service Discovery

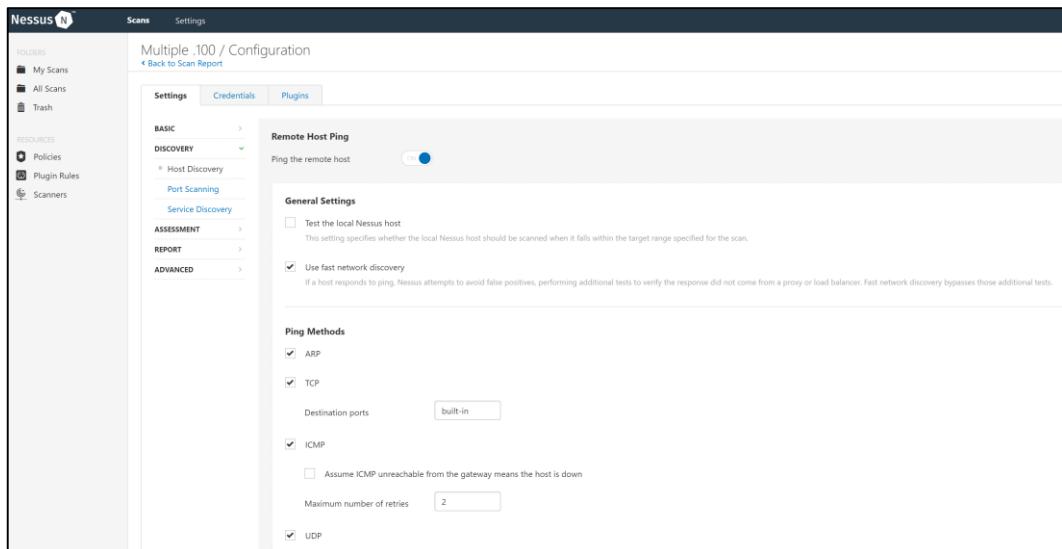


Figura 22. Escaneo simple con herramienta Nessus – Host Discovery

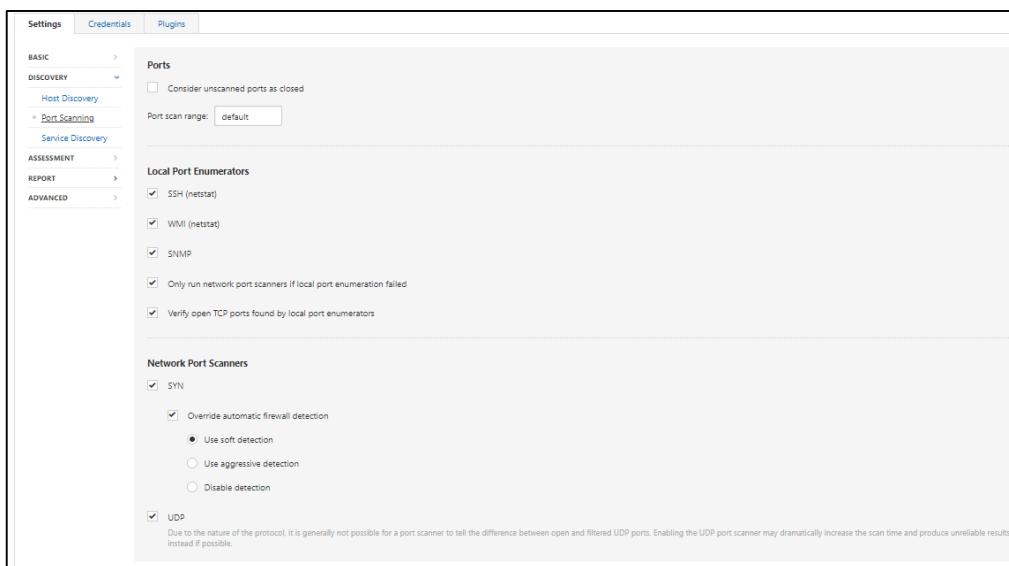


Figura 23. Escaneo simple con herramienta Nessus – Service Discovery

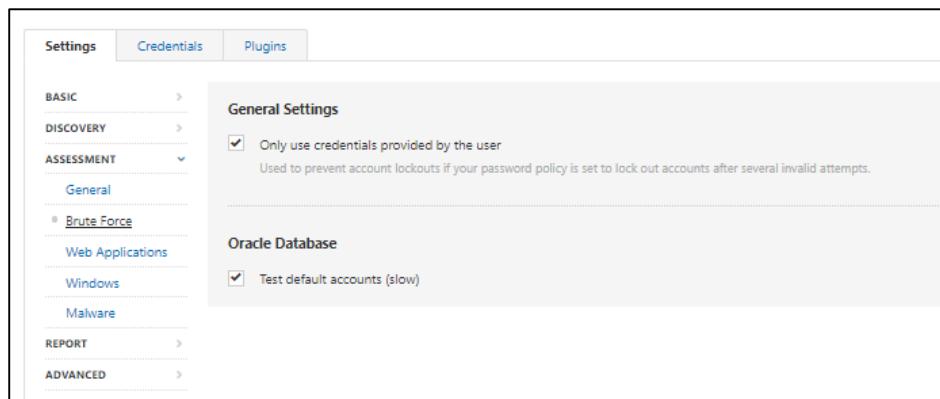


Figura 24. Escaneo simple con herramienta Nessus – Fuerza bruta

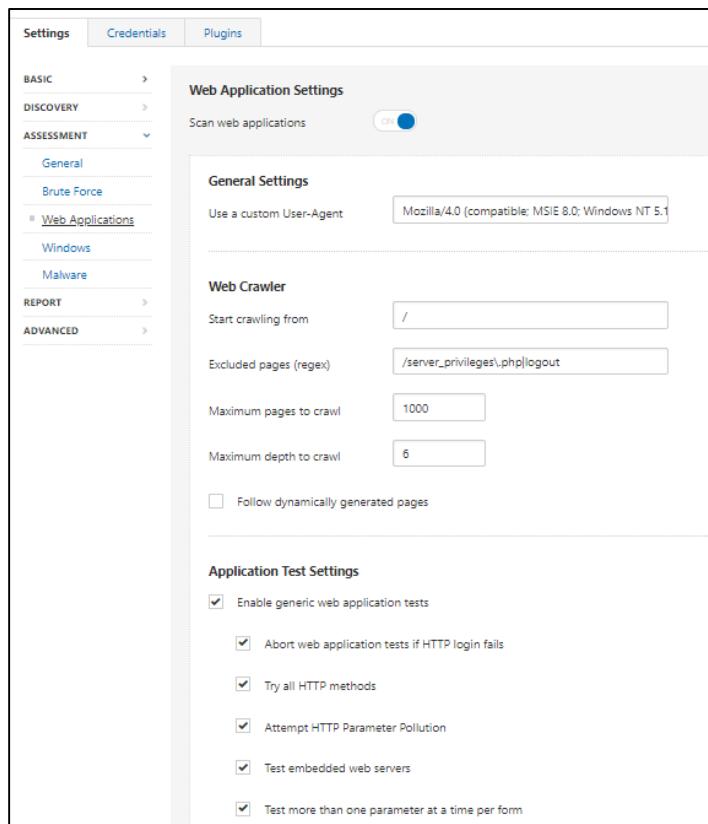
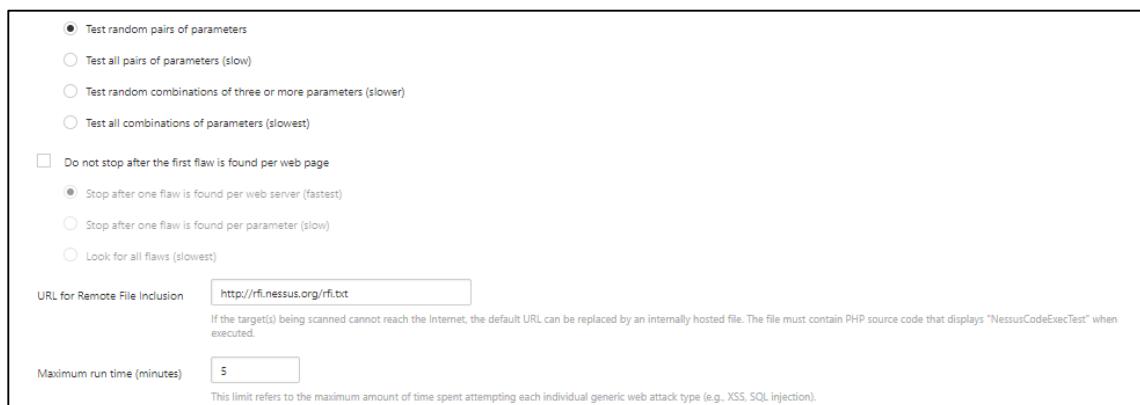


Figura 25. Escaneo simple con herramienta Nessus – Aplicaciones Web



Test random pairs of parameters  
 Test all pairs of parameters (slow)  
 Test random combinations of three or more parameters (slower)  
 Test all combinations of parameters (slowest)

Do not stop after the first flaw is found per web page  
 Stop after one flaw is found per web server (fastest)  
 Stop after one flaw is found per parameter (slow)  
 Look for all flaws (slowest)

URL for Remote File Inclusion:   
If the target(s) being scanned cannot reach the Internet, the default URL can be replaced by an internally hosted file. The file must contain PHP source code that displays "NessusCodeExecTest" when executed.

Maximum run time (minutes):   
This limit refers to the maximum amount of time spent attempting each individual generic web attack type (e.g., XSS, SQL injection).

Figura 26. Escaneo simple con herramienta Nessus – Service Discovery

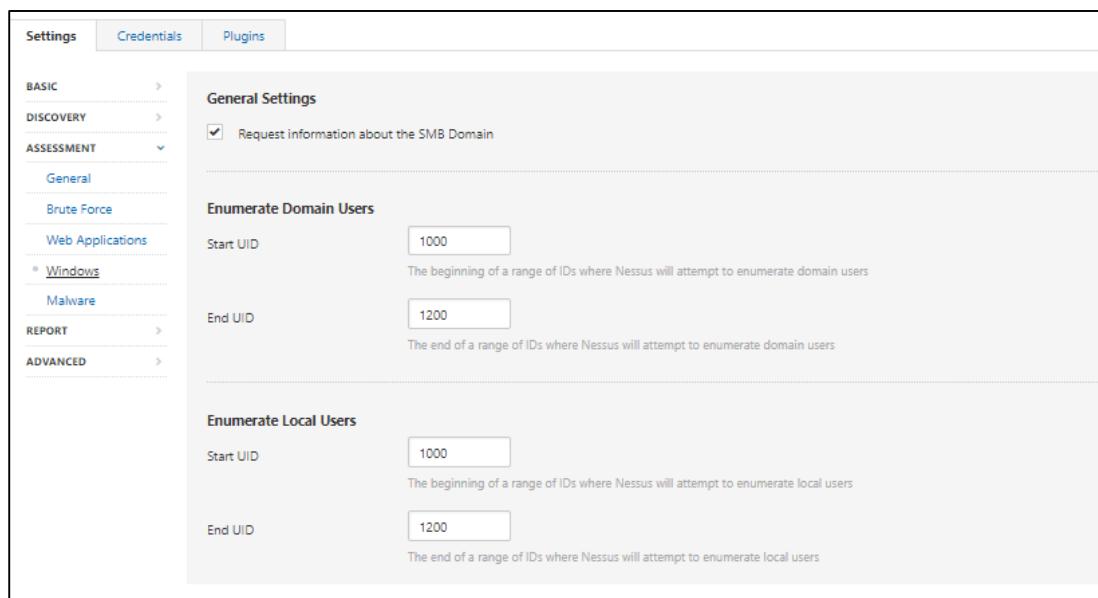


Figura 27. Escaneo simple con herramienta Nessus – Windows

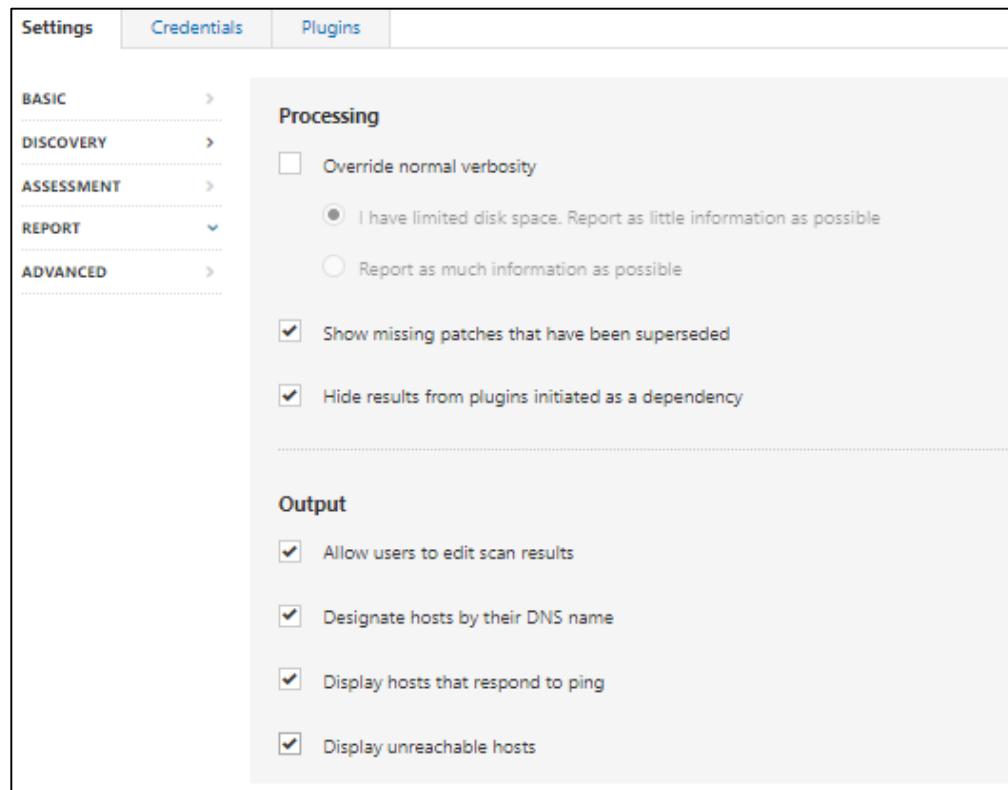


Figura 28. Escaneo simple con herramienta Nessus

Se presentan a continuación las pruebas realizadas sobre la fecha correspondiente y descripción asociada:

### 10.3.1 Pruebas realizadas semana 1 de Abril de 2019

Se inicia el escaneo de puertos sobre los servidores con la herramienta Nmap en cada uno de los rangos:

```
C:\WINDOWS\system32>nmap --script=vuln *.*.100.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 21:13 Hora est. Pacífico, Sudamérica
Nmap scan report for *.*.100.10
Host is up (0.12s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs: CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible. It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
  http://ha.ckers.org/slowloris/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

Figura 29. Evidencia vulnerabilidad CVE-2007-6750 sobre todos servidores rango .100

```
C:\WINDOWS\system32>nmap --script=vuln *.*.200.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 21:18 Hora est. Pacífico, Sudamérica
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for *.*.200.10
Host is up (0.13s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
3306/tcp  open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)

Host script results:
| firewall-bypass:
|_ Firewall vulnerable to bypass through ftp helper. (IPv4)

Nmap done: 1 IP address (1 host up) scanned in 38.06 seconds
```

Figura 30. Evidencia vulnerabilidad CVE-2012-2122 sobre todos servidores rango .200

Se logra realizar la instalación de la herramienta Nessus sobre Kali Linux, se ejecuta el escaneo en básico por medio de la VPN instalada en Windows 10, sin embargo, no es posible ejecutar la prueba con éxito.

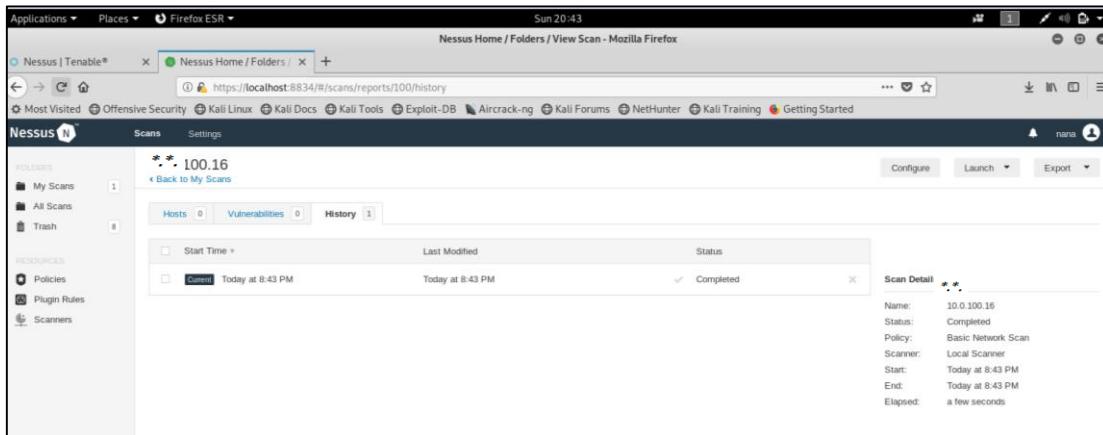


Figura 31. Evidencia falla escaneos en Linux

```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\System32>nmap --script=vuln *.*.100.11
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 18:59 Hora est. Pacífico,
Sudamérica
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address <0 hosts up> scanned in 131.79 seconds
```

Figura 32. Evidencia 28 Abril

```
C:\Windows\system32>nmap *.*.100.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-28 14:52 Hora est. Pacífico, Sudamérica
dnet: Failed to open device eth1
QUITTING!
```

Figura 33. Nmap Windows 7

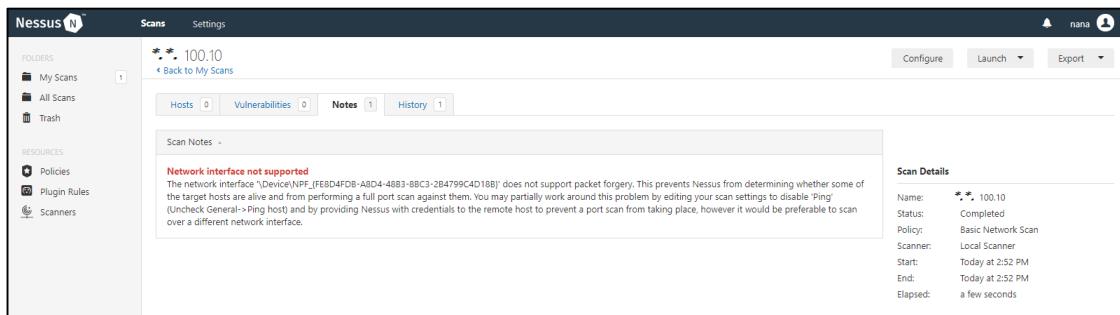


Figura 34. Nessus Windows 7

**Descripción error:** Error al recibir paquetes o transmitirlos de manera adecuada, puede pasar porque Winpcap no está instalado o esta corrupto, solución desinstalar, reinstalar, revisar que la tarjeta de red está en modo promiscuo y eso puede estar afectando el escaneo. Porque Nessus debe permitir escanear sin habilitar la opción “quitar ping a host remoto”, sino con todas las funcionalidades para que el escaneo sea más amplio. [19]

Quitando ping a host remoto (Discovery custom). Si funciona, aunque antes servía sin habilitar esa opción y se podían seleccionar puertos “default” o “all”.

### 10.3.2 Ejecución de las pruebas

El escaneo sobre los 30 servidores en producción se realiza desde el sistema operativo Windows 7 y Windows 10 realizando conexión por VPN canal que nos ha habilitado la empresa para realizar las pruebas requeridas.

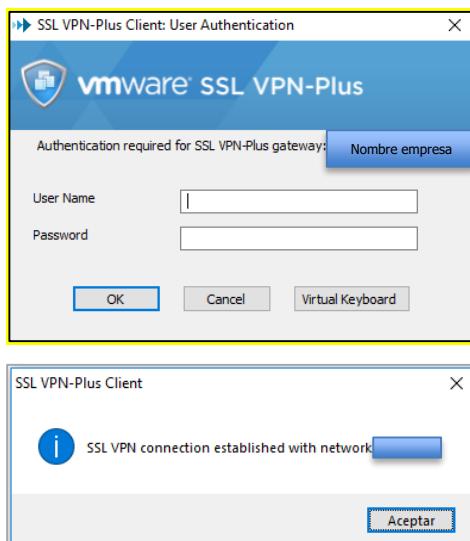


Figura 35. Conexión a la VPN establecida

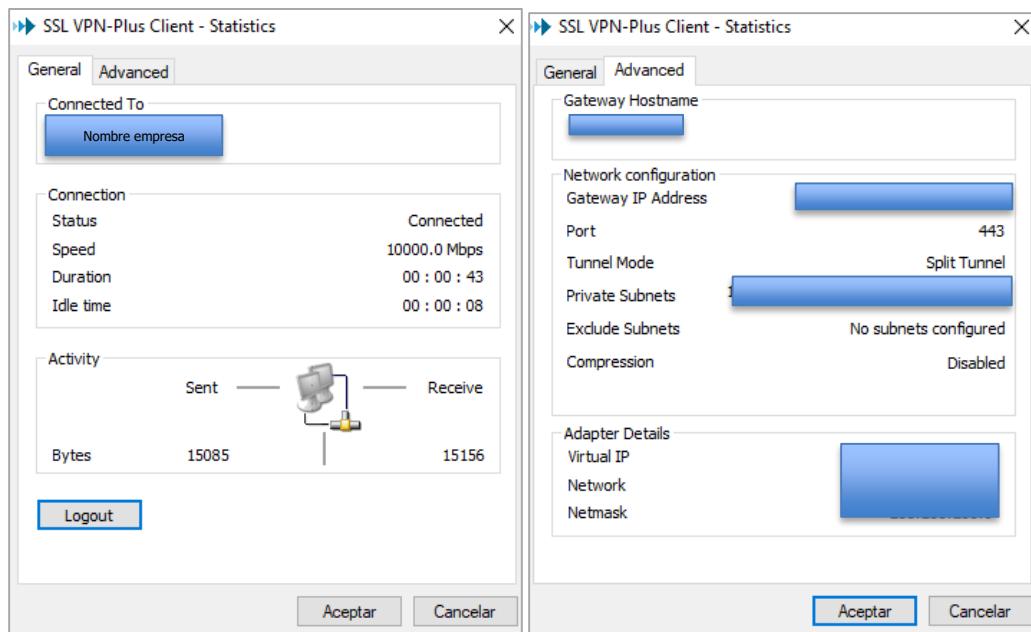


Figura 36. Verificación de conexión a la VPN

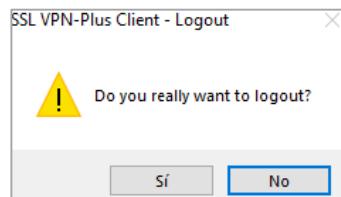


Figura 37. Desconexión de la VPN

Se valida que estemos dentro de la red después de conectarse por medio de la VPN ingresando a una página web y digitando alguna de las direcciones IP de los servidores, probamos una dirección de cada rango donde el .100 y .110 siempre responden, el rango de IPs .200 no mostraba la conexión o visualización en página web sin embargo siempre permitió realizar los escaneos con la herramienta Nessus y Nmap.

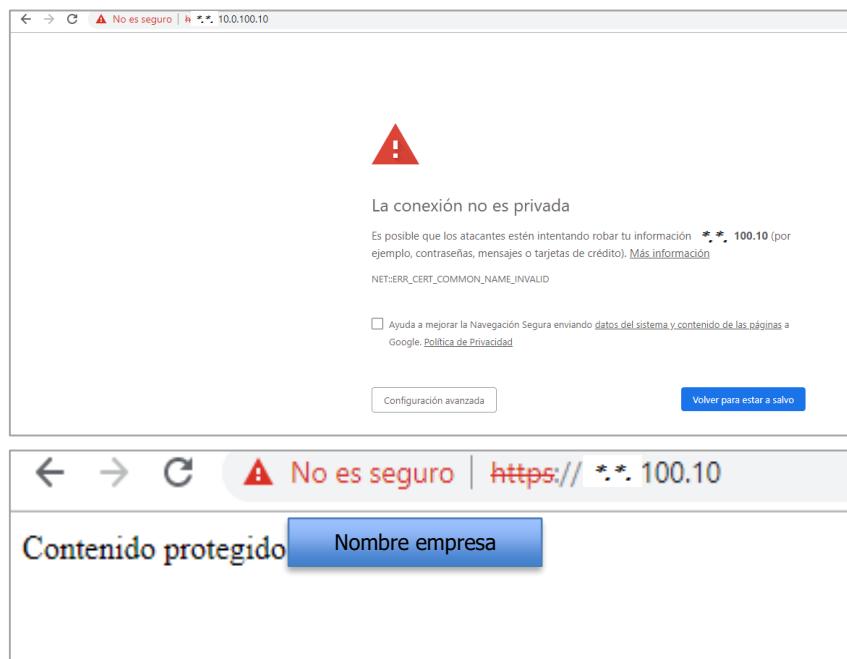


Figura 38. Evidencia conexión IP \*.\*.100.10 del rango de IPs .100

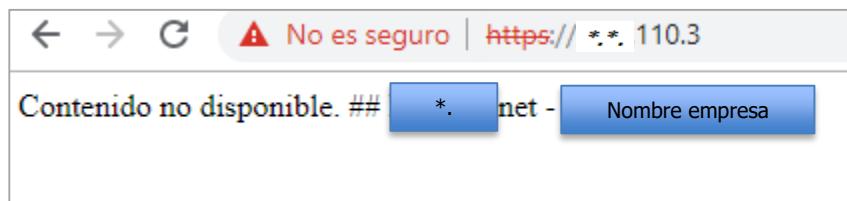


Figura 39. Evidencia conexión IP \*.\*.110.3 del rango de IPs .110

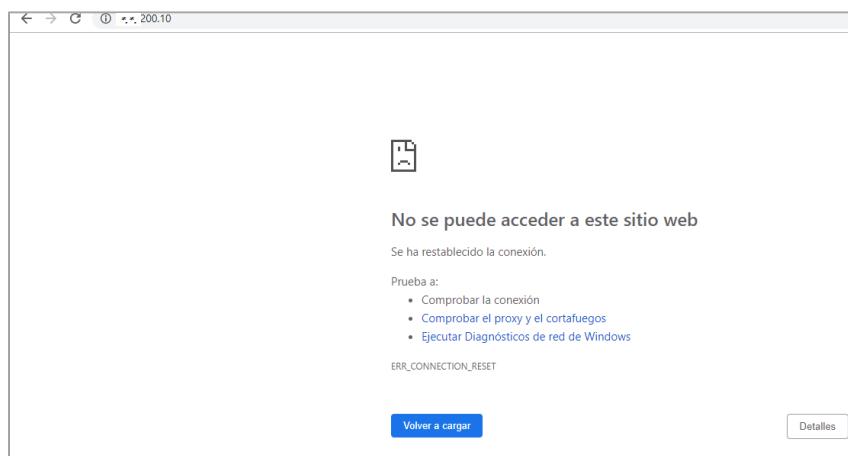


Figura 40. Prueba conexión IP \*.\*.200.10 del rango de IPs .200

### 10.3.3 Revisión conexiones activas

En algunas ocasiones al realizar pruebas de conexión de los puertos sobre los servidores, genera correctamente la conexión desde la empresa, como se presenta en la siguiente imagen:

C:\Windows\system32>netstat *.* 100.10			
Conexiones activas			
Proto	Dirección local	Dirección remota	Estado
TCP	*.*.0.2:36671	*.*.110.4:4430	ESTABLISHED
TCP	*.*.0.2:37502	*.*.100.14:11234	SYN_SENT
TCP	*.*.0.2:37518	*.*.100.13:11234	SYN_SENT
TCP	*.*.0.2:37785	*.*.100.12:https	ESTABLISHED
TCP	*.*.0.2:37831	*.*.110.4:8080	ESTABLISHED
TCP	*.*.0.2:38007	*.*.110.4:4430	ESTABLISHED
TCP	*.*.0.2:38053	*.*.100.15:8080	ESTABLISHED
TCP	*.*.0.2:38067	*.*.100.12:https	ESTABLISHED
TCP	*.*.0.2:38075	*.*.110.3:9443	ESTABLISHED
TCP	*.*.0.2:38110	*.*.100.20:8083	ESTABLISHED
TCP	*.*.0.2:38112	*.*.100.12:https	ESTABLISHED
TCP	*.*.0.2:38128	*.*.110.4:4430	ESTABLISHED
TCP	*.*.0.2:38147	*.*.100.14:25300	SYN_SENT
TCP	*.*.0.2:38151	*.*.110.2:8080	ESTABLISHED
TCP	*.*.0.2:38161	*.*.110.4:8118	ESTABLISHED
TCP	*.*.0.2:38177	*.*.100.14:https	ESTABLISHED
TCP	*.*.0.2:38178	*.*.100.12:https	ESTABLISHED
TCP	*.*.0.2:38185	*.*.110.2:9443	ESTABLISHED
TCP	*.*.0.2:38211	*.*.100.13:https	ESTABLISHED
TCP	*.*.0.2:38212	*.*.110.4:4430	ESTABLISHED
TCP	*.*.0.2:38213	*.*.110.4:8080	ESTABLISHED
TCP	*.*.0.2:38215	*.*.110.2:9443	ESTABLISHED
TCP	*.*.0.2:38225	*.*.100.15:https	ESTABLISHED
TCP	*.*.0.2:38226	*.*.100.16:https	ESTABLISHED
TCP	*.*.0.2:38230	*.*.100.15:8083	ESTABLISHED
TCP	*.*.0.2:38235	*.*.100.16:8083	ESTABLISHED
TCP	*.*.0.2:38240	*.*.110.3:https	ESTABLISHED
TCP	*.*.0.2:38241	*.*.100.13:https	ESTABLISHED
TCP	*.*.0.2:38244	*.*.100.17:8084	ESTABLISHED
TCP	*.*.0.2:38245	*.*.110.3:8880	ESTABLISHED
TCP	*.*.0.2:38246	*.*.100.20:https	ESTABLISHED
TCP	*.*.0.2:38247	*.*.100.19:http	ESTABLISHED
TCP	*.*.0.2:38248	*.*.110.2:8083	ESTABLISHED
TCP	*.*.0.2:38249	*.*.100.14:https	ESTABLISHED
TCP	*.*.0.2:38250	*.*.100.19:https	ESTABLISHED
TCP	*.*.0.2:38251	*.*.100.19:http	ESTABLISHED
TCP	*.*.0.2:38252	*.*.110.4:8118	ESTABLISHED

Figura 41. Revisión conexiones activas (Netstat)

Algunas ocasiones para todos los servidores mostro una imagen similar a la que se presenta a continuación, no se evidencia que sean del servidor evaluado, todo el origen es el pc local desde donde se efectúa la prueba del escaneo (192.168.0.5).

C:\Users\NANA>netstat -an 200.12						C:\Users\NANA>netstat -an 100.12					
Conexiones activas						Conexiones activas					
Proto	Dirección local	Dirección remota	Estado	Proto	Dirección local	Dirección remota	Estado	Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:1573	Nanitronik:1574	ESTABLISHED	TCP	127.0.0.1:1573	Nanitronik:1574	ESTABLISHED	TCP	127.0.0.1:1573	Nanitronik:1573	ESTABLISHED
TCP	127.0.0.1:1574	Nanitronik:1573	ESTABLISHED	TCP	127.0.0.1:1574	Nanitronik:1573	ESTABLISHED	TCP	127.0.0.1:1581	Nanitronik:1582	ESTABLISHED
TCP	127.0.0.1:1581	Nanitronik:1582	ESTABLISHED	TCP	127.0.0.1:1582	Nanitronik:1581	ESTABLISHED	TCP	127.0.0.1:13030	Nanitronik:50041	ESTABLISHED
TCP	127.0.0.1:1582	Nanitronik:1581	ESTABLISHED	TCP	127.0.0.1:13030	Nanitronik:50041	ESTABLISHED	TCP	127.0.0.1:13061	Nanitronik:53467	ESTABLISHED
TCP	127.0.0.1:13030	Nanitronik:50041	ESTABLISHED	TCP	127.0.0.1:13061	Nanitronik:53467	ESTABLISHED	TCP	127.0.0.1:13030	Nanitronik:13030	ESTABLISHED
TCP	127.0.0.1:13061	Nanitronik:53467	ESTABLISHED	TCP	127.0.0.1:13061	Nanitronik:13030	ESTABLISHED	TCP	127.0.0.1:13061	Nanitronik:13061	ESTABLISHED
TCP	127.0.0.1:13061	Nanitronik:13030	ESTABLISHED	TCP	127.0.0.1:13061	Nanitronik:13061	ESTABLISHED	TCP	192.168.0.5:12278	217:4070	ESTABLISHED
TCP	127.0.0.1:13061	Nanitronik:13061	ESTABLISHED	TCP	192.168.0.5:12278	47:https	ESTABLISHED	TCP	192.168.0.5:12278	do-20:https	ESTABLISHED
TCP	192.168.0.5:12273	217:4070	ESTABLISHED	TCP	192.168.0.5:12278	47:https	ESTABLISHED	TCP	192.168.0.5:12368	52.242.210.82:https	ESTABLISHED
TCP	192.168.0.5:12278	47:https	ESTABLISHED	TCP	192.168.0.5:12368	52.242.210.82:https	ESTABLISHED	TCP	192.168.0.5:13007	52.242.210.82:https	ESTABLISHED
TCP	192.168.0.5:13007	52.242.210.82:https	ESTABLISHED	TCP	192.168.0.5:13049	host131:https	ESTABLISHED	TCP	192.168.0.5:13051	52.230.222.68:https	ESTABLISHED
TCP	192.168.0.5:13028	52.242.210.82:https	ESTABLISHED	TCP	192.168.0.5:13051	52.230.222.68:https	ESTABLISHED	TCP	192.168.0.5:13055	vt-in-f188:https	ESTABLISHED
TCP	192.168.0.5:13049	host131:https	ESTABLISHED	TCP	192.168.0.5:13055	vt-in-f188:https	ESTABLISHED	TCP	192.168.0.5:13057	192.16.59.1:https	ESTABLISHED
TCP	192.168.0.5:13051	52.230.222.68:https	ESTABLISHED	TCP	192.168.0.5:13057	192.16.59.1:https	ESTABLISHED	TCP	192.168.0.5:13057	53:https	ESTABLISHED
TCP	192.168.0.5:13055	vt-in-f188:https	ESTABLISHED	TCP	192.168.0.5:13080	gru06s09-in-f101:https	ESTABLISHED	TCP	192.168.0.5:13080	52.242.210.82:https	ESTABLISHED
TCP	192.168.0.5:13057	53:https	ESTABLISHED	TCP	192.168.0.5:13333	8.18.25.24:http	ESTABLISHED	TCP	192.168.0.5:13336	63.251.166.36:https	CLOSE_WAIT
TCP	192.168.0.5:13080	gru06s09-in-f101:https	ESTABLISHED	TCP	192.168.0.5:13337	63.251.166.36:https	CLOSE_WAIT	TCP	192.168.0.5:13332	ec2-34-192-123-20:https	CLOSE_WAIT
TCP	192.168.0.5:13080	52.242.210.82:https	ESTABLISHED	TCP	192.168.0.5:13338	63.251.166.36:https	CLOSE_WAIT	TCP	192.168.0.5:13340	gru06s09-in-f106:https	ESTABLISHED
TCP	192.168.0.5:13080	40.97.24.18:https	TIME_WAIT	TCP	192.168.0.5:13340	gru06s09-in-f106:https	ESTABLISHED	TCP	192.168.0.5:13342	gru06s09-in-f106:https	ESTABLISHED
TCP	192.168.0.5:13080	52.189.124.18:https	ESTABLISHED	TCP	192.168.0.5:13342	gru06s09-in-f106:https	ESTABLISHED	TCP	192.168.0.5:13344	gru06s09-in-f106:https	ESTABLISHED
TCP	192.168.0.5:13080	8.18.25.24:https	ESTABLISHED	TCP	192.168.0.5:13344	gru06s09-in-f106:https	ESTABLISHED	TCP	192.168.0.5:13345	gru06s09-in-f106:https	ESTABLISHED
TCP	192.168.0.5:13080	52.18.25.72:https	ESTABLISHED	TCP	192.168.0.5:13345	gru06s09-in-f106:https	ESTABLISHED	TCP	192.168.0.5:13346	gru06s09-in-f106:https	ESTABLISHED
TCP	192.168.0.5:13080	gru06s09-in-f106:https	ESTABLISHED	TCP	192.168.0.5:13346	gru06s09-in-f106:https	ESTABLISHED	TCP	192.168.0.5:13347	52.114.32.7:https	ESTABLISHED
Conexiones activas						Conexiones activas					
Proto	Dirección local	Dirección remota	Estado	Proto	Dirección local	Dirección remota	Estado	Proto	Dirección local	Dirección remota	Estado
TCP	127.0.0.1:1573	Nanitronik:1574	ESTABLISHED	TCP	127.0.0.1:1574	Nanitronik:1574	ESTABLISHED	TCP	127.0.0.1:1574	Nanitronik:1573	ESTABLISHED
TCP	127.0.0.1:1574	Nanitronik:1573	ESTABLISHED	TCP	127.0.0.1:1574	Nanitronik:1582	ESTABLISHED	TCP	127.0.0.1:1581	Nanitronik:1582	ESTABLISHED
TCP	127.0.0.1:1581	Nanitronik:1582	ESTABLISHED	TCP	127.0.0.1:1582	Nanitronik:1581	ESTABLISHED	TCP	127.0.0.1:13030	Nanitronik:50041	ESTABLISHED
TCP	127.0.0.1:1582	Nanitronik:1581	ESTABLISHED	TCP	127.0.0.1:13061	Nanitronik:53467	ESTABLISHED	TCP	127.0.0.1:13061	Nanitronik:13030	ESTABLISHED

Figura 42. Revisión conexiones activas (Nestat)

### 10.3.4 Revisión de puertos abiertos/cerrados(nmap/zenmap)

Se realiza escaneo desde Zenmap para validar los puertos que se encuentran abiertos en los servidores.

```
Initiating SYN Stealth Scan at 22:32
Scanning *.*.110.4 [65535 ports]
Discovered open port 135/tcp on *.*.110.4
Discovered open port 3389/tcp on *.*.110.4
Discovered open port 139/tcp on *.*.110.4
Discovered open port 8080/tcp on *.*.110.4
Discovered open port 445/tcp on *.*.110.4
Discovered open port 8118/tcp on *.*.110.4
Discovered open port 49670/tcp on *.*.110.4
Discovered open port 5985/tcp on *.*.110.4
Discovered open port 4430/tcp on *.*.110.4
Discovered open port 47001/tcp on *.*.110.4
Discovered open port 47101/tcp on *.*.110.4
Discovered open port 49667/tcp on *.*.110.4
Discovered open port 49677/tcp on *.*.110.4
Discovered open port 51252/tcp on *.*.110.4
Discovered open port 47100/tcp on *.*.110.4
Discovered open port 4530/tcp on 1 *.*.110.4
Discovered open port 5672/tcp on *.*.110.4
Discovered open port 49668/tcp on *.*.110.4
Discovered open port 9200/tcp on 1 *.*.110.4
Discovered open port 49666/tcp on *.*.110.4
Discovered open port 943/tcp on 10 *.*.0.4
Discovered open port 49664/tcp on *.*.110.4
Discovered open port 9300/tcp on *.*.110.4
Discovered open port 5432/tcp on *.*.110.4
Discovered open port 3333/tcp on *.*.110.4
Discovered open port 49665/tcp on *.*.110.4
Discovered open port 1433/tcp on *.*.110.4
Discovered open port 47500/tcp on *.*.110.4
Completed SYN Stealth Scan at 22:33, 64.34s elapsed (65535 total ports)
Initiating Service scan at 22:33
Scanning 28 services on *.*.110.4
```

Figura 43. Revisión conexiones activas (Nestat)

### 10.3.5 Pruebas de conectividad (ping)

En ocasiones daba respuesta la conexión y prueba por ping, en otras ocasiones no generaba respuesta posiblemente por restricción a nivel de firewall desde el objetivo.

```
C:\Users\NANA>ping *.*.100.10

Haciendo ping a *.*.100.10 con 32 bytes de datos:
Respuesta desde *.*.100.10: bytes=32 tiempo=178ms TTL=63
Respuesta desde *.*.100.10: bytes=32 tiempo=92ms TTL=63
Respuesta desde *.*.100.10: bytes=32 tiempo=89ms TTL=63

Estadísticas de ping para *.*.100.10:
  Paquetes: enviados = 3, recibidos = 3, perdidos = 0
              (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 89ms, Máximo = 178ms, Media = 119ms
```

Figura 44. Prueba de conectividad respuesta por ping rango .100

```
C:\Users\NANA>ping *.*.110.4

Haciendo ping a *.*.110.4 con 32 bytes de datos:
Respuesta desde *.*.110.4: bytes=32 tiempo=91ms TTL=127
Respuesta desde *.*.110.4: bytes=32 tiempo=87ms TTL=127

Estadísticas de ping para 10.0.110.4:
  Paquetes: enviados = 2, recibidos = 2, perdidos = 0
              (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 87ms, Máximo = 91ms, Media = 89ms
```

Figura 45. Prueba de conectividad respuesta por ping rango .110

```
C:\Users\NANA>ping *.*.200.52

Haciendo ping a *.*.200.52 con 32 bytes de datos:
Respuesta desde *.*.200.52: bytes=32 tiempo=88ms TTL=63
Respuesta desde *.*.200.52: bytes=32 tiempo=88ms TTL=63

Estadísticas de ping para *.*.200.52:
  Paquetes: enviados = 2, recibidos = 2, perdidos = 0
              (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 88ms, Máximo = 88ms, Media = 88ms
```

Figura 46. Prueba de conectividad respuesta por ping rango .200

IPv4 Tabla de enrutamiento					
Destino de red	Máscara de red	Puerta de enlace	Interfaz	Métrica	
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.5	25	
*.*.100.0	255.255.255.0	*.*.0.1	*.*.0.2	26	
*.*.100.255	255.255.255.255	*.*.0.1	*.*.0.2	26	
*.*.110.0	255.255.255.0	*.*.0.1	*.*.0.2	26	
*.*.110.255	255.255.255.255	*.*.0.1	*.*.0.2	26	
*.*.150.0	255.255.255.0	*.*.0.1	*.*.0.2	26	
*.*.150.255	255.255.255.255	*.*.0.1	*.*.0.2	26	
*.*.200.0	255.255.255.0	*.*.0.1	*.*.0.2	26	
*.*.200.255	255.255.255.255	*.*.0.1	*.*.0.2	26	
*.*.0.0	255.255.255.0	En vínculo	*.*.0.2	281	
*.*.0.2	255.255.255.255	En vínculo	*.*.0.2	281	
*.*.0.255	255.255.255.255	En vínculo	*.*.0.2	281	
127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	331	
127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	331	
127.255.255.255	255.255.255.255	En vínculo	127.0.0.1	331	
192.168.0.0	255.255.255.0	En vínculo	192.168.0.5	281	
192.168.0.5	255.255.255.255	En vínculo	192.168.0.5	281	
192.168.0.255	255.255.255.255	En vínculo	192.168.0.5	281	
192.168.56.0	255.255.255.0	En vínculo	192.168.56.1	281	
192.168.56.1	255.255.255.255	En vínculo	192.168.56.1	281	
192.168.56.255	255.255.255.255	En vínculo	192.168.56.1	281	
192.168.153.0	255.255.255.0	En vínculo	192.168.153.1	291	
192.168.153.1	255.255.255.255	En vínculo	192.168.153.1	291	
192.168.153.255	255.255.255.255	En vínculo	192.168.153.1	291	
192.168.203.0	255.255.255.0	En vínculo	192.168.203.1	291	
192.168.203.1	255.255.255.255	En vínculo	192.168.203.1	291	
192.168.203.255	255.255.255.255	En vínculo	192.168.203.1	291	
200.62.44.131	255.255.255.255	192.168.0.1	192.168.0.5	26	

Figura 47. Tabla de enrutamiento e interfaces

### 10.3.6 Escaneo con Nessus

Se realizaron pruebas sobre la herramienta Nessus con perfil avanzado múltiple con todas las opciones de escaneo sobre plataforma Windows 7 y Windows 10, a continuación, se muestra ejemplos de escaneo en cada rango, los activos identificados a los cuales se les realizaría escaneos y los datos de vulnerabilidades consolidados sobre una tabla de Excel.



Figura 48. Escaneo sobre Nessus rango .100

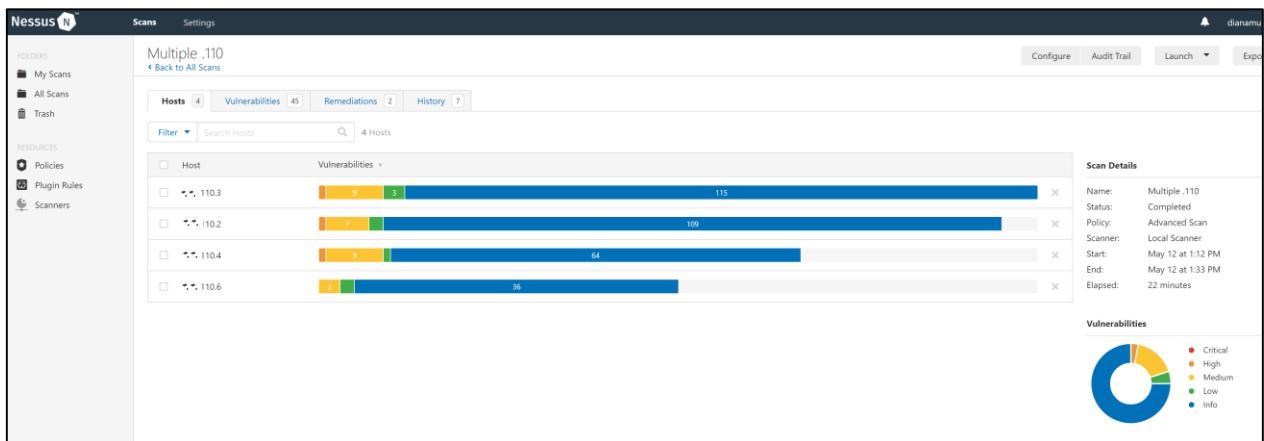


Figura 49. Escaneo sobre Nessus rango .100

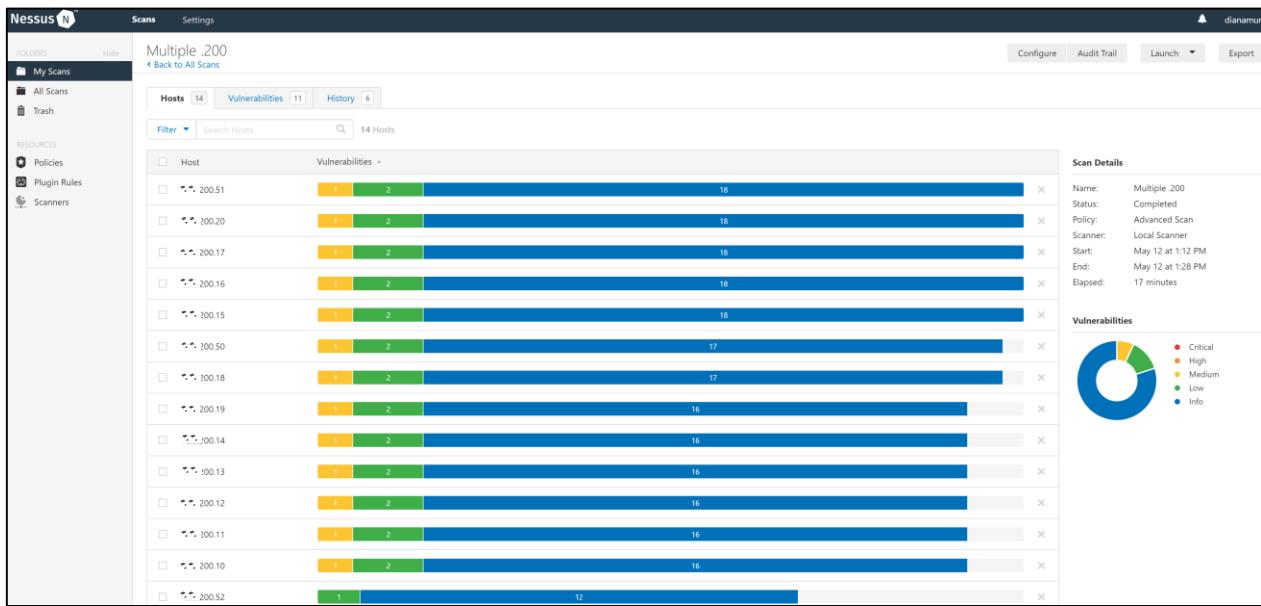


Figura 50. Escaneo sobre Nessus rango .100

Tabla 12. Inventario de Activos ( Anexo 17 - Inventario de activos)

Inventario y Evaluacion de Riesgos							
Activo	ID Activo	IP	Descripcion	Clasificacion			
				C	I	D	Valor Activo
Servidor	1	**.100.9	Caracteristicas no identificadas	4	3	5	5
Servidor	2	**.100.10	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	3	**.100.11	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	4	**.100.12	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	5	**.100.13	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	6	**.100.14	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	7	**.100.15	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	8	**.100.16	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	9	**.100.17	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	10	**.100.18	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	11	**.100.19	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	12	**.100.20	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	13	**.110.2	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	14	**.110.3	S.O:Linux Kernel 3.10 on CentOS Linux release 7 Servidor Apache /2,4,6(CentOS) OpenSSL /1,0,1e-fips PHP/5,4,16 Mozilla /4,0 SSH-2,0-OpenSSH_6,6,1 DNS:*,*,*.net;Digicert Inc SSL version: TLSv1,1,1,2 Servidores: SSH, Web.	5	5	5	15
Servidor	15	**.110.4	S.O:Windows Server 2016 Standard 14393 Netbios name:SRV-CTRLROOM-01 computer name:SRV-CTRLROOM-01; domain name=Workgroup SSL v3 Mozilla 4,0 DCERPC services:Lsaprc_endpoint,Lsa_eas_endpoint,ipsec.proxy manager client server endpoint,dhcpv6 client rpc service,base firerwall engine api, SMB v1,2	5	5	5	15
Servidor	16	**.110.6	S.O: Mozilla /4,0 Servidor Apache SSH 2,0;OpenSSH 7,4	5	5	5	15
Servidor	17	**.200.10	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	18	**.200.11	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	19	**.200.12	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	20	**.200.13	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	21	**.200.14	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	22	**.200.15	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	23	**.200.16	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	24	**.200.17	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	25	**.200.18	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	26	**.200.19	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	27	**.200.20	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	28	**.200.50	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	29	**.200.51	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15
Servidor	30	**.200.52	SSH v2,0 - OpenSSH 6,6,1	5	5	5	15

Tabla 13. Escaneos consolidados sobre Excel (Anexo 18 - Registro fase producción)

FECHA	RESPONSABLE	TOOL	DURACION	PERFILE ESCANEADO	IP	CРИТИЧНОСТЬ	КАНТОВ	ВУЛНЕРАБИЛІТІ	ПУРТО	SO
1/5/2019	CARLOS MCGOLLON	Nessus-W10	43	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	HTPP TRACE / TRACK Methods Allowed	443 / tcp / https	Linux Kernel 3
1/5/2019	CARLOS MCGOLLON	Nessus-W10	43	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSH Weak Algorithms Supported	22 / tcp / ssh	Linux Kernel 3
1/5/2019	CARLOS MCGOLLON	Nessus-W10	43	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSL Medium Strength Cipher Suites Supported (SWEET32)	443 / tcp / https	Linux Kernel 3
1/5/2019	CARLOS MCGOLLON	Nessus-W10	43	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
1/5/2019	CARLOS MCGOLLON	Nessus-W10	43	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
5/5/2019	DIANA BARERA	Nessus-W10	10	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	HTPP TRACE / TRACK Methods Allowed	443 / tcp / https	Linux Kernel 3
5/5/2019	DIANA BARERA	Nessus-W10	9	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSH Weak Algorithms Supported	22 / tcp / ssh	Linux Kernel 3
5/5/2019	DIANA BARERA	Nessus-W10	10	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSL Medium Strength Cipher Suites Supported (SWEET32)	443 / tcp / https	Linux Kernel 3
5/5/2019	DIANA BARERA	Nessus-W10	10	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
5/5/2019	DIANA BARERA	Nessus-W10	10	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
6/5/2019	CARLOS MCGOLLON	Nessus-W10	62	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	HTPP TRACE / TRACK Methods Allowed	443 / tcp / https	Linux Kernel 3
6/5/2019	CARLOS MCGOLLON	Nessus-W10	62	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSH Weak Algorithms Supported	22 / tcp / ssh	Linux Kernel 3
6/5/2019	CARLOS MCGOLLON	Nessus-W10	62	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSL Medium Strength Cipher Suites Supported (SWEET32)	443 / tcp / https	Linux Kernel 3
6/5/2019	CARLOS MCGOLLON	Nessus-W10	62	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
6/5/2019	CARLOS MCGOLLON	Nessus-W10	62	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
7/5/2019	DIANA MUNAR	Nessus-W10	9	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	HTPP TRACE / TRACK Methods Allowed	443 / tcp / https	Linux Kernel 3
7/5/2019	DIANA MUNAR	Nessus-W10	9	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSH Weak Algorithms Supported	22 / tcp / ssh	Linux Kernel 3
7/5/2019	DIANA MUNAR	Nessus-W10	9	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSL Medium Strength Cipher Suites Supported (SWEET32)	443 / tcp / https	Linux Kernel 3
7/5/2019	DIANA MUNAR	Nessus-W10	9	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
7/5/2019	DIANA MUNAR	Nessus-W10	9	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	HTPP TRACE / TRACK Methods Allowed	443 / tcp / https	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSH Weak Algorithms Supported	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSL Medium Strength Cipher Suites Supported (SWEET32)	443 / tcp / https	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
8/5/2019	DIANA BARERA	Nessus-W10	23	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	HTPP TRACE / TRACK Methods Allowed	443 / tcp / https	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSH Weak Algorithms Supported	22 / tcp / ssh	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSL Medium Strength Cipher Suites Supported (SWEET32)	443 / tcp / https	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	MEDIUM	1	SSL/TLS Protocol Initialization Vector Implementation Informa	8083 / tcp / www	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Server CBC Mode Ciphers Enabled	22 / tcp / ssh	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak MAC Algorithms Enabled	22 / tcp / ssh	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	HTPP TRACE / TRACK Methods Allowed	443 / tcp / https	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSL Medium Strength Cipher Suites Supported (SWEET32)	443 / tcp / https	Linux Kernel 3
12/5/2019	DIANA MUNAR	Nessus-W10	52	SCAN AVANZADO MÚLTIPLE	*.*.100.10	LOW	1	SSH Weak Algorithms Supported	22 / tcp / ssh	Linux Kernel 3

### **10.3.7 Pruebas manuales**

Posterior a las pruebas de escaneo con herramientas, de acuerdo a los resultados obtenidos en cuanto a puertos e información encontradas, se inician algunas pruebas manuales para verificar que los registros generados son ciertos y no falsos positivos.

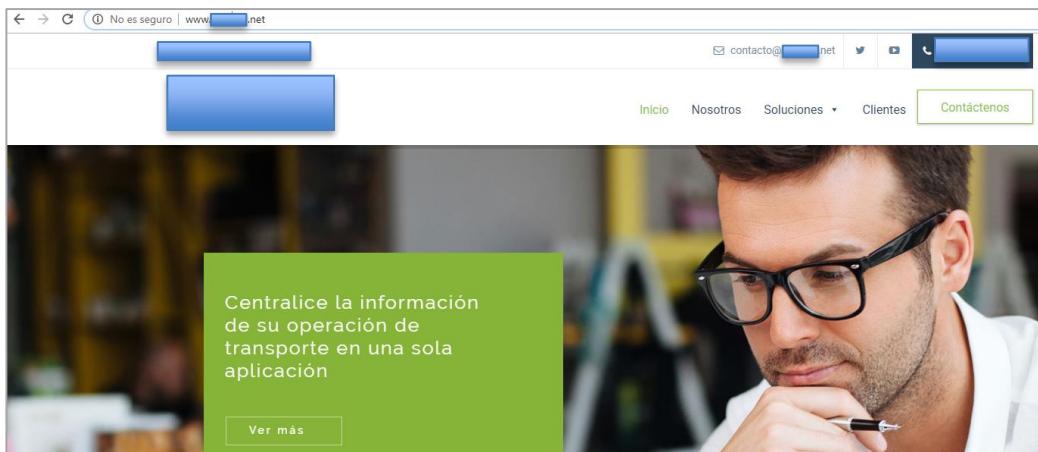


Figura 51. Prueba manual – Ingreso a Intranet de la empresa

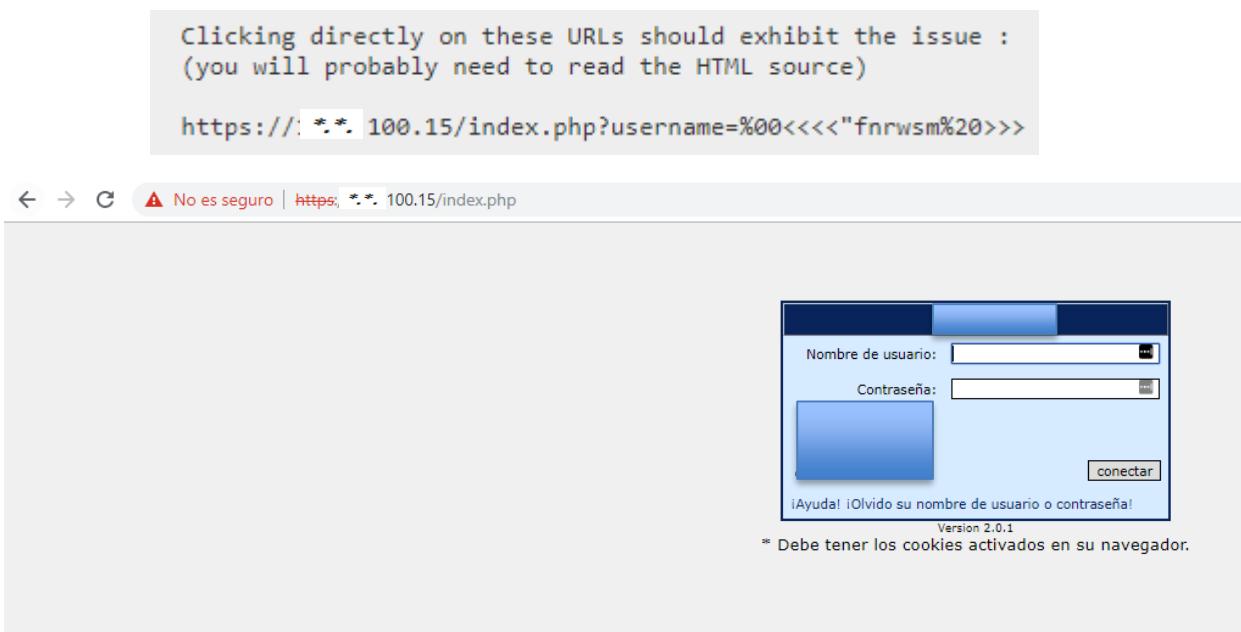


Figura 52. Prueba manual - Plugin 49067

The screenshot shows the "Plugin Output" section of the Nessus interface. It has a header "Plugin Output" and a sub-header "tcp/443". Below this, a message states "Nessus was able to verify the issue using the following URL :" followed by a URL: "https:// \*.\* 100.15/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000".

```
Plugin Output
tcp/443

Nessus was able to verify the issue using the following URL :

https:// *.* 100.15/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

Figura 53. Prueba manual - Plugin 46803

  No es seguro   <a href="https://100.15/index.php?_=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">https://100.15/index.php?_=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000</a>																																							
<b>PHP Credits</b>																																							
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #a0a0ff;">PHP Group</th><th></th></tr> </thead> <tbody> <tr> <td style="background-color: #e0e0ff;">Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski</td><td></td></tr> </tbody> </table>		PHP Group		Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski																																			
PHP Group																																							
Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski																																							
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #a0a0ff;">Language Design &amp; Concept</th><th></th></tr> </thead> <tbody> <tr> <td style="background-color: #e0e0ff;">Andi Gutmans, Rasmus Lerdorf, Zeev Suraski</td><td></td></tr> </tbody> </table>		Language Design & Concept		Andi Gutmans, Rasmus Lerdorf, Zeev Suraski																																			
Language Design & Concept																																							
Andi Gutmans, Rasmus Lerdorf, Zeev Suraski																																							
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="background-color: #a0a0ff;">PHP 4 Authors</th></tr> <tr> <th style="background-color: #a0a0ff;">Contribution</th><th style="background-color: #a0a0ff;">Authors</th></tr> </thead> <tbody> <tr> <td style="background-color: #e0e0ff;">Zend Scripting Language Engine</td><td style="background-color: #e0e0ff;">Andi Gutmans, Zeev Suraski</td></tr> <tr> <td style="background-color: #e0e0ff;">Extension Module API</td><td style="background-color: #e0e0ff;">Andi Gutmans, Zeev Suraski, Andrei Zmievski</td></tr> <tr> <td style="background-color: #e0e0ff;">UNIX Build and Modularization</td><td style="background-color: #e0e0ff;">Stig Bakken, Sascha Schumann</td></tr> <tr> <td style="background-color: #e0e0ff;">Win32 Port</td><td style="background-color: #e0e0ff;">Shane Caraveo, Zeev Suraski</td></tr> <tr> <td style="background-color: #e0e0ff;">Server API (SAPI) Abstraction Layer</td><td style="background-color: #e0e0ff;">Andi Gutmans, Shane Caraveo, Zeev Suraski</td></tr> <tr> <td style="background-color: #e0e0ff;">Streams Abstraction Layer</td><td style="background-color: #e0e0ff;">Wez Furlong</td></tr> </tbody> </table>		PHP 4 Authors		Contribution	Authors	Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski	Extension Module API	Andi Gutmans, Zeev Suraski, Andrei Zmievski	UNIX Build and Modularization	Stig Bakken, Sascha Schumann	Win32 Port	Shane Caraveo, Zeev Suraski	Server API (SAPI) Abstraction Layer	Andi Gutmans, Shane Caraveo, Zeev Suraski	Streams Abstraction Layer	Wez Furlong																						
PHP 4 Authors																																							
Contribution	Authors																																						
Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski																																						
Extension Module API	Andi Gutmans, Zeev Suraski, Andrei Zmievski																																						
UNIX Build and Modularization	Stig Bakken, Sascha Schumann																																						
Win32 Port	Shane Caraveo, Zeev Suraski																																						
Server API (SAPI) Abstraction Layer	Andi Gutmans, Shane Caraveo, Zeev Suraski																																						
Streams Abstraction Layer	Wez Furlong																																						
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="background-color: #a0a0ff;">SAPI Modules</th></tr> <tr> <th style="background-color: #a0a0ff;">Contribution</th><th style="background-color: #a0a0ff;">Authors</th></tr> </thead> <tbody> <tr> <td style="background-color: #e0e0ff;">ActiveScript</td><td style="background-color: #e0e0ff;">Wez Furlong</td></tr> <tr> <td style="background-color: #e0e0ff;">AOLserver</td><td style="background-color: #e0e0ff;">Sascha Schumann</td></tr> <tr> <td style="background-color: #e0e0ff;">Apache 1.3</td><td style="background-color: #e0e0ff;">Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar</td></tr> <tr> <td style="background-color: #e0e0ff;">Apache 2.0 Handler</td><td style="background-color: #e0e0ff;">Ian Holsman, Justin Erenkrantz (based on Apache 2.0 Filter code)</td></tr> <tr> <td style="background-color: #e0e0ff;">Apache 2.0</td><td style="background-color: #e0e0ff;">Sascha Schumann, Aaron Barnert</td></tr> <tr> <td style="background-color: #e0e0ff;">Caudium / Roxen</td><td style="background-color: #e0e0ff;">David Hedbor</td></tr> <tr> <td style="background-color: #e0e0ff;">CGI / FastCGI</td><td style="background-color: #e0e0ff;">Rasmus Lerdorf, Stig Bakken, Shane Caraveo</td></tr> <tr> <td style="background-color: #e0e0ff;">CLI</td><td style="background-color: #e0e0ff;">Edin Kadribasic, Marcus Boerger</td></tr> <tr> <td style="background-color: #e0e0ff;">Embed</td><td style="background-color: #e0e0ff;">Edin Kadribasic</td></tr> <tr> <td style="background-color: #e0e0ff;">ISAPI</td><td style="background-color: #e0e0ff;">Andi Gutmans, Zeev Suraski</td></tr> <tr> <td style="background-color: #e0e0ff;">Java Servlet</td><td style="background-color: #e0e0ff;">Sam Ruby</td></tr> <tr> <td style="background-color: #e0e0ff;">NSAPI</td><td style="background-color: #e0e0ff;">Jayakumar Muthukumarasamy, Uwe Schindler</td></tr> <tr> <td style="background-color: #e0e0ff;">phttpd</td><td style="background-color: #e0e0ff;">Thies C. Arntzen</td></tr> <tr> <td style="background-color: #e0e0ff;">pi3web</td><td style="background-color: #e0e0ff;">Holger Zimmermann</td></tr> <tr> <td style="background-color: #e0e0ff;">thttpd</td><td style="background-color: #e0e0ff;">Sascha Schumann</td></tr> <tr> <td style="background-color: #e0e0ff;">tux</td><td style="background-color: #e0e0ff;">Sascha Schumann</td></tr> <tr> <td style="background-color: #e0e0ff;">WebJames</td><td style="background-color: #e0e0ff;">Alex Waugh</td></tr> </tbody> </table>		SAPI Modules		Contribution	Authors	ActiveScript	Wez Furlong	AOLserver	Sascha Schumann	Apache 1.3	Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar	Apache 2.0 Handler	Ian Holsman, Justin Erenkrantz (based on Apache 2.0 Filter code)	Apache 2.0	Sascha Schumann, Aaron Barnert	Caudium / Roxen	David Hedbor	CGI / FastCGI	Rasmus Lerdorf, Stig Bakken, Shane Caraveo	CLI	Edin Kadribasic, Marcus Boerger	Embed	Edin Kadribasic	ISAPI	Andi Gutmans, Zeev Suraski	Java Servlet	Sam Ruby	NSAPI	Jayakumar Muthukumarasamy, Uwe Schindler	phttpd	Thies C. Arntzen	pi3web	Holger Zimmermann	thttpd	Sascha Schumann	tux	Sascha Schumann	WebJames	Alex Waugh
SAPI Modules																																							
Contribution	Authors																																						
ActiveScript	Wez Furlong																																						
AOLserver	Sascha Schumann																																						
Apache 1.3	Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar																																						
Apache 2.0 Handler	Ian Holsman, Justin Erenkrantz (based on Apache 2.0 Filter code)																																						
Apache 2.0	Sascha Schumann, Aaron Barnert																																						
Caudium / Roxen	David Hedbor																																						
CGI / FastCGI	Rasmus Lerdorf, Stig Bakken, Shane Caraveo																																						
CLI	Edin Kadribasic, Marcus Boerger																																						
Embed	Edin Kadribasic																																						
ISAPI	Andi Gutmans, Zeev Suraski																																						
Java Servlet	Sam Ruby																																						
NSAPI	Jayakumar Muthukumarasamy, Uwe Schindler																																						
phttpd	Thies C. Arntzen																																						
pi3web	Holger Zimmermann																																						
thttpd	Sascha Schumann																																						
tux	Sascha Schumann																																						
WebJames	Alex Waugh																																						
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="background-color: #a0a0ff;">Module Authors</th></tr> <tr> <th style="background-color: #a0a0ff;">Module</th><th style="background-color: #a0a0ff;">Authors</th></tr> </thead> <tbody> <tr> <td style="background-color: #e0e0ff;">Assert</td><td style="background-color: #e0e0ff;">Thies C. Arntzen</td></tr> <tr> <td style="background-color: #e0e0ff;">BC Math</td><td style="background-color: #e0e0ff;">Andi Gutmans</td></tr> <tr> <td style="background-color: #e0e0ff;">Bzip2</td><td style="background-color: #e0e0ff;">Sterling Hughes</td></tr> <tr> <td style="background-color: #e0e0ff;">Calendar</td><td style="background-color: #e0e0ff;">Shane Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong</td></tr> <tr> <td style="background-color: #e0e0ff;">cpdf</td><td style="background-color: #e0e0ff;">Uwe Steinmann</td></tr> </tbody> </table>		Module Authors		Module	Authors	Assert	Thies C. Arntzen	BC Math	Andi Gutmans	Bzip2	Sterling Hughes	Calendar	Shane Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong	cpdf	Uwe Steinmann																								
Module Authors																																							
Module	Authors																																						
Assert	Thies C. Arntzen																																						
BC Math	Andi Gutmans																																						
Bzip2	Sterling Hughes																																						
Calendar	Shane Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong																																						
cpdf	Uwe Steinmann																																						

Figura 54. Prueba manual - Puerto 443 Index

crack	Alexander Feldman
ctype	Hartmut Holzgraefe
CURL	Sterling Hughes
Cyrus	Sterling Hughes
DBA	Sascha Schumann, Marcus Boerger
dBBase	Jim Winstead
DBM	Rasmus Lerdorf, Jim Winstead
dbx (database abstraction)	Marc Boeren, Rui Hirokawa, Frank M. Kromann
domxml	Uwe Steinmann, Christian Stocker
dotnet	Sam Ruby
EXIF	Rasmus Lerdorf, Marcus Boerger
FBSQL	Frank M. Kromann
FDF	Uwe Steinmann
FilePro	Chad Robinson
FriBidi	Omri Ben-Zvi, Tal Peer
FTP	Stefan Esser, Andrew Skalski
GD imaging	Rasmus Lerdorf, Stig Bakken, Jim Winstead, Jouni Ahto, Ilya Alshanetsky, Pierre-Alain Joye
GetText	Alex Plotnick
GNU GMP support	Stanislav Malyshev
HwAPI	Uwe Steinmann
HyperWave	Uwe Steinmann
IMAP	Ren Logan, Mark Musone, Brian Wang, Kaj-Michael Lang, Antoni Pamies Olive, Rasmus Lerdorf, Andrew Skalski, Chuck Hagenbuch, Daniel R Kalowsky
Informix	Danny Heijl, Christian Cartus, Come' Cornelius
Ingres II	David Hénot
InterBase	Jouni Ahto, Andrew Avdeev, Ard Biesheuvel
IRCg	Sascha Schumann
Java	Sam Ruby
LDAP	Amritay Isaacs, Eric Warneke, Rasmus Lerdorf, Gerrit Thomson, Stig Venaas
MCAL	Mark Musone, Chuck Hagenbuch
mcrypt	Sascha Schumann, Derick Rethans
MCVE	Brad House, Chris Faulhaber, Steven Schoch
mhash	Sascha Schumann
mime_magic	Hartmut Holzgraefe
MING	Dave Hayden, Frank M. Kromann
mnoGoSearch	Sergey Kartashoff, Alex Barkov, Ramil Kalimullin
MS SQL	Frank M. Kromann
msession	Mark L. Woodward
mSQL	Zeev Suraski
Multibyte String Functions	Tsukada Takuya, Rui Hirokawa
MySQL	Zeev Suraski, Zak Greant, Georg Richter
ncurses	Ilya Alshanetsky, Wez Furlong, Hartmut Holzgraefe, Georg Richter
OC18	Stig Bakken, Thies C. Arntzen, Andy Saulins, David Benson, Maxim Maletsky
ODBC	IStig Bakken, Andreas Karajannis, Frank M. Kromann, Daniel R. Kalowsky
OpenSSL	Stig Venaas, Wez Furlong, Sascha Kettler
Oracle	Stig Bakken, Mitch Golden, Rasmus Lerdorf, Andreas Karajannis, Thies C. Arntzen
Ovrimos	Nikos Mavroyanopoulos
pcntl	Jason Greene
PDF	Uwe Steinmann, Rainer Schaaf
Perl Compatible Regexps	Andrei Zmievski
Posix	Kristian Köhntopp
PostgreSQL	Jouni Ahto, Zeev Suraski, Yasuo Ohgaki
Pspell	Vlad Krupin
qtdom	Jan Borsodi
Readline	Thies C. Arntzen
Recode	Kristian Köhntopp
Sessions	Sascha Schumann, Andrei Zmievski
Shared Memory Operations	Slava Poliakov, Ilya Alshanetsky
SNMP	Rasmus Lerdorf, Harrie Hazewinkel, Mike Jackson, Steven Lawrence, Johann Hanne
Sockets	Chris Vandomelein, Sterling Hughes, Daniel Beulshausen, Jason Greene
SWF	Sterling Hughes
Sybase-CT	Zeev Suraski, Tom May, Timm Friebe
Sybase-DB	Zeev Suraski
System V Message based IPC	Wez Furlong
System V Semaphores	Tom May
System V Shared Memory	Christian Cartus
tokenizer	Andrei Zmievski
User-space object overloading	Andrei Zmievski
Verisign Payflow Pro	John Donagher, David Croft
W32API	James Moore
WDDX	Andrei Zmievski
Win32 COM	Alan Brown, Wez Furlong, Harald Radi, Zeev Suraski
XML	Stig Bakken, Thies C. Arntzen
xmiprc	Dan Libby
YAZ	Adam Dickmeiss
Yellow Pages	Stephanie Wehner, Fredrik Ohm
Zip	Sterling Hughes
Zlib	Rasmus Lerdorf, Stefan Roehrich, Zeev Suraski, Jade Nicoletti

PHP Documentation	
Authors	Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Philip Olson, Georg Richter, Damien Seguy, Jakub Vrana
Editor	Philip Olson
User Note Maintainers	Mehdi Achour, Friedhelm Betz, Vincent Gevers, Aidan Lister, Nuno Lopes, Tom Sommer
Other Contributors	Previously active authors, editors and other contributors are listed in the manual.

PHP 4.4 Quality Assurance Team	
Ilia Alshanetsky, Stefan Esser, Moriyoshi Koizumi, Sebastian Nohn, Derick Rethans, Melvyn Sopacua, Jani Taskinen	

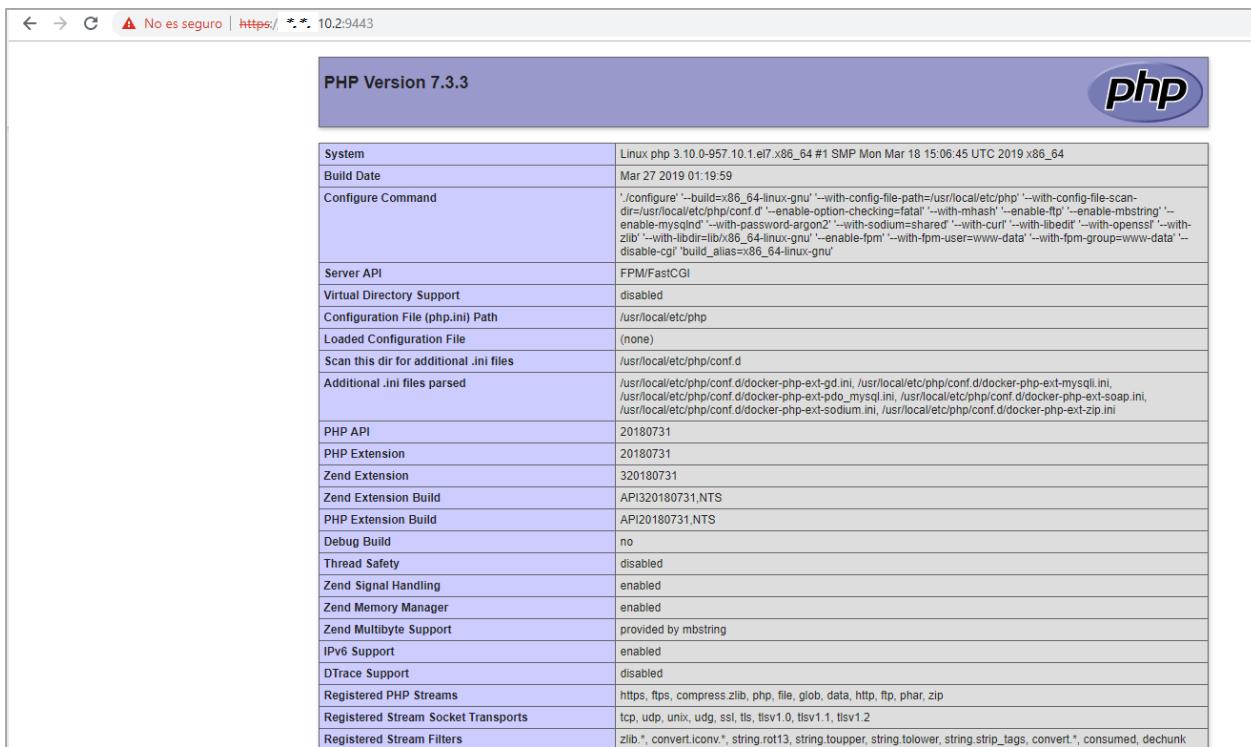
  

PHP Website Team	
Hannes Magnusson, Colin Viebrock, Jim Winstead	

Figura 55. Prueba manual - Puerto 443 Index



Figura 56. Prueba manual - Plugin 106375



PHP Version 7.3.3	
System	Linux php 3.10.0-957.10.1.el7.x86_64 #1 SMP Mon Mar 18 15:06:45 UTC 2019 x86_64
Build Date	Mar 27 2019 01:19:59
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-mbstring' '--enable-mysqnd' '--with-password-argon2' '--with-sodium=shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=/lib/x86_64-linux-gnu' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini, /usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-soap.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini, /usr/local/etc/php/conf.d/docker-php-ext-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress_zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

Figura 57. Prueba manual - Puerto 9080 pasa a 9443

Configuration		
cgi-fcgi		
php-fpm	active	
Directive	Local Value	Master Value
cgi.discard_path	0	0
cgi.fix_pathinfo	1	1
cgi.force_redirect	1	1
cgi.nph	0	0
cgi.redirect_status_env	no value	no value
cgi.rfc2616_headers	0	0
fastcgi.error_header	no value	no value
fastcgi.logging	1	1
fpm.config	no value	no value

Core		
PHP Version		
Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	no value	no value
display_errors	On	On
display_startup_errors	Off	Off
doc_root	no value	no value
dooref_ext	no value	no value
dooref_root	no value	no value
enable_dl	On	On
enable_post_data_reading	On	On
error_append_string	no value	no value
error_log	no value	no value
error_prepend_string	no value	no value

Figura 58. Prueba manual - Puerto 9080 pasa a 9443

curl.cainfo		
	no value	no value

date		
date/time support	enabled	
timelib version	2018.01RC3	
"Olson" Timezone Database Version	2018.9	
Timezone Database	internal	
Default timezone	UTC	

Directive	Local Value	Master Value
date.default_latitude	31.7867	31.7867
date.default_longitude	35.2333	35.2333
date.sunrise_zenith	90.583333	90.583333
date.sunset_zenith	90.583333	90.583333
date.timezone	no value	no value

dom		
DOM/XML	enabled	
DOM/XML API Version	20031129	
libxml Version	2.9.4	
HTML Support	enabled	
XPath Support	enabled	
XPointer Support	enabled	
Schema Support	enabled	
RelaxNG Support	enabled	

fileinfo		
fileinfo support	enabled	
libmagic	533	

filter		
Input Validation and Filtering	enabled	
Directive	Local Value	Master Value
filter.default	unsafe_raw	unsafe_raw
filter.default_flags	no value	no value

Figura 59. Prueba manual - Puerto 9080 pasa a 9443



Figura 60. Prueba manual – Plugin 106375

PHP Version 7.3.4

System	Linux php 3.10.0-862.6.3.el7.x86_64 #1 SMP Tue Jun 26 16:32:21 UTC 2018 x86_64
Build Date	Apr 6 2019 02:32:35
Configure Command	'/configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqli' '--with-password-argon2' '--with-sodium-shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=/lib/x86_64-linux-gnu' '--enable-fpm' '--with-fpm-user=www-data' '--with-fpm-group=www-data' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini, /usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-soap.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini, /usr/local/etc/php/conf.d/docker-php-ext-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, convert.iconv*, string.rot13, string.toupper, string.toLowerCase, string.strip_tags, convert.*, consumed, dechunk

Figura 61. Prueba manual – Puerto 9943

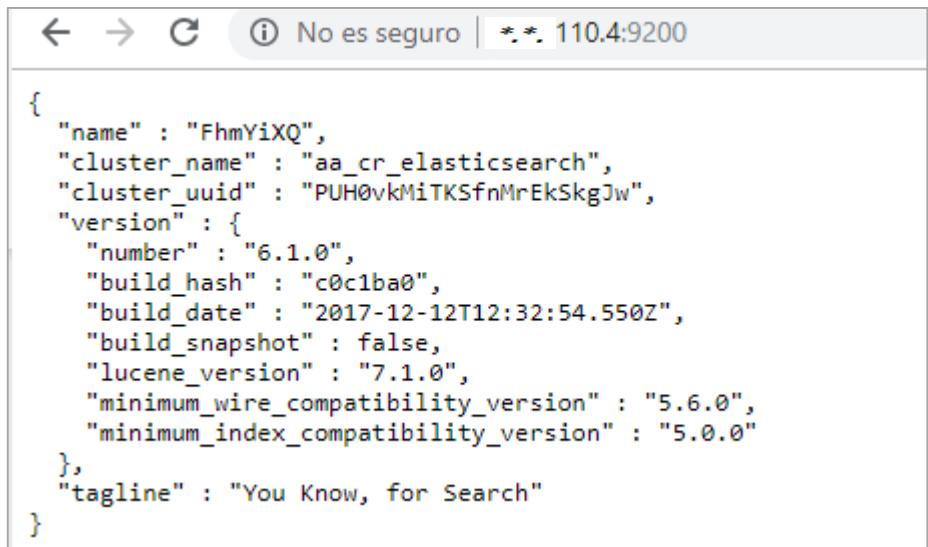
Plugin Output

tcp/9200

```
URL : http:// *.*.110.4:9200/
Installed version : 6.1.0
Fixed version : 6.4.1
```

Figura 62. Plugin 117665

threat	[threat] Lexmark printers open both TCP and UDP port 9200 for some unknown purpose.
--------	---

```
{  
  "name" : "FhmYiXQ",  
  "cluster_name" : "aa_cr_elasticsearch",  
  "cluster_uuid" : "PUH0vkMiTKSfnMrEkSkgJw",  
  "version" : {  
    "number" : "6.1.0",  
    "build_hash" : "c0c1ba0",  
    "build_date" : "2017-12-12T12:32:54.550Z",  
    "build_snapshot" : false,  
    "lucene_version" : "7.1.0",  
    "minimum_wire_compatibility_version" : "5.6.0",  
    "minimum_index_compatibility_version" : "5.0.0"  
  },  
  "tagline" : "You Know, for Search"  
}
```

Figura 63. Plugin 117665 – Puerto 9200

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

- https:// \*.\*. 100.15/
- https:// \*.\*. 100.15/index.php
- https:// \*.\*. 100.15/install/

Figura 64. Plugin 85582

<https://100.15/install/>

**dotProject Installer**

Welcome to the dotProject Installer! It will setup the database for dotProject and create an appropriate config file. In some cases a manual installation cannot be avoided.

**There is an initial Check for (minimal) Requirements appended down below for troubleshooting. At least a database connection must be available and ..../includes/config.php must be writable for the webserver!**

**It would appear that you already have a dotProject installation. The installer will attempt to upgrade your system, however it is a good idea to take a full backup first!**

[Start Upgrade](#)

**Check for Requirements**

- PHP Version >= 4.1 ✓ (4.4.9)
- Server API ✓ (apache2handler)
- GD Support (for GANTT Charts) ✓
- Zip compression Support ✓
- File Uploads ✓ (Max File Upload Size: 8M)
- Session Save Path writable? ✓ (/tmp)

**Database Connectors**

The next tests check for database support compiled with php. We use the ADOdb database abstraction layer which comes with drivers for many databases. Consult the ADOdb documentation for details.

For the moment only MySQL is fully supported, so you need to make sure it is available.

- iBase Support ✗ Not available
- Informix Support ✗ Not available
- LDAP Support ✗ Not available
- mSQL Support ✗ Not available
- MSSQL Server Support ✗ Not available
- MySQL Support ✓ (MySQL)
- ODBC Support ✗ Not available
- Oracle Support ✗ Not available
- PostgreSQL Support ✗ Not available
- SQLite Support ✗ Not available
- Sybase Support ✗ Not available

**Check for Directory and File Permissions**

If the message 'World Writable' appears after a file/directory, then Permissions for this File have been set to allow all users to write to this file/directory. Consider changing this to a more restrictive setting to improve security. You will need to do this manually.

- /includes/config.php writable? ✗ Configuration process can still be continued. Configuration file will be displayed at the end, just copy & paste this and upload.
- /files/writable? ✓
- /files/temp/writable? ✗ PDF report generation will be disabled
- /locales/en/writable? ✗ Translation files cannot be saved. Check /locales and subdirectories for permissions.

**Recommended PHP Settings**

- Safe Mode = OFF? ✓
- Register Globals = OFF? ✗ There are security risks with this turned ON
- Session AutoStart = ON? ✗ Try setting to ON if you are experiencing a WhiteScreenOfDeath
- Session Use Cookies = ON? ✓
- Session Use Trans Sid = OFF? ✓

**Other Recommendations**

The dotProject team openly recommend Free Open Source software (FOSS). This is not just because dotProject is a FOSS application, but because we believe that the FOSS development method results in better software, with a lower Total Cost of Ownership (TCO).

These recommendations reflect that belief, and the fact that as FOSS developers, we develop on FOSS systems, so they will have better support sooner than other non-FOSS systems.

- Free Operating System? ✓ (Linux: Interno 3.10.0-327.36.1.el7.x86\_64 #1 SMP Sun Sep 18 13:04:29 UTC 2016 x86\_64)
- Supported Web Server? ✓ (Apache)
- Standards Compliant Browser? ✓ (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36)

Figura 65. Prueba manual - Pluggin 85582 - \*.\*.100.15/install/



Figura 66. Prueba manual – Puerto 8083

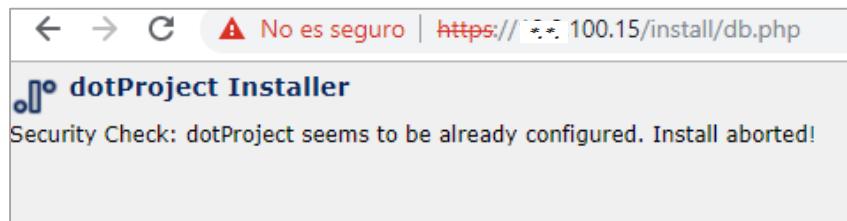


Figura 67. Prueba manual - Plugin10662

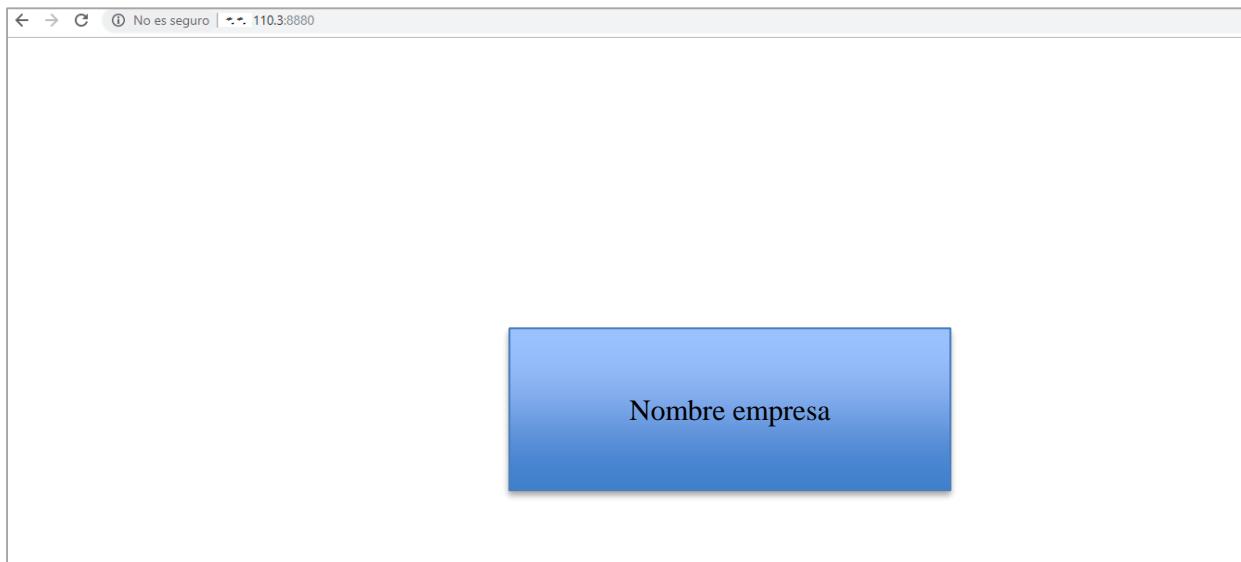


Figura 68. Plugin 12479

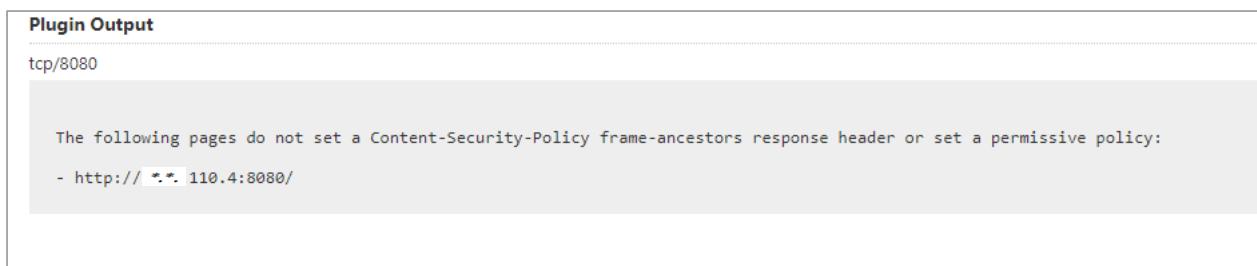


Figura 69. Plugin 50344

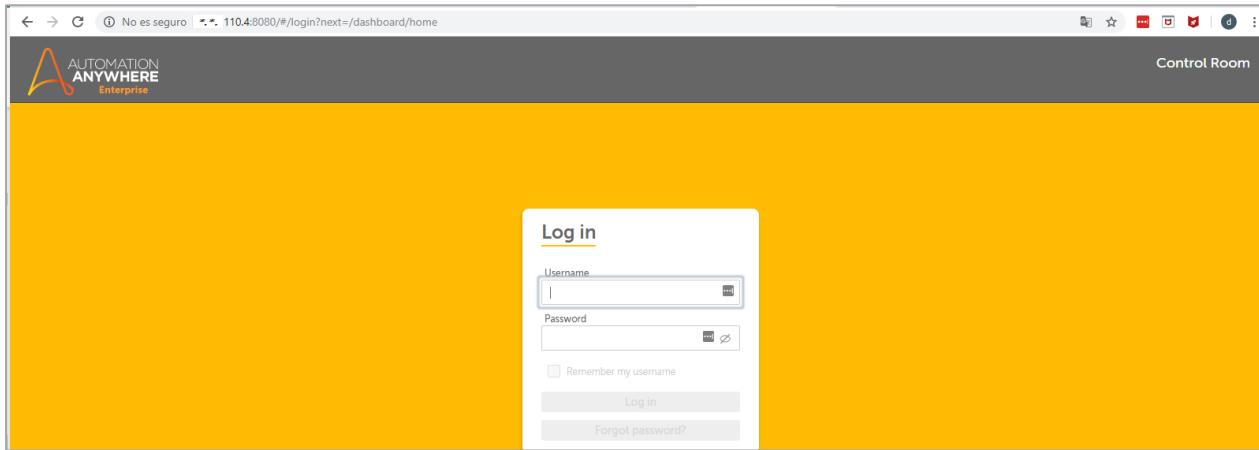


Figura 70. Plugin 50344 Puerto 8080

## 11. Resultados

Gracias a la metodología adoptada relacionando los pasos a seguir para el análisis y obtención de resultados esperados se ha culminado con éxito las expectativas que se tenían al inicio del proyecto en cuanto a lograr obtener los diferentes tipos de aplicaciones, encontrar los niveles de parches que requieren los sistemas y aplicaciones, así como el listado de las vulnerabilidades y la familia a la que corresponden.

La finalidad de las pruebas de escaneos realizados es poder brindarle a la empresa la facilidad de elegir entre las diferentes acciones o herramientas que puede utilizar para aseguramiento de la misma, con el fin de garantizar los resultados obtenidos de los escaneos realizados y basados en la metodología, se realizaron algunas simulaciones de acceso a los Plugins débiles encontrados para verificar que no haya sido un falso positivo, se creó una matriz de riesgo (Anexo 2 – Matriz de Riesgo) para analizar y evaluar el riesgo, determinar el impacto sobre sistemas y operación del negocio, y así priorizar de acuerdo a la criticidad, impacto y probabilidad de una posible explotación de la vulnerabilidad encontrada, adicional se consolidó la información de escaneos sobre las herramientas Nmap y Nessus con la finalidad de detectar el servidor más vulnerable o en su defecto los puertos abiertos que deben revisarse en cada uno de los servidores para evitar ser vulnerable a ataques.

A continuación, se presentan unas gráficas de consolidación de información obtenida en las herramientas de escaneo, generando una analítica para exponer los datos encontrados y así evidenciar mejoras que requieran los sistemas o las aplicaciones de acuerdo a las vulnerabilidades encontradas en cada servidor ( Anexo 20 - Graficas resultados).

## 11.1 Criticidad de vulnerabilidades

El siguiente gráfico muestra el número de vulnerabilidades documentadas encontradas al largo de los escaneos en los servidores en la fase de producción sobre herramienta Nessus y Nmap, de acuerdo a la criticidad, se registran 37 vulnerabilidades en todos los servidores con mayor resultado vulnerabilidades tipo “Medium” de acuerdo a la criticidad.

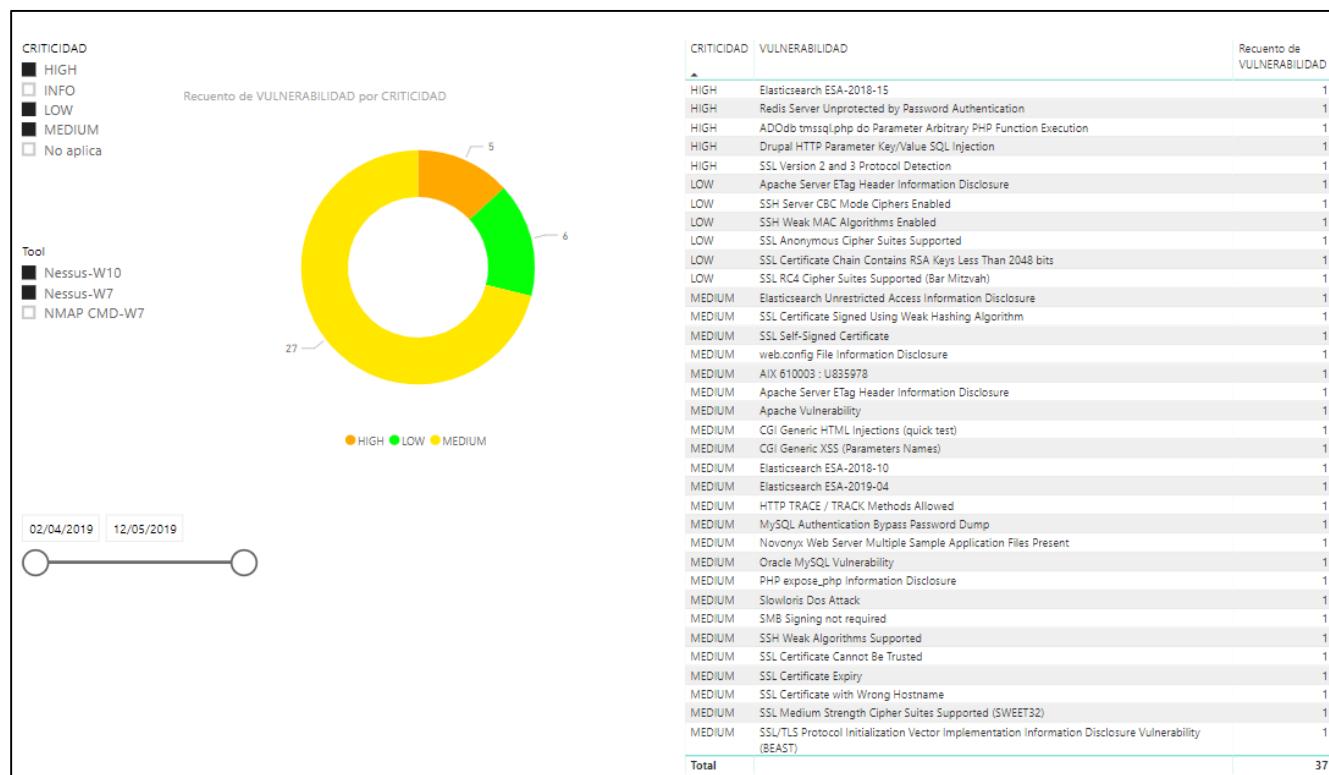


Figura 71. Vulnerabilidades detectadas

## 11.2 Vulnerabilidades de acuerdo a criticidad

En la siguiente gráfica se muestra la cantidad de vulnerabilidades encontradas en los escaneos de acuerdo a la criticidad (High - medium – low), se resalta que la cantidad de vulnerabilidades encontradas son: 5 en criticidad alta, 27 en criticidad Medium y 6 en criticidad medio donde la Vulnerabilidad Apache Server eTag Header se repite en criticidad alta para unos servidores y criticidad media para otros.

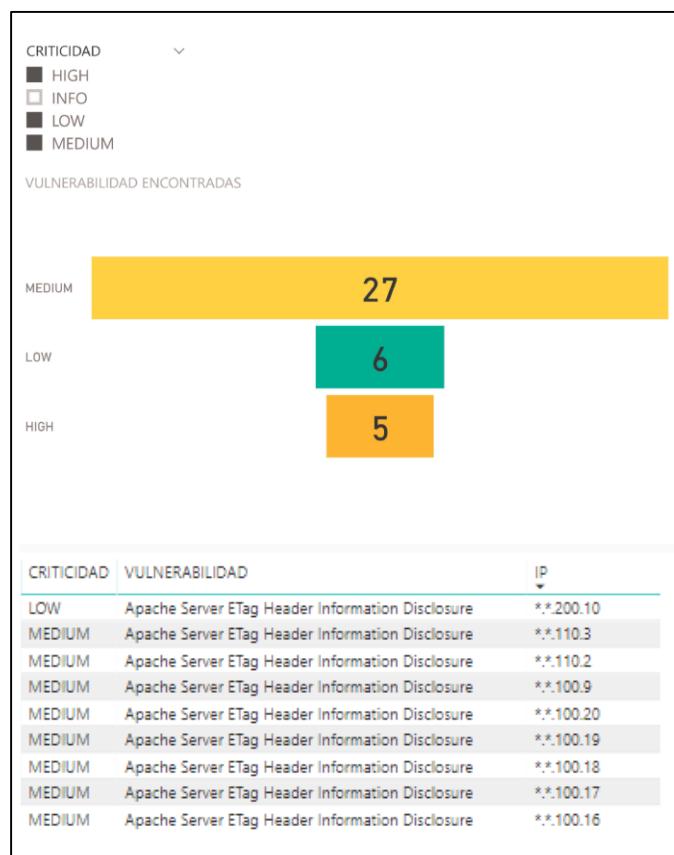


Figura 72. Vulnerabilidades por criticidad

## 11.2 Vulnerabilidades en cada servidor

En la siguiente gráfica se muestra la cantidad de vulnerabilidades encontradas en cada servidor, el cual en primer lugar está el servidor \*.\*.100.15 que registra 16 vulnerabilidades encontradas, seguido por el servidor con IP \*.\*.110.4 el cual también registra 16 vulnerabilidades encontradas durante todas las pruebas y escaneos realizados correspondiente a vulnerabilidades tipo SSL.

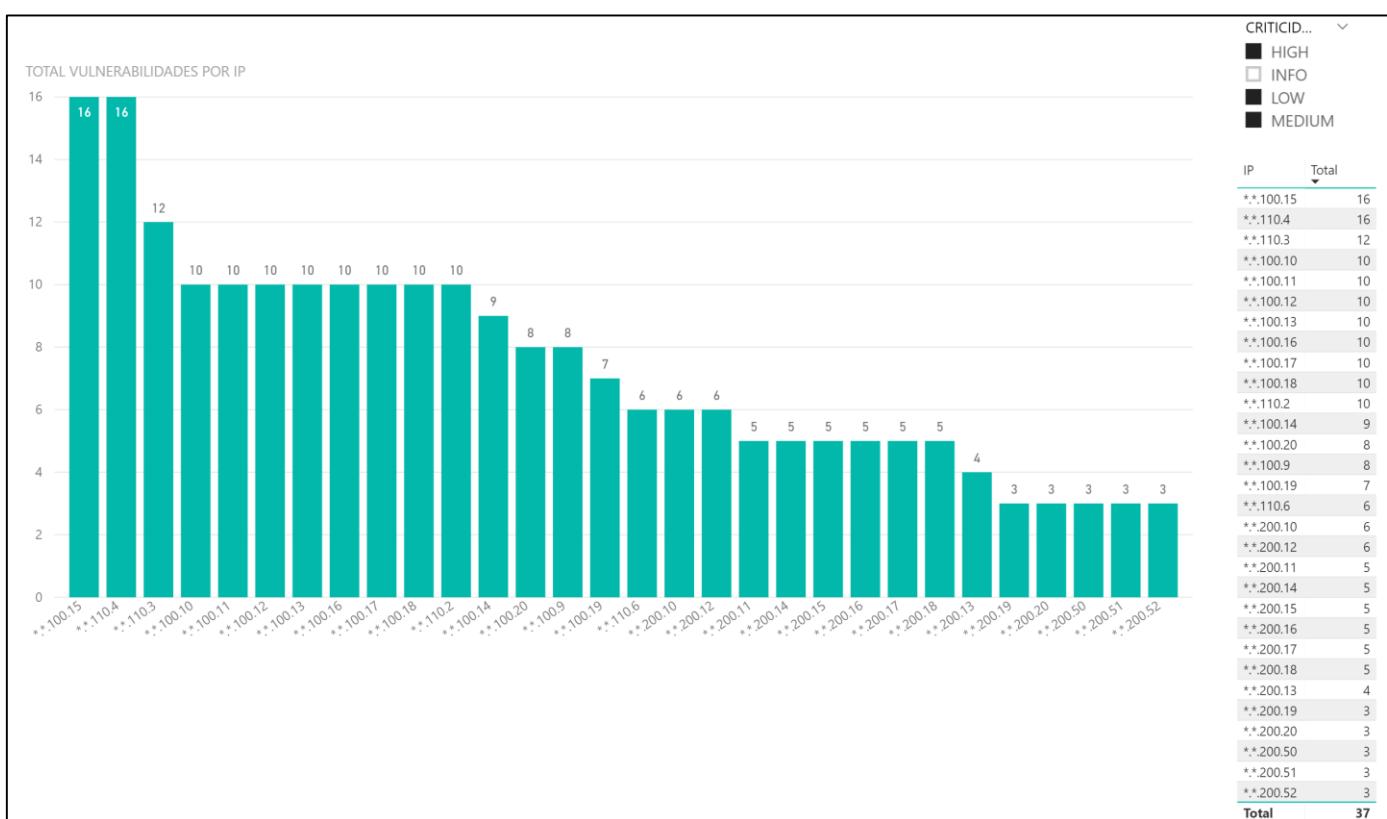


Figura 73. Vulnerabilidades en servidores

### 11.3 Vulnerabilidades en servidor por criticidad

En la siguiente gráfica se muestra la cantidad de vulnerabilidades encontradas por criticidad en cada servidor durante el periodo de escaneo en la fase de producción, estando en primer lugar como más vulnerable el servidor \*.\*.100.15 con un total de 16 vulnerabilidades detalladas 1 tipo alta, 13 media y 2 bajas el cual según registros y escaneos tiene sistema Sistema Operativo Linux CentOS, seguido por el servidor con IP \*.\*.110.4 que también registra 16 vulnerabilidades en total, registradas 2 tipo alta, 12 tipo media y 2 bajas, el cual cuenta con Sistema Operativo Windows Server 2016.

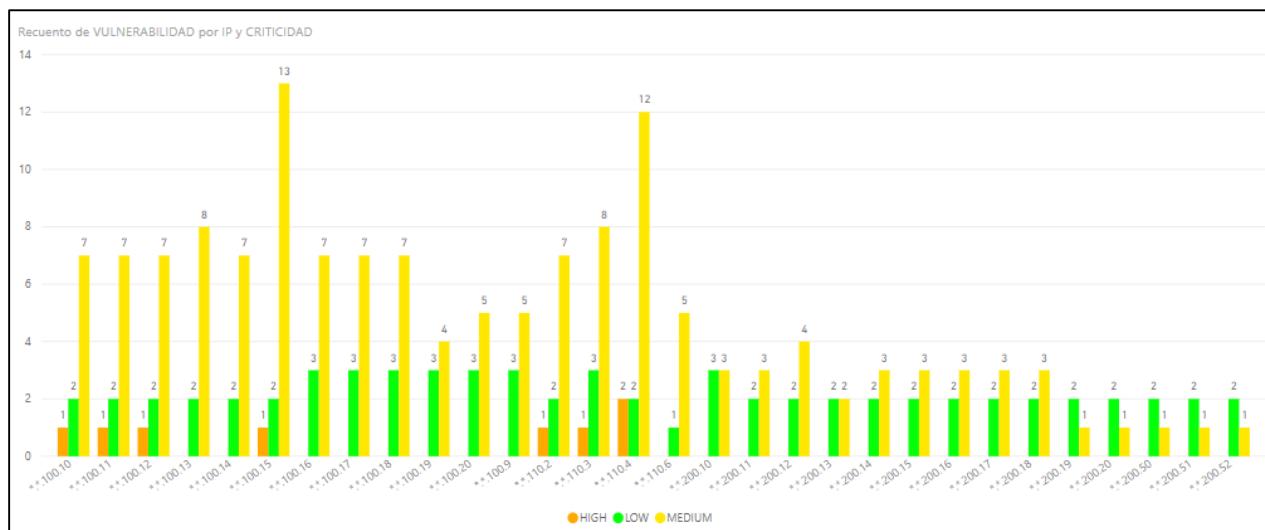


Figura 74. Vulnerabilidades en servidores por criticidad

## 11.4 Vulnerabilidades según la familia

La siguiente gráfica muestra las vulnerabilidades encontradas de acuerdo a la familia correspondiente, con el porcentaje de participación de acuerdo a la cantidad de vulnerabilidades escaneadas durante la fase de producción, presentado en primer lugar la familia "General" que corresponde a vulnerabilidades tipo SSL por Certificados o auto firmas.

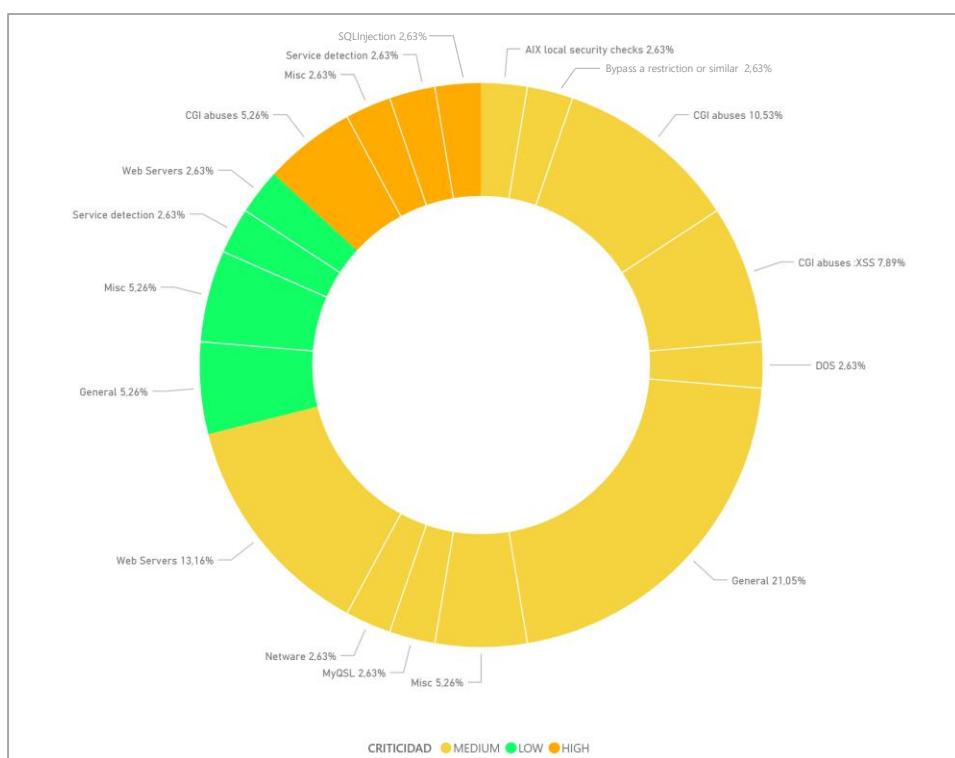


Figura 75. Vulnerabilidades según familia

## 11.5 Vulnerabilidades según sistema operativo

La siguiente gráfica muestra las vulnerabilidades encontradas en los servidores de acuerdo al sistema operativo que tiene cada uno correspondiente a la criticidad, el cual en primer lugar vulnerabilidad tipo “Medium” en sistema operativo Linux Kernel 3.10 CentOS, correspondiente a vulnerabilidades como Apache Server, HTTP, SSH, SSL.

Esta gráfica se genera para analizar durante el periodo de tiempo de la fase de producción consolidar todos los registros y no afirma que un sistema operativo es más seguro que otro, adicional que la diferencia entre la cantidad de vulnerabilidades encontradas en nivel “Medium” entre un sistema y otro es mínimo sin importar que tipo de vulnerabilidades existen ni las remediaciones que existan.

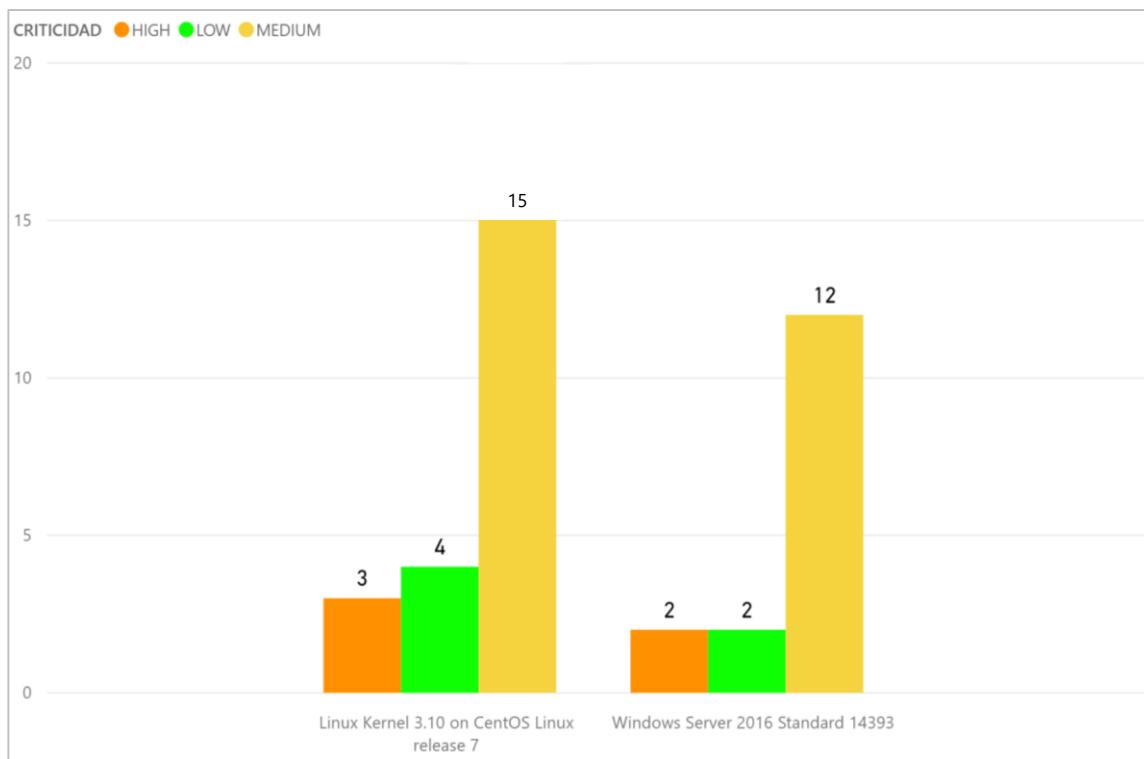


Figura 76. Vulnerabilidades según sistema operativo por criticidad

## 12. Discusión

Este proyecto tiene como propósito identificar y describir la práctica en evaluación de vulnerabilidades que pueden presentarse en los sistemas informáticos de una compañía. Ante todo, se muestra aquellos eventos que más se dieron en cada uno de los servidores que fueron sujetos a la práctica efectuada, donde se generó cada una de las vulnerabilidades, que no se tenían en cuenta, por grado de criticidad. Igualmente, se identificaron aquellos puertos abiertos y huecos de seguridad que en algún momento podrían llegar a generar impacto, sobre la integridad, confidencialidad o disponibilidad de la información, otras señales que podrían experimentar las compañías expuestas a cualquier hecho de cibercriminales es que los puertos que dan acceso a los servidores que contienen la información estén abiertos sin ninguna regulación a los mismos.

El despliegue a eventos relacionadas con todas las vulnerabilidades encontradas, se registran en los diferentes anexos destacando el rango de criticidad (critica, alta, media, baja) que están expuestos dichos servidores. No se presentaron en cantidad, profunda de criticidad a nivel de seguridad. En los últimos años, como lo es sabido se ha elevado el número de ataques a la seguridad informática a nivel mundial, cada vez se atacan más los sistemas informáticos, ya sea para cometer delitos, robos de información, venta y secuestro de la misma, los ataques han sido eventos recurrentes de tipo catastrófico que han afectado a toda la información e incluso ocasionan con la misma entrada a los sistemas terrorismo no solo a nivel informático sino a nivel físico a diferentes naciones, ya que ésta ha sido azotada por varios cibercriminales.

Por lo tanto, es evidente que se reporten como eventos a la compañía que nos dio la posibilidad de tratar la experiencia o laboratorio como objeto de estudios de los servidores como la muestra de las vulnerabilidades encontradas. No menos importante es que el grupo de estudiantes, tuvo una gran colaboración del grupo de la empresa, quien apoyo desde el gerente de la compañía, como los ingenieros e incluso, personal destinado para cumplir con las tareas y cronogramas asociados al mismo proyecto. Se realizaron reuniones de presentación, reuniones presenciales, discusiones tanto telefónicamente como a través de video conferencia, y retroalimentación de todo lo encontrado en los mismos y en constante comunicación.

A continuación, se muestra en la siguiente tabla la base de información consolidada de las vulnerabilidades encontradas, como base de la elaboración del plan de remediación para la empresa el cual brindamos como recomendación de acuerdo los resultados obtenidos durante el desarrollo del proyecto ( Anexo 3- Plan de Remediación).

Tabla 14. Tabla consolidada para Plan de Remediación ( Anexo 22 - Remediación)

NESSUS PLUGIN ID	Nombre vulnerabilidad	Ips afectadas	Puertos *fuente IANA	CVE	CVSS SCORE V3	Tipo	Familia	Descripción	Solucion	Fecha ejecucion
100634	Redis Server Unprotected by Password Authentication	*.*.110.2.*.*.110.3	6379 no asignado/TC P	N/A	9.8	Remoto	Misc	El Servidor Redis (Remote dictionary Server) es una herramienta de estructura de datos de código abierto. Teniendo en cuenta que esta diseñado para ser accedido en entornos de confianza, no debería estar expuesto a internet. Debe restringirse todas las peticiones externas a excepción del tráfico conocido de clientes de confianza en la red.	Dado que la vulnerabilidad asociada a este servidor hace referencia a que este se encuentra sin contraseña esta se debe configurar de manera que sea robusta para que el servidor rechace peticiones de clientes no autenticados y así prevenir ataques de fuerza bruta . Para ello usando el comando REWRITE se modifica el archivo redis.conf( /etc/redis) y se digita lo siguiente: config set requirepass "contraseña"	Corto Plazo
117665	Elasticsearch ESA-2018-15	*.*.110.4	9200 WAP-WSP /TCP	CVE-2018-3831	8.8	Remoto	CGI abuses	Elasticsearch es un motor de búsqueda que permite realizar búsquedas por una gran cantidad de datos de un texto específico, escrito en Java y se basa sobre una licencia Apache. En versiones anteriores a 6.4.1 o 5.6.12 existe una vulnerabilidad de divulgación de información confidencial como contraseñas, tokens o nombres	Se recomienda actualización a la versión 6.4.1 de Elasticsearch o superior.	Corto Plazo
20384	ADODB tmssql.php do Parameter Arbitrary PHP function execution	*.*.100.15	443 HTTPS /TCP	CVE-2006-0147	7.5	Remoto	CGI abuses	ADODb es un paquete de librerías para PHP y Python de bases de datos que permite el desarrollo de aplicaciones web. Existe una vulnerabilidad en PHP hasta la versión 4.6.9 sobre el archivo test/tmssql.php que permite al atacante ejecutar funciones PHP de manera arbitraria, tiene repercusión sobre la confidencialidad, integridad y disponibilidad de la información..	Se recomienda actualización a la versión ADODB a 4.7 para eliminar esta vulnerabilidad.	Corto Plazo
20007	SSL Version 2 and 3 protocol detection	*.*.110.4	1433 MS-SQL-S /TCP	N/A	7.5	Remoto	Service detection	El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0	Se recomienda deshabilitar conexiones cifradas bajo el protocolo SSL 2.0 y 3.0 y utilizar a cambio TLS 1.1	Corto Plazo
42873	SSL medium strength cipher suites supported(sweet 32)	*.*.100.10.*.*.100.11 *.*.100.12.*.*.100.13 *.*.100.14.*.*.100.15 *.*.100.16.*.*.100.17 *.*.100.18.*.*.100.19 *.*.100.20.*.*.110.3 *.*.110.4.*.*.110.6  *.*.100.16.*.*.100.17.*.*.100.18 *.*.100.19.*.*.100.20.*.*.110.3 *.*.110.4	443 HTTPS /TCP	CVE-2016-2183	7.5	Remoto	General	La vulnerabilidad a la que están expuestos estos servidores se conoce como ataque "SWEET32" (asignado como CVE-2016-2183), en donde un atacante remoto puede obtener información confidencial(obtener datos de texto plano) debido a un error en el cifrado DES/3DES que se utiliza como parte del protocolo SSL/TLS.	Dado que no se debería utilizar cifrados de bloques de 64 bits, el servidor web debería configurarse para aceptar 128 bits, debería ofrecer 3DES como cifrado de solo respaldo. Las bibliotecas y aplicaciones TLS deben limitar las sesiones de esta a través de una renegociación TLS o cerrando la conexión e iniciando una nueva.	Corto Plazo
11213	HTTP TRACE / TRACK Methods Allowed	*.*.100.9.*.*.100.10 *.*.100.11.*.*.100.12 *.*.100.13 *.*.100.14.*.*.100.15 *.*.100.15.*.*.100.17 *.*.100.18.*.*.100.19 *.*.100.20.*.*.110.2 *.*.110.3 *.*.110.6  *.*.100.9.*.*.100.17.*.*.100.18 *.*.100.19 *.*.100.20.*.*.110.2 *.*.110.3 *.*.110.4	443 HTTPS /TCP	CVE-2003-1567, CVE-2004-2320, CVE-2010-0386	5.8	Remoto	Web Servers	Son métodos HTTP que se utilizan para depurar las conexiones del servidor web. Trace está habilitado por defecto en instalaciones de Apache.	Si se ejecuta Apache versión 1.3.34/2.0.55 o sobre la versión 2.2 se debe agregar la directiva TraceEnable en el archivo httpd.conf y establecer el valor desactivado. Se puede crear una regla mod_rewrite que deshabilite los métodos Http. Se debe reiniciar el servidor de apache para actualizar los cambios aplicados.	Mediano Plazo
90517	SSH weak algorithms supported	*.*.100.9.*.*.100.10.*.*.100.11 *.*.100.12.*.*.100.13 *.*.100.14.*.*.100.15 *.*.100.16.*.*.100.17 *.*.100.18.*.*.100.19 *.*.100.20.*.*.110.3 *.*.200.10.*.*.200.11 *.*.200.12.*.*.200.13 *.*.200.14.*.*.200.15 *.*.200.16.*.*.200.17 *.*.200.18.*.*.200.19 *.*.200.20.*.*.200.50 *.*.200.51	22 SSH /TCP	N/A	4.3	Remoto	Misc	El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles o ningún algoritmo en absoluto.	Se debe eliminar el cifrado débil para ello se debe modificar el archivo /etc/ssh/sshd_config y agregar lo siguiente: Ciphers aes128-ctr,aes192-ctr,aes256-ctr Lo anterior se puede agregar al final del archivo o donde se encuentre el Ciphers. Una vez guardado el archivo se debe reiniciar el servicio de ssh. Dependiendo de la versión del S.O, se agregarán más opciones de cifrado o menos dependiendo el caso.	Mediano Plazo

Mencionado lo anterior, se asevera que, teniendo un buen aseguramiento, y supervisando a menudo todos los sistemas con un buen escaneo, ya sea a nivel de vulnerabilidades, posibles ataques o puertos abiertos, sin dejar en un plazo largo de hacerlo, llevará y ayudará a las empresas a minimizar las vulnerabilidades que están expuestas en sus sistemas de información y como consecuencia, se sentirán en ambiente adecuado de confiabilidad de la información que estas generan confianza en cada transacción o iteración que hagan de sus datos con los sistemas a conectar.

Se recomienda que, para evaluaciones posteriores, se pueda llevar el mismo procedimiento, de ejecución de las remediaciones entregadas, escaneando nuevas vulnerabilidades a los mismos servidores, con la finalidad de comprobar que los cambios y remediaciones que se implementaron durante el proyecto son consistentes, contextualmente que permitirá certificar que la metodología aplicada, logra incrementar la seguridad de informática y llevar al mínimo las vulnerabilidades que todas las compañías están expuestas.

### **13. Conclusiones**

De acuerdo con los resultados de la encuesta realizada por ESET Latinoamérica para el documento ESET Security Report 2014, la explotación de vulnerabilidades se ha convertido en la mayor preocupación de las empresas en materia de seguridad, seguida de otros incidentes como infección por malware, fraudes, phishing o ataques de denegación de servicio (DoS). En este sentido, la evaluación cobra relevancia para evitar las incidencias relacionadas con la explotación de las mismas y como un medio para la aplicación de un elemento de la denominada seguridad ofensiva, a través de los escáneres de vulnerabilidades.

Es por esto que se requiere enfatizar y evaluar la seguridad de las empresas realizando actualizaciones de seguridad, lo cual sería la principal protección ante las vulnerabilidades existentes. Estos procesos de escaneo pueden tomar algo de tiempo durante la búsqueda de buenas herramientas, consolidación de información y analítica, sin embargo, de toda esta información permite tomar medidas preventivas y generar remediaciones a tiempo que mejoren la seguridad de la empresa.

Los resultados del análisis de riesgo proveen información sobre las debilidades y vulnerabilidades que tiene una organización, desde aquí se tiene una visión general para tomar decisiones frente a las mejoras que se deben adoptar para garantizar la seguridad de la empresa en cuanto a los sistemas de información.

El proceso de implementar un procedimiento como buena práctica que permita tener un lineamiento iterativo y controlado con el fin de garantizar la seguridad de los sistemas dentro de

la empresa requiere verificación constante y registro de eventos encontrados durante cada una de las fases de la metodología adoptada para lograr salvaguardar los activos de la empresa.

Es importante comprobar periódicamente el nivel de seguridad de la empresa en cuanto a la protección de servidores con el fin de asegurar los recursos de la organización y así mismo la información contenida en ellos.

La auditoría de sistemas debe considerarse como un método que colabora en la mejora de procesos de seguridad al interior de la información.

Es recomendable que en la empresa se cuente con una metodología adaptada como buena práctica con la finalidad de implementar como guía y seguimiento paso a paso para realizar análisis de vulnerabilidades existentes en los sistemas y así poder aceptar, mitigar o reducir el riesgo en la seguridad y así salvaguardar los activos de la organización.

## 14. Documentación de Referencia

- [1] M. Osores, «Innovación en ciberseguridad se acelera por aumento de ataques,» 30 Mayo 2019. [En línea]. Available: <https://searchdatacenter.techtarget.com/es/noticias/252464261/Innovacion-en-ciberseguridad-se-acelera-por-aumento-de-ataques>.
- [2] COLPRENSA, «elcolombiano.com,» 12 Abril 2018. [En línea]. Available: [www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174](http://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174).
- [3] TECNOSFERA, «eltiempo.com,» 03 Agosto 2017. [En línea]. Available: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-conexiones-a-banda-ancha-en-colombia-116374>.
- [4] SGS, «Formación como auditores internos en el estándar ISO 27001:2013,» de Marzo, Bogotá, 2019.
- [5] M. A. Mendoza, «La importancia de identificar, analizar y evaluar vulnerabilidades,» Noviembre 2014. [En línea]. Available: <https://www.welivesecurity.com/la-es/2014/11/12/identificar-analizar-evaluar-vulnerabilidades/>.
- [6] C. Gutierrez, «¿Qué es y por qué hacer un Análisis de Riesgos?,» Agosto 2012. [En línea]. Available: <https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/>.
- [7] «Estándares abiertos sobre vulnerabilidades,» Agosto 2018. [En línea]. Available: <https://www.blogdelciso.com/2018/08/15/estandares-abiertos-sobre-vulnerabilidades/>.

- [8] «CVSS,» 2019. [En línea]. Available: <https://www.first.org/cvss/>.
- [9] M. A. Mendoza, «Vulnerabilidades: ¿qué es CVSS y cómo utilizarlo?,» Agosto 2014. [En línea]. Available: <https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/>.
- [10] C. E. Mogollón, «Exposición OWASP,» de *Materia Seguridad en S.O y APPs - Especialización Seguridad en Redes Telemáticas - Universidad El Bosque*, Bogotá, 2018.
- [11] C. Commons, «OWASP Top 10,» 2017. [En línea]. Available: <https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf>.
- [12] P. Herzog, «OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad,» 2000- 2003. [En línea]. Available: <https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml>.
- [13] «NESSUS ES LA SOLUCIÓN N.º 1,» 2019. [En línea]. Available: <https://es-la.tenable.com/products/nessus/nessus-professional>.
- [14] E. Editorial, 2019. [En línea]. Available: <https://reportedigital.com/iot/nmap/>.
- [15] «Zenmap,» 2019. [En línea]. Available: <https://nmap.org/zenmap/>.
- [16] P. Arnedo, «Top of the best vulnerability scanners for penetration testing in 2019.,» 2019. [En línea]. Available: <http://seguridadinformaticaactual.com/2019/05/26/top-de-los-mejores-escaneres-de-vulnerabilidad-para-pruebas-de-penetracion-en-el-2019/>.

- [17] R. Castro, «Presentación Seguridad en Redes,» de *Especialización Seguridad en Redes Telemáticas*, Bogotá, 2019.
- [18] www.isecom.org, «OSSTMM 3,» [En línea]. Available: <http://www.isecom.org/mirror/OSSTMM.3.pdf>.
- [19] «Tenable community,» 27 Enero 2018. [En línea]. Available: <https://community.tenable.com/s/article/Resolving-the-network-interface-does-not-support-packet-forgery-error>.

## 15. Glosario

**Activo:** Algo que tiene valor para la organización (ISO/IEC 13335-1:2004). Compuesto por información, procesos, personas, infraestructura y aplicaciones.

**Amenaza:** Posibilidad de violar la seguridad que existe si se da una circunstancia, capacidad, acción o evento que puede infringir la seguridad y causar daño. Esto es, una amenaza es el posible riesgo de que una vulnerabilidad sea explotada. Evento que puede provocar un incidente en la organización produciendo daños o pérdidas materiales/inmateriales. Situación o evento que puede generar un incidente o afectar un recurso. Posibilidad de violar la seguridad. [17]

**Análisis de riesgos:** Permite conocer cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades, para establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

**Ataque:** Asalto a la seguridad del sistema derivada de una amenaza inteligente, es decir, un acto deliberado que intenta evadir los servicios de seguridad y violar las políticas de seguridad de un sistema. Puede ser pasivo o activo:

**Ataque Activo:** Interfiere con el tráfico legítimo de la red, entre los tipos se encuentra: suplantación de identidad, modificación del mensaje, denegación, repetición, retransmisión. [17]

**Ataque Pasivo:** Monitoreo no autorizado por un intruso el tráfico en la red para capturar información; escucha y analiza el tráfico; no afecta recursos.

**Ciberataque:** Es la explotación de forma deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Estos ataques utilizan código malicioso para alertar la lógica o los datos del ordenador, lo que puede comprometer la información y provocar delitos cibernéticos.

**Confidencialidad:** Los componentes del sistema serán accesibles solo por aquellos usuarios autorizados, impedir el acceso no autorizado.

**CPE (Common platform enumeration):** es un esquema de nombres estructurado para sistemas, software y paquetes de tecnología de la información. Basado en la sintaxis genérica para los Identificadores Uniformes de Recursos (URI), el CPE incluye un formato de nombre formal, un método para verificar nombres contra un sistema y un formato de descripción para unir texto y pruebas a un nombre.

**CVE (Common vulnerabilities and exposures):** Lista de entradas que contiene un número de identificación, una descripción y al menos una referencia pública, para vulnerabilidades de seguridad informática conocidas públicamente. Se utilizan en numerosos productos y servicios de ciberseguridad de todo el mundo.

**CVSS (Common vulnerability score system):** El Sistema de puntuación de vulnerabilidad común (CVSS) proporciona una manera de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje su gravedad. La puntuación numérica se puede traducir a una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades. CVSS es un estándar publicado utilizado por organizaciones de todo el mundo, se encuentra actualmente en la versión 3.0.

**CWE (Common weakness enumeration specification):** Proporciona un lenguaje común (lista desarrollada por la comunidad) para encontrar, tratar las causas de las vulnerabilidades de seguridad del software tal como se encuentran en el código, diseño, o arquitectura del sistema. Sirve como línea base para la identificación de debilidades, mitigación y esfuerzo de prevención. Cada Id individual representa un tipo de vulnerabilidad individual. Mantainded por Corporacion MITRE que proporciona una lista en detalle para cada CWE individual.

**Disponibilidad:** Propiedad de un sistema o recurso de estar disponible, utilizable, operacional; los servicios deben estar siempre activos (24x7x365) es decir los componentes del sistema

y/o datos a solicitud de usuarios cuando así lo deseen.

**Integridad:** Componentes del sistema solo pueden ser creados y modificados por los usuarios autorizados, impedir la manipulación de la información.

**NVD (National vulnerability database):** Repositorio del gobierno de los Estados Unidos de donde se toman los datos de vulnerabilidades CVE. Incluye bases de datos de referencias de listas de verificación de seguridad, fallas de software relacionadas con la seguridad, configuraciones erróneas, nombres de producto y métricas de impacto.

**Nessus:** Analizador de vulnerabilidades más completo en el mercado actual.

**Nmap:** Network Mapper, es un código libre y abierto (OpenSource), es la utilidad por excelencia, para el descubrimiento de redes y auditorías de seguridad.

**Norma ISO/IEC 27000:** Familia de estándares ISO orientados a la seguridad de la información.

Incluye conceptos y definiciones que soportan a la familia. Algunos integrantes importantes son:

- **ISO 27001:** Norma principal, requisitos del SGSI. Indica que se debe hacer.
- **ISO 27002:** Controles recomendados de la norma ISO 27001. Indica cómo se hace.
- **ISO 27003:** Guía implementación siguiendo PHVA
- **ISO 27005:** Estándar de gestión de riesgos de seguridad de la información.

**Open Source:** Código Abierto; Expresión con la que se conoce al software distribuido y desarrollado libremente

**Openvas:** es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. Permite la actualización continua de la base de Pruebas de Vulnerabilidades de Red. Es una herramienta principal de OSSIM, todos los productos que la componen son software libre y la mayoría de ellos son distribuidos bajo licencia GPL.

**OSSTM:** Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM). Incluye un marco de trabajo que describe las fases que habría que realizar para la ejecución de la auditoría. Está compuesto por diversas fases; que permite probar bajo un marco la seguridad operativa de ubicaciones físicas, flujo de trabajo, seguridad inalámbrica, de telecomunicaciones, de redes de datos y cumplimiento para finalmente lograr desarrollar un informe de auditoría con las pruebas de seguridad realizadas.

**OVAL (Open vulnerability and assessment language):** Es una comunidad/estándar de seguridad de la información internacional para promover contenido de seguridad abierto al público. Son definiciones de diversas fuentes, en donde se puede verificar información de vulnerabilidades o parches. Va integrado con el sitio web de cvedetails.com para navegar entre CVE, productos y detalles de definiciones OVAL.

**OWASP:** Proyecto abierto de seguridad de aplicaciones web. Genera un top 10 de vulnerabilidades (riesgos seguridad) a nivel mundial de aplicaciones web.

**Plan de remediación:** Documento que permita corregir las fallas identificadas y evaluadas, en conformidad con los resultados de la priorización. En general, la corrección de estas fallas se relaciona con la aplicación de actualizaciones o parches de seguridad o ajustes a la configuración o eliminación de software.

**Procedimiento de gestión de vulnerabilidades:** Es un documento que incluye las fases para la realización de la evaluación de vulnerabilidades de activos de una infraestructura tecnológica, en el cual se encuentran las debilidades de las plataformas de software o hardware para solucionar las fallas, antes de que puedan generar un impacto negativo o la materialización de eventos indeseados e inesperados. Por normatividad se debe definir la frecuencia de ejecución de las pruebas el cual depende del sector.

**PTES Technical Guidelines:** El Estándar de Ejecución de Pruebas de Penetración fue creado por algunas de las mentes más brillantes y expertos definitivos en la industria de pruebas de penetración. Consta de siete fases de prueba de penetración y puede usarse para

realizar una prueba de penetración efectiva en cualquier entorno.

**Remediación:** Acciones aplicadas para cerrar o eliminar una vulnerabilidad tales como: cierre de puertos, aplicación de parches, actualización de software ajustes a la configuración o eliminación del software afectado.

**Retina:** Es uno de los escáneres más potente de vulnerabilidades que existen en el mercado, proporciona pruebas de vulnerabilidad para múltiples plataformas, evaluación de vulnerabilidades y la capacidad de crear sus propias auditorías

**Riesgo:** Estimación del grado de exposición de 1 o más activos de información ante la materialización de una amenaza que pueda impactar negativamente o causar daños en una organización. Se puede aceptar, mitigar, o transferir. Se busca reducir a un nivel que resulte aceptable.

**Seguridad de la información:** Proteger la información de una organización, independientemente del lugar en el que se localice: impresos en papel, discos duros de las computadoras, etc. Tiene 3 principios fundamentales: Confidencialidad, Integridad, Disponibilidad. Su radio de acción cubre análisis de riesgos, seguridad personal/física, gestión de comunicaciones, control acceso, gestión de incidentes, gestión continuidad del negocio, entre otros.

**Seguridad informática:** Proteger las infraestructuras tecnológicas y de comunicación que soportan la operación de una organización(hardware,software) y que estas sean utilizadas de la manera indicada por la organización. Su radio de acción cubre pruebas de evaluación de vulnerabilidades, test de penetración, hacking ético, entre otros.

**SGSI (Sistema de gestión de seguridad de la información):** Orientado a gestionar riesgos del negocio. Es el concepto central sobre el que se construye la norma ISO 27001. Debe ser realizado mediante un proceso sistemático, documentado, conocido por toda la organización. Ayuda a establecer las políticas y procedimientos en relación a los objetivos de negocio de la organización con el objeto de mantener un nivel de exposición siempre

menor al nivel de riesgo que la propia organización ha decidido asumir.

**VPN:** Una red privada virtual (RPV), es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

**Vulnerabilidad:** Punto débil en la seguridad de un sistema informático que permiten que un atacante comprometa la integridad, disponibilidad, confidencialidad de la información.

**Zenmap:** Herramienta similar a Nmap pero en ambiente gráfico, el cual permite observar el estado de los puertos personalizando los tipos o perfiles de escaneo.

## **16. Anexos**

- Anexo 1 - Acta de Calificación y Aprobación de Trabajo de Grado
- Anexo 2 - Carta presentación estudiantes - PGC-F1
- Anexo 3 - Carta aceptación propuesta de proyecto de grado - PGC-F2
- Anexo 4 - Carta aprobación del trabajo de grado - PGC-F3
- Anexo 5 - Carta aceptación empresa PGC-F6
- Anexo 6 - Procedimiento gestión de vulnerabilidades
- Anexo 7 - Herramientas de escaneo
- Anexo 8 - Escaneo Zenmap
- Anexo 9 - Enrutamiento de la red
- Anexo 10 - Registro Fase de Pruebas
- Anexo 11 - Escaneo Nessus 15Feb
- Anexo 12 - Pruebas Feb25 Mar03
- Anexo 13 - Escaneo Múltiple
- Anexo 14 - Escaneo Retina
- Anexo 15 - Pruebas Mar04
- Anexo 16 - Pruebas Mar11-17 Retina
- Anexo 17 - Inventario de activos
- Anexo 18 - Registro fase producción
- Anexo 19 - Matriz de Riesgo
- Anexo 20 - Graficas resultados
- Anexo 21 - Plan de Remediación
- Anexo 22 - Remediación