HACKING ÉTICO BASADO EN LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD – OSSTMM, APLICADO A LA RAMA JUDICIAL, SECCIONAL ARMENIA

ALLEN DAVID ZULUAGA MATEUS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ARMENIA, QUINDÍO
2017

HACKING ÉTICO BASADO EN LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD – OSSTMM, APLICADO A LA RAMA JUDICIAL, SECCIONAL ARMENIA

ALLEN DAVID ZULUAGA MATEUS

Trabajo de grado aplicado, para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. Esp. FRANCISCO JAVIER HILARION NOVOA
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ARMENIA, QUINDÍO
2017

Nota de Aceptación

_____
_____
_____
_____
_____

_____
Firma presidente del jurado

_____
Firma del jurado

_____
Firma Jurado

Armenia, Quindío.
Noviembre de 2017.

Dedicatoria:

A mi esposa y a mis hijos, por apoyarme en este nuevo proceso de formación académica y de crecimiento personal, por entender mis ausencias y el tiempo que he tenido que dejar de compartir con ellos, para dedicarlo a mis estudios, por siempre estar allí a mi lado, alentándome a cada momento.

A mis padres, por inculcarme la importancia del estudio, la autodisciplina, la constancia y la dedicación, principios sin los cuales sería imposible estar alcanzando las metas que me he fijado.

Agradecimientos:

A Julián Ochoa Arango, profesional apasionado y entregado, ejemplo de disciplina, juicio y perseverancia, por abrirme las puertas de la Entidad y permitirme desarrollarme profesionalmente, apoyándome en todo momento.

A Alexander Moreno Rojas, por compartir conmigo, sin recelo alguno, sus conocimientos y dominio sobre los temas relacionados con la tecnología y la seguridad informática.

A los ingenieros Salomón González y francisco Javier Hilarión Novoa, quienes siempre han estado pendiente de la ejecución del presente proyecto, orientándome continuamente, apoyándome y alentándome día a día.

CONTENIDO

pág.

ÍNDICE DE TABLAS

pág.

ÍNDICE DE FIGURAS

pág.

TÍTULO

Hacking Ético Basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM, Aplicado a La Rama Judicial, Seccional Armenia.

INTRODUCCIÓN

El presente documento aborda el tema del hacking ético utilizado como una herramienta para diagnosticar el nivel de seguridad informática de una entidad u organización, entendiendo que a través de esta práctica es posible identificar vulnerabilidades y debilidades asociadas a la seguridad de la información y de los sistemas informáticos. Es necesario tener en cuenta que la práctica del hacking ético debe apoyarse en una herramienta que permita realizar la identificación y documentación de amenazas y vulnerabilidades de una manera metodológica, es por esto que el presente proyecto se apoya en la Metodología Abierta de Testeo de Seguridad, a través de su manual asociado denominado Open Source Security Testing Methodology Manual - OSSTMM

Es importante tener en cuenta que un diagnóstico de este tipo genera un impacto positivo en cualquier entidad que entienda y asuma el valor y la importancia que tiene hoy día, el garantizar la confiabilidad, autenticidad e integridad de la información. Además, para entidades como la Rama Judicial y en concreto la Dirección Seccional de Administración Judicial de Armenia, este hacking ético es un muy buen punto de partida para evaluar el nivel de seguridad informática, permitiendo que se generaren situaciones que influyan la toma de las decisiones enfocadas en mejorar los niveles de seguridad informática.

Ahora bien, en cuanto a modelos de referencia o parámetros con los cuales pueda medirse el nivel de seguridad informática de una entidad, existen normas técnicas y/o de mejores prácticas, como es el caso de la familia de normas ISO 27000, o el marco de trabajo COBIT, entre otras, las cuales se encuentran orientadas hacia la seguridad de la información. Éstas establecen algunos criterios o elementos que se deben cumplir para garantizar la gestión de seguridad de la información. Igualmente, existen herramientas como lo son OSSTMM, ISSAF y OWASP, que pueden utilizarse como una guía metodológica para verificar el cumplimiento de diferentes criterios de seguridad de la información, esto con la intensión de identificar y describir las posibles vulnerabilidades asociadas a determinada infraestructura tecnológica, entendiendo como infraestructura tecnológica los recursos hardware, software y políticas que soportan la operación tecnológica de una entidad.

Así las cosas, el enfoque con el que se aborda el presente trabajo, es la aplicación del hacking ético como herramienta para el diagnóstico de vulnerabilidades y debilidades en la gestión de la seguridad informática, apoyándose en el Manual de la Metodología Abierta de Testeo de Seguridad - OSSTMM, lo cual se considera como un buen punto referencia para evaluar el nivel de seguridad informática de la Rama Judicial, seccional Armenia.

1. EL PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

La Dirección Ejecutiva Seccional de Administración Judicial de Armenia, precisa conocer el nivel de seguridad informática y las posibles vulnerabilidades a las que sus sistemas informáticos se encuentran expuestos, sin embargo, no se ha aplicado herramienta o metodología alguna que permita evaluar su seguridad informática y así obtener una medida del mencionado nivel de seguridad y/o posibles vulnerabilidades asociadas a sus activos informáticos. Esto ayudara enormemente a la Entidad a evaluar la efectividad de sus controles e implementar nuevas salvaguardas que permitan asegurar tales activos informáticos, con el fin de generar un mayor nivel confianza en sus procesos asociados a tecnológicas de la información.

1.2 DESCRIPCIÓN DEL PROBLEMA

La principal función de la Dirección Ejecutiva de Administración Judicial es la de proveer las condiciones necesarias para el correcto funcionamiento de los diferentes Despachos Judiciales y Administrativos de todo el país. Su estructura administrativa se divide en regiones llamadas “Seccionales”, siendo la Dirección Ejecutiva Seccional de Administración Judicial del Quindío, el ente administrativo encargado de gestionar y administrar, la infraestructura de TI de la Rama Judicial, para todo el Departamento del Quindío, dando cobertura su capital y los once (11) municipios. Dentro de sus funciones se encuentra la implementación, soporte, mantenimiento y mejoramiento de toda la infraestructura tecnológica que utilizan los diferentes despachos judiciales y administrativos, para el cumplimiento de su función misional, que no es otra que la de impartir y administrar justicia en nombre de la Nación. En apoyo a esta misión, la Entidad ha venido implementando diferentes herramientas tecnológicas y sistemas de información, a través de los cuales se busca optimizar la gestión judicial, la administración de justicia y tener una justicia más cercana al ciudadano, en lo cual, la Seccional Quindío, ha sido pionera a nivel nacional.

Es necesario informar que, en materia de seguridad informática, esta Entidad únicamente cuenta algunos procedimientos, propios del Sistema Integrado de Gestión de Calidad y Medio Ambiente – SIGMA, estos procedimientos son:

- Caracterización proceso de gestión tecnológica
- Procedimiento para generación de proyectos relacionados con tecnología de información
- Procedimiento para administrar y soportar infraestructura tecnológica y de comunicaciones

- Procedimiento para administrar y soportar aplicaciones de bases de datos y sistemas operativos de servidores de red en la rama judicial
- Procedimiento para consolidar requerimientos tecnológicos e informáticos

Sin embargo, y pese a los grandes esfuerzos realizados y logros obtenidos, la Entidad no cuenta con una política de seguridad de la información claramente definida, ni mucho menos con un Sistema de Gestión de Seguridad de la Información – SGSI debidamente implementado. Estas premisas, sustentan la vital importancia de tener una medida que identifique el nivel de seguridad informática con que actualmente se cuenta, en donde además puedan observarse las debilidades y fortalezas en cuanto a la gestión de la infraestructura tecnológica. Lo anterior se convertirá en el diagnóstico inicial que permitirá tomar decisiones que propendan por la protección y aseguramiento de la información que administra la Entidad.

Debido a la inexistencia de una norma técnica relacionada con la seguridad informática, que haya sido debidamente adoptada e implementada por la Entidad, es viable la realización de un hacking ético, haciendo posible evidenciar las debilidades y vulnerabilidades que en materia de seguridad informática, pudieran detectarse. A su vez, con base en los resultados aportados por este hacking ético, sería posible establecer un punto de partida para que la Entidad tome las medidas y correcciones pertinentes, en pro de mejorar la Seguridad Informática, para posteriormente generar nuevas iteraciones en el ciclo de mejora de la seguridad de la información, generando un impacto positivo en la Entidad y en beneficio de la comunidad en general.

1.3 FORMULACIÓN DEL PROBLEMA

¿Cómo un Hacking Ético a la infraestructura tecnológica de la Rama Judicial de Armenia, basado en la metodología abierta de testeo de seguridad – OSSTMM, permitirá encontrar vulnerabilidades y determinar el nivel de seguridad informática en dicha dirección seccional?

2. JUSTIFICACIÓN

La información es un valioso activo para entidades como la Rama Judicial, por lo cual se dirigen una gran cantidad de recursos con el fin de garantizar su seguridad. Dicha información, además de ser considerada como uno de los activos más valiosos de la Entidad, debe ser observada a través de su dinámica y evolución, la cual va de la mano con los avances tecnológicos.

La importancia del desarrollo del presente proyecto radica en la necesidad de mantener la integridad, confidencialidad y disponibilidad de la información, enfocándose en asegurar y solidificar la infraestructura tecnológica a través de la cual se administra o gestiona dicha información. La anterior es una tarea evolutiva, que debe moldearse conforme al cambio en las necesidades de la Entidad y así mismo debe ajustarse, conforme a los avances tecnológicos.

De la mano de la evolución tecnológica mencionada anteriormente, han evolucionado también los métodos y mecanismos de seguridad de la información, pero así mismo, los atacantes informáticos han crecido en conocimientos y herramientas, por lo cual es de vital importancia que las diferentes entidades cuenten con las medidas de protección adecuadas para salvaguardar su información, razón por la cual se hace necesario identificar debilidades o vulnerabilidades que podrían ser aprovechadas por un atacante para causar un impacto negativo en la seguridad de la información. Es allí donde el hacking ético cobra un rol importantísimo, sirviendo este como una medida que ofrece las bases que permiten posteriormente, establecer un plan de acción que enfocado a asegurar tal información.

La realización del presente hacking ético indudablemente genera un impacto positivo en las políticas de seguridad de la información de la Rama Judicial, pues se constituye en un elemento de entrada que permite la toma de decisiones basadas en hechos, en pro de la seguridad de la información. Esto a su vez redunda en un beneficio para los usuarios del aparato judicial, pues la información asociada a sus procesos judiciales, se encontrará mejor protegida, generando una mayor confianza en la Entidad.

Otro de los grandes beneficios que genera el presente hacking ético, es que permite a la Rama Judicial, tomar decisiones de manera preventiva, generando soluciones en materia de ciberseguridad, que permitan eliminar las posibles vulnerabilidades encontradas, antes de que estas sean explotadas por un atacante.

3. OBJETIVOS

Para el desarrollo del presente proyecto, se han planteado los siguientes objetivos generales y específicos:

3.1 OBJETIVO GENERAL

Realizar un Hacking Ético a la infraestructura tecnológica de la Rama Judicial de Armenia, basado en la metodología abierta de testeo de seguridad – OSSTMM, a fin de determinar vulnerabilidades a la seguridad informática, que posteriormente se puedan tratar por la Entidad.

3.2 OBJETIVOS ESPECÍFICOS

I. Recabar información que permita planear el hacking ético, para lograr el acceso a la infraestructura tecnológica de la Rama Judicial, Seccional Armenia.

II. Realizar un escaneo de vulnerabilidades a través de técnicas de hacking, que permitan detectar las fallas de seguridad por las cuales se podría ingresar a la infraestructura tecnológica.

III. Obtener y mantener el acceso a la infraestructura tecnológica de la Rama Judicial, a través de la utilización de herramientas de hacking, para confirmar las vulnerabilidades en materia de seguridad informática que pudiera tener la Entidad.

IV. Realizar un informe con los resultados del hacking ético, que contenga recomendaciones que puedan ayudar a la entidad a fortalecer su seguridad informática.

4. ALCANCE Y DELIMITACIÓN

El presente proyecto abarca la realización de un hacking ético, basado en OSSTMM y aplicado a la infraestructura tecnológica de la Dirección Seccional de Administración Judicial de Armenia, para la sede Palacio de Justicia "*Fabio Calderón Botero*.

Dentro del presente proyecto, se incluirán fases de hacking ético tales como:

- **Reconocimiento**: Donde se recaba la información necesaria para poder llevar a cabo que permita llevar a cabo la operación de hackeo
- **Escaneo**: Aquí se realiza un análisis de vulnerabilidades para determinar cuáles grietas de seguridad pueden explotarse luego, para lograr el acceso
- **Obtener Acceso**: En esta fase se pone en práctica lo indagado, se explotan las vulnerabilidades y se logra el acceso
- **Mantener Acceso**: Una vez ya dentro del sistema, se aplican técnicas como generación de backdoors, instalación de troyanos y escalonamiento de privilegios.

Para finalizar se presentará un informe y se realizaran unas recomendaciones de seguridad, que buscan reparar las posibles vulnerabilidades encontradas.

Es necesario aclarar que en el alcance de este proyecto no se incluyen otras sedes judiciales diferentes al Palacio de Justicia "*Fabio Calderón Botero"* ni tampoco aplica para otras ciudades o Direcciones Seccionales, sin embargo, si se podrán evaluar aplicaciones o servicios web que no estén alojadas en la Seccional Armenia.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Existen algunos textos académicos y de investigación que, bajo la misma línea del presente trabajo, abordan el tema del hacking ético y las pruebas de penetración, relacionándose con la metodología OSSTMM, algunos de ellos son:

"*Aplicación de auditoría penetration testing para contribuir con la seguridad de la información en los sistemas informáticos de la empresa Data Business SAC, Trujillo*", es la tesis para optar por el título de ingeniero de sistemas computacionales, desarrollada por Walter Gonzalo Cruz Saavedra, de la Universidad Privada del Norte de Trujillo, Perú. En dicho documento, se aplica una auditoria tipo pentest, a través de la metodología OSSTMM, cumpliendo con las fases de reconocimiento, escaneo y enumeración, obtención de acceso, mantención de acceso y borrado de huellas[1], esto con el fin de contribuir a la seguridad de la información de dicha organización. De dicho trabajo, es posible abstraer el modelo de desarrollo de las pruebas, paso a paso y evaluando los dominios de seguridad pertinentes.

De otro lado, el documento de trabajo de grado en ingeniería informática "*Propuesta de implementación de una metodología de auditoría de seguridad informática*", desarrollado por Roberto López Santoyo, de la Universidad Autónoma de Madrid, realiza una revisión y comparativa de las metodologías OSSTMM, PTES, NIST 800-115, OWASP Testing Guide. Después de hacer una comparativa entre el ámbito digital, físico, social, la guía técnica, métricas e informes de las metodologías anteriormente mencionadas, se elige OSSTMM, como la metodología más completa para este tipo de actividad, basado en que es la única que da alcance a todos los ámbitos de la seguridad y además cuenta con unas métricas que facilitan la forma de preparar los informes[2].

Este último documento, ratifica que la elección de la metodología OSSTMM, como guía metodología para el desarrollo del Hacking Ético a la Rama Judicial, Seccional

[1] Cruz Saavedra, W. G. (02 de junio de 2014). *Universdidad Privada del Norte.* Obtenido de Repositori Institucional: http://repositorio.upn.edu.pe/bitstream/handle/11537/10239/Cruz%20Saavedra%20Walter%20Gonzalo.pdf?sequence=1&isAllowed=y

[2] LÓPEZ SANTOYO, R. (junio de 2015). *Repositorio Universidad Autónoma de Madrid.* Obtenido de Universidad Autónoma de Madrid: https://repositorio.uam.es/bitstream/handle/10486/668900/Lopez_Santoyo_Roberto_tfg.pdf?sequence=1&isAllowed=y

Armenia, es acertada, en relación con las guías o metodologías existentes que se podrían aplicar para el desarrollo del presente proyecto.

5.2 MARCO CONTEXTUAL

Como se describió anteriormente en el capítulo 0 INTRODUCCIÓN

El presente documento aborda el tema del hacking ético utilizado como una herramienta para diagnosticar el nivel de seguridad informática de una entidad u organización, entendiendo que a través de esta práctica es posible identificar vulnerabilidades y debilidades asociadas a la seguridad de la información y de los sistemas informáticos. Es necesario tener en cuenta que la práctica del hacking ético debe apoyarse en una herramienta que permita realizar la identificación y documentación de amenazas y vulnerabilidades de una manera metodológica, es por esto que el presente proyecto se apoya en la Metodología Abierta de Testeo de Seguridad, a través de su manual asociado denominado Open Source Security Testing Methodology Manual - OSSTMM

Es importante tener en cuenta que un diagnóstico de este tipo genera un impacto positivo en cualquier entidad que entienda y asuma el valor y la importancia que tiene hoy día, el garantizar la confiabilidad, autenticidad e integridad de la información. Además, para entidades como la Rama Judicial y en concreto la Dirección Seccional de Administración Judicial de Armenia, este hacking ético es un muy buen punto de partida para evaluar el nivel de seguridad informática, permitiendo que se generaren situaciones que influyan la toma de las decisiones enfocadas en mejorar los niveles de seguridad informática.

Ahora bien, en cuanto a modelos de referencia o parámetros con los cuales pueda medirse el nivel de seguridad informática de una entidad, existen normas técnicas y/o de mejores prácticas, como es el caso de la familia de normas ISO 27000, o el marco de trabajo COBIT, entre otras, las cuales se encuentran orientadas hacia la seguridad de la información. Éstas establecen algunos criterios o elementos que se deben cumplir para garantizar la gestión de seguridad de la información. Igualmente, existen herramientas como lo son OSSTMM, ISSAF y OWASP, que pueden utilizarse como una guía metodológica para verificar el cumplimiento de diferentes criterios de seguridad de la información, esto con la intensión de identificar y describir las posibles vulnerabilidades asociadas a determinada infraestructura

tecnológica, entendiendo como infraestructura tecnológica los recursos hardware, software y políticas que soportan la operación tecnológica de una entidad.

Así las cosas, el enfoque con el que se aborda el presente trabajo, es la aplicación del hacking ético como herramienta para el diagnóstico de vulnerabilidades y debilidades en la gestión de la seguridad informática, apoyándose en el Manual de la Metodología Abierta de Testeo de Seguridad - OSSTMM, lo cual se considera como un buen punto referencia para evaluar el nivel de seguridad informática de la Rama Judicial, seccional Armenia.

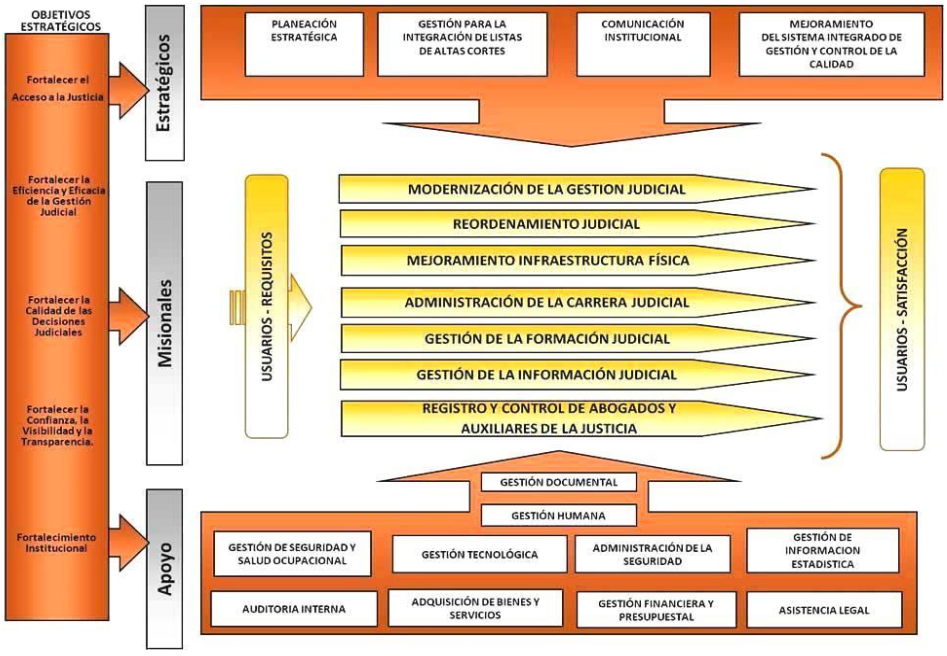
EL PROBLEMA, la Rama Judicial es una Entidad de Orden Nacional que se encuentra dividida geográficamente en seccionales y administrativamente en unidades funcionales, siendo la Dirección Seccional de Administración Judicial de Armenia, el organizo que administra y gestiona los recursos en el Departamento del Quindío, para brindar la infraestructura y logística necesaria que permita a los diferentes despachos judiciales, cumplir con su labor misional.

A nivel de procesos, en la Dirección Ejecutiva Seccional de Administración Judicial, existen 3 macroprocesos, estos son:

- Estratégicos
- Misionales
- Apoyo

Dentro de los procesos de apoyo, se encuentra el proceso de *Gestión Tecnológica*, cuyo objetivo es el de gestionar, administrar y mantener los recursos informáticos y de comunicaciones, para el desarrollo de los objetivos institucionales [3], lo cual es apreciable en la siguiente imagen:

Figura 1. Mapa de Procesos



[3] CONSEJO SUPERIOR DE LA JUDICATURA. (s.f.). *Sistema Integrado de Gestión de Calidad y Medio Ambiente - SIGMA*. Recuperado el 29 de marzo de 2017, de Mapa de procesos: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/portal/index.php?idcategoria=8

Fuente:
http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/portal/index.php?idcategoria=8

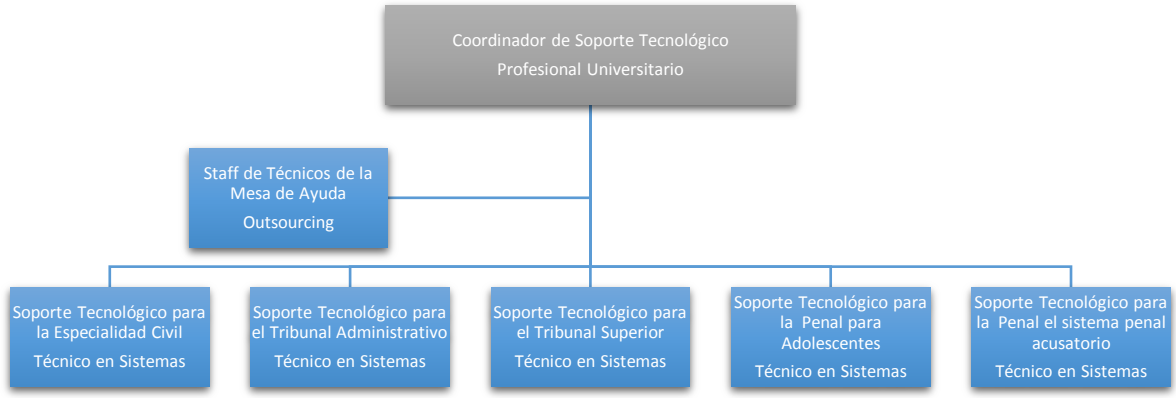
A continuación, se ilustra el organigrama de la Dirección Ejecutiva de Administración Judicial, en donde se resaltada el área de informática.

Figura 2. Organigrama Dirección Ejecutiva de Administración Judicial

Fuente: el autor

El área de informática de la Dirección Seccional de Administración Judicial tiene una estructura y conformación diferente a la Nivel Central. En el Nivel Seccional, se observa una estructura estratégica y de planeación, conformada por Divisiones y con unos lideres para cada división, esto conforme a las necesidades de la Entidad. Ya en el Nivel Seccional, la estructura organizacional es más operativa, en donde existe un coordinador de soporte tecnológico y un grupo técnico y operativo distribuido por especialidades judiciales, tal como se observa a continuación:

Figura 3. Estructura organizacional del área informática



Fuente: el autor

El área de informática está a cargo de un profesional universitario y cuenta con un grupo técnico de apoyo, para atender los requerimientos de todas las especialidades judiciales, además de un staff de técnicos de la mesa de ayuda, quienes brindan el soporte de primer nivel.

A continuación, se relacionan las funciones del área de informática, las cuales están en cabeza de dicho profesional, quien, a su vez, se apoya en su grupo de trabajo para la realización de tales actividades:

- ✓ Atender las solicitudes técnicas de los usuarios.
- ✓ Velar por la seguridad e integridad de la información.
- ✓ Verificar la conectividad de los usuarios.
- ✓ Servicio de mantenimiento preventivo para los equipos de cómputo para las seccionales.
- ✓ Desarrollar, implementar y soportar los sistemas de información al servicio de la Rama Judicial
- ✓ Verificar el cumplimiento del Plan de Modernización Tecnológica de la Rama Judicial y del Plan de Inversiones

Además de las anteriores funciones, el área de informática también brinda apoyo a los estudios técnicos para procesos en materia de contratación de elementos tecnológicos.

Una de las funciones más importantes del área de informática, es la de administrar y gestionar las bases de datos de los sistemas de información que soportan la operación de la Entidad.

Ahora bien, la Rama Judicial no ha sido ajena al proceso de penetración de las TICs[4], hoy día muchas de sus actividades son administradas y gestionadas a través de sistemas de información, el principal de ellos Justicia XXI, del tipo Cliente – Servidor, que además ahora cuenta con una versión web, denominada Justicia XXI Web, que se encuentra en periodo de implantación a través de planes piloto en algunas seccionales y algunas especialidades del aparato judicial, a continuación se detallan algunas de las aplicaciones informáticas que se usan en la Rama Judicial

Tabla 1. Aplicaciones informáticas de la Rama Judicial

Aplicaciones Informáticas de la Rama Judicial		
Función Judicial	**Función Judicial**	**Función Administrativa**
Justicia XXI Consulta Jurisprudencia Depósitos Judiciales	Reparto Notificaciones SAIDOJ (Archivo) Depósitos Judiciales	SIERJU (Estadística Judicial) URNA (Registro Nacional de Abogados y Auxiliares de la Justicia) SCALA (Carrera Judicial) KACKTUS (Recurso Humano) SIIF SICOF (Inventarios)

Fuente: el autor

Para apoyar todo este proceso, la Rama Judicial estableció en su Plan Sectorial de Desarrollo para la vigencia 2015 – 2018, una política institucional denominada P*olítica Tecnológica*[5], esta política cuenta con un componente denominado *Plan Estratégica Tecnológico de la Rama Judicial*, a través del cual la Rama Judicial ha venido fortaleciendo fuertemente su componente de infraestructura de TI, es así como se renovó todo el parque computacional de la Entidad, igualmente se mejoró la conectividad y acceso a internet, a través de canales MPLS con última milla en fibra óptica, en todo el territorio Nacional, también se han puesto en marcha sistemas de información de cara al ciudadano, tal como lo es la consulta de procesos, justicia XXI, registros nacionales de personas emplazadas y del Código General del Proceso – CGP.

[4] CONSEJO SUPERIOR DE LA JUDICATURA. (s.f.). *Corporación Exelencia en la Justicia.* Obtenido de Presente y Futuro de las TICS en la Rama Judicial: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjD9uOwwInUAhVMJCYKHaQnDOsQFgg1MAQ&url=http%3A%2F%2Fwww.cej.org.co%2Findex.php%2Fcomponent%2Fdocman%2Fdoc_download%2F393-presentacion-consejo-superior-de-la-judicatura%3FItemid%3

[5] CONSEJO SUPERIOR DE LA JUDICATURA. (2015). *Rama Judicial.* Obtenido de Plan Sectorial de Desarrollo: https://www.ramajudicial.gov.co/documents/1513685/5113559/Plan_Sectorial_de_Desarrollo_Rama_Judicial_2015-2018+%283%29.pdf/a7b785e1-fb02-4ff6-905b-c16ac93df312

Todo lo anterior sirve como preparación y como plataforma para una meta que tiene la Rama Judicial y es el *Expediente Digital y Litigio en Línea*, esto permitirá implementar una política de cero papel, que todos los expedientes judiciales sean gestionados electrónicamente y que los abogados litigantes y ciudadanos que se integran al aparato judicial, puedan desde sus casas u oficinas, presentar demandas, acciones de tutela y demás acciones constitucionales, así mismo las notificaciones, respuestas y fallos se realizaran de manera electrónica y las audiencias podrían hacerse por medios virtuales, como ya ocurre desde hoy.

En cuanto al Expediente Digital y Litigio en Línea, ya se han logrado avances a nivel de piloto, como lo es el caso de la sentencia 73001312100220130016601, 73001312100120130014501, 73001312100120140001100, de junio 16 de 2014, en donde la Sala Civil Especializada en Restitución de Tierras, adscrita al Tribunal Superior de Bogotá, falló a favor de una víctima del conflicto armado, la restitución de unos predios baldíos en Ataco, Tolima, ordenando al INCODER, realizar la restitución de los mismos[6].

Entendiendo el impacto que tiene la seguridad informática en todos estos cambios y modernización que está viviendo la Rama Judicial, se debe procurar por contar con unos niveles ideales de seguridad de la información y es allí, donde la metodología OSSTMM en el marco de un Ethical Hacking podrá evidenciar si existen falencias en esta materia y permitirá a la Entidad fortalecerse y estar preparada para asumir estos nuevos retos que se le presentan.

5.3 MARCO TEÓRICO

La masificación de Internet y las telecomunicaciones, ha permitido la penetración de las Tecnologías de la Información y las Telecomunicaciones, en todo nivel, lo cual ha creado en las diferentes entidades ya sean del Estado, privadas o de la sociedad civil, la necesidad imperativa de integrar diferentes sistemas de información a su quehacer y por tanto la protección de dichos sistemas y de la información misma se ha convertido en un objetivo estratégico, pues así como los avances tecnológicos en los últimos años han sido bastante significativos, también la cantidad de amenazas han ido incrementando. El Ministerio de Tecnologías de la Información y las Comunicaciones, en Colombia, indica que tan solo en el año 2011,

[6] AMBITO JURIDICO. (20 de junio de 2014). *Noticias Juridicas y Analisis de Nuevas Leyes*. Obtenido de Sentencia “cero papel” restituye predios a víctimas del conflicto: https://www.ambitojuridico.com/BancoConocimiento/Civil-y-Familia/noti-142006-05-sentencia-cero-papel-restituye-predios-a-victimas-del-conflicto

se llevaron a cabo más de 550 ataques exitosos a entidades del Estado[7]; la anterior cifra ha venido en aumento, teniendo años muy críticos tal como el 2014.

Adicionalmente y debido a la gran importancia que ha venido tomando la información, llegando incluso a ser considerada como un activo muy valioso al interior de las diferentes organizaciones, es que la seguridad informática adquiere un especial valor, pues su objetivo de garantizar que la información de cualquier organización, se conserve bajo tres pilares fundamentales, los cuales se describen en Figura 4, es ya una necesidad para todas las entidades y organizaciones que incorporan Tics en su misión.

Figura 4. Pilares de la seguridad de la información

Fuente: http://www.inseguridadinformatica.com/2012/03/introduccion-la-seguridad-de-la.html

Bajo el marco de estos tres pilares, y de un par más como lo son la "autenticidad" y la "no repudiación", los cuales hacen referencia a que los sujetos intervinientes en la comunicación deben poderse identificar plenamente y además debe comprobarse que efectivamente son ellos quienes emiten o reciben la información; se han sentado las bases para la seguridad informática, pues a partir ellos se han elaborado normas técnicas que sugieren las directrices que se deben tener en cuenta en materia de seguridad informática, también han surgido metodologías, protocolos y

[7] MINTIC. (s.f.). *Ministerio de Tecnologias de la Informacion y las Comunicaciones*. Obtenido de Fortalecimiento de la gestion en el Estado: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html

guías de buenas prácticas, todas en pro de la seguridad informática y de la información[8].

Ahora bien, el punto de partida para la implementación de alguna de las herramientas tales como sistemas de gestión para seguridad de la información - SGSI, manuales y políticas de buenas prácticas en seguridad informática, etc., es la realización de un diagnostico que permita conocer el nivel de seguridad informática con que cuenta una entidad u organización, cuáles son sus riesgos asociados y si estos están controlados, además de cuáles son sus posibles amenazas o vulnerabilidades en materia de seguridad informática. Para lo anterior es pertinente la aplicación de metodologías, prácticas o herramientas que permitan establecer estos criterios y tomar las directrices necesarias, relacionadas con el objetivo de proteger la información y OSSTMM, es una de ellas.

Adicionalmente, es entendible que el hacking ético permite la implementación de estas herramientas de diagnóstico, posibilitando que, a través de esta actividad, sea posible establecer ese punto de partida, ese estado actual del nivel de seguridad informática, para lo cual es preciso exponer inicialmente algunos conceptos relacionados.

5.3.1 El Hacker

El primero de ellos es definir que un hacker, esta palabra fue acuñada en 1960, en el Instituto Técnico de Massachusetts - MIT y se relaciona con el sonido que hacían los aparatos telefónicos cuando eran golpeados para que "funcionaran". En un sentido más amplio, hacker es una persona con amplios conocimientos en informática y con capacidades para intervenir, alterar o modificar, productos, dispositivos tecnológicos o sistemas informáticos, con buenas o malas intenciones[9].

Existen principalmente dos tipos de hacker según sus intenciones, estos son los Hackers de Sombrero Blanco – White Hat Hacker y los Hackers de Sombrero Negro – Black Hat Hacker. Estos últimos, también denominados ciberdelincuentes, son hackers que realizan actividades ilícitas, explotando vulnerabilidades para acceder a información o medios no autorizados, con fines que pueden ir desde lo económico, hasta la mera satisfacción personal o incluso en actos de terrorismo.

---

[8] ALARCÓN SALVATIERRA, P. A., BARRIGA DÍAZ, R. A., & ALARCÓN SALVATIERRA, J. A. (2016). La Importancia de la Seguridad Informática en las Instituciones Gubernamentales. *Revista Caribeña de Ciencias Sociales - ISSN: 2257-7630*.

[9] MUÑOZ DE FRUTOS, A. (31 de octubre de 2015). *ComputerHoy*. Obtenido de ¿Qué es un hacker y qué tipos de hacker existen?: http://computerhoy.com/noticias/software/que-es-hacker-que-tipos-hacker-existen-36027

Ahora bien, centrándose en el concepto de White Hat Hacker, también denominado hacker ético, es una persona con igual nivel de conocimientos que un Black Hat Hacker, pero con un nivel moral y ético muy alto, con lo cual se enfoca en la búsqueda y análisis de vulnerabilidades para encontrar solución a las mismas, realizado tales actividades de búsqueda análisis de vulnerabilidades, a diferentes entidades y organizaciones, pero con el consentimiento de las mismas y con la finalidad de que las posibles vulnerabilidades encontradas puedan ser corregidas, logrando incrementar el nivel de seguridad informática de dichas entidades y organizaciones.

Dicho lo anterior, es posible entender que el hacking ético, contempla aquellas actividades encaminadas a encontrar y analizar vulnerabilidades en materia de seguridad de la informática, en las diferentes entidades y organizaciones, además contando con el conocimiento y aprobación de las mismas y con el propósito de que tales vulnerabilidades sean solucionadas en pro de la seguridad de la información[10].

5.3.2 Hacking Ético

En el campo del hacking ético, existen metodologías o marcos de trabajo, que permiten la ejecución y documentación de esta actividad, de una manera ordenada, algunas de estas metodologías son Open Source Security Testing Methodology Manual – OSSTMM o Manual de la Metodología Abierta de Testeo de Seguridad, Open Web Application Security Project – OWASP, enfocado a determinar y combatir las causas de inseguridad en el software, principalmente en aplicaciones web, e Information Systems Security Assessment Framework – ISSAF, el cual es un marco de trabajo enfocado en las practicas relacionadas a un testeo de seguridad.

5.3.3 OSSTMM

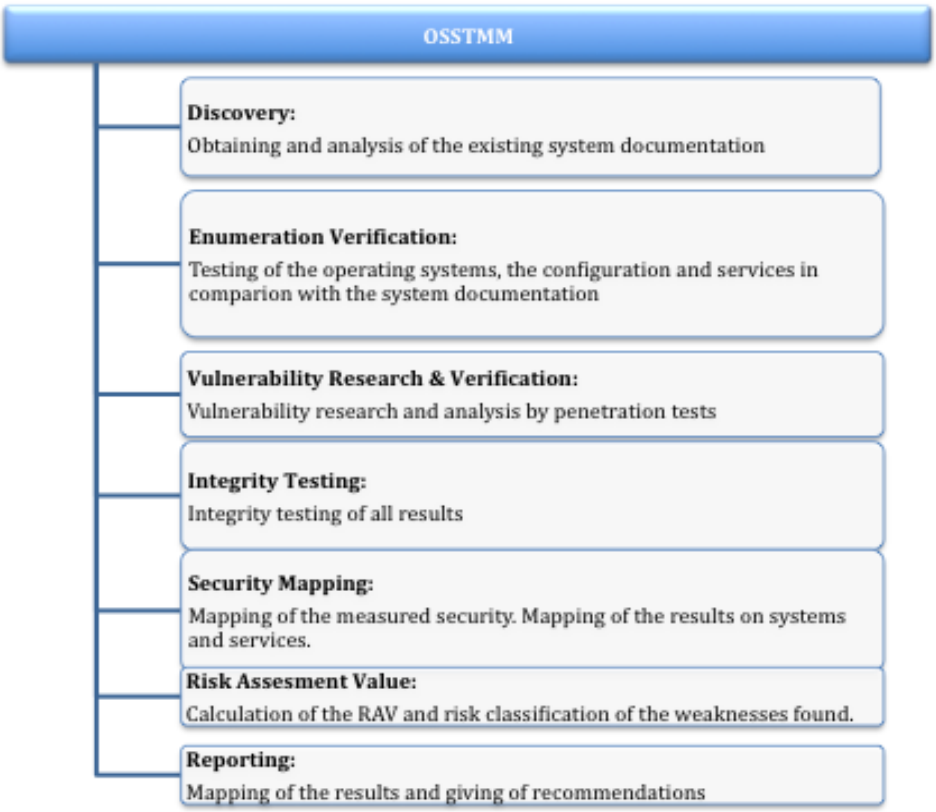
El Manual de la Metodología Abierta de Testeo de Seguridad u Open Source Security Testing Methodology Manual, es una metodología desarrollada por el Instituto para la Seguridad y Metodologías Abiertas o ISECOM, por sus siglas en inglés (Institute for Security and Open Methodologies), y fue publicada a finales del año 2000, lo cual marcó un hito pues hasta el momento no existían documentos que de manera abierta y estandarizada, agruparan las actividades a tener en cuenta, por parte de un profesional en seguridad informática, a la hora de realizar una

[10] CORONEL SUÁREZ, I. A. (2016). *Aplicar Hackeo Ético para Detección de Vulnerabildiades Mediante Herramientas Open Source en las Aplicaciones Web de una Institución de Educación Superior.* Obtenido de Escuela Superior Politecnica del Litoral: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/37397/D-103391.pdf

evaluación de seguridad[11]. Después de su publicación, ISECOM ha venido actualizando la metodología OSSTMM, hasta encontrarse en este momento en su versión 3.

Esta metodología, se basa en 7 grandes fases, las cuales se ilustran en Figura 5:

Figura 5. Fases OSSTMM



Fuente: *http://geekslinuxchile.blogspot.com.co/2015/09/categorizaciones-osstmm-pentesting.html*

Como se observa en la anterior imagen, las fases de OSSTMM, proporcionan una metodología que se encuentra totalmente alineada con lo expuesto en el capítulo **¡Error! No se encuentra el origen de la referencia.** de este documento, en donde

[11] RACCIATTI, H. M. (13 de diciembre de 2010). *Infosec Island*. Obtenido de Tiempos de Cambio: OSSTMM 3 - Una Introducción: http://www.infosecisland.com/blogview/10215-Tiempos-de-Cambio-OSSTMM-3-Una-Introduccin-.html

se hace una descripción más detallada de las fases de la metodología, las herramientas aplicables a cada fase y los resultados de la aplicación de estas.

A grandes rasgos, OSSTMM aborda las siguientes etapas:

- ✓ Obtener y analizar la información existente del sistema
- ✓ Testear los sistemas operativos, su configuración y servicios en comparación con la documentación del sistema
- ✓ Búsqueda de vulnerabilidades y análisis a través de test de penetración
- ✓ Realizar pruebas de integridad a todos los resultados
- ✓ Mapear los resultados de los sistemas y servicios evaluados
- ✓ Realizar Evaluación del Riesgo – RAV, para las debilidades encontradas
- ✓ Mapear los resultados y dar recomendaciones

Estas etapas tienen una correlación directa con las fases del hacking ético, así:

Tabla 2. Correlación entre Etapas del H.E. y Fases OSSTMM

Etapa H.E.	Fase OSSTMM
Planeación	- Obtener y analizar la información existente del sistema
Descubrimiento	- Testear los sistemas operativos, su configuración y servicios en comparación con la documentación del sistema
Ataque	- Búsqueda de vulnerabilidades y análisis a través de test de penetración - Realizar pruebas de integridad a todos los resultados
Reporte	- Mapear los resultados de los sistemas y servicios evaluados - Realizar Evaluación del Riesgo – RAV, para las debilidades encontradas - Mapear los resultados y dar recomendaciones

Fuente: el autor

Como se observa, la metodología OSSTMM propone un modelo de análisis y evaluación de vulnerabilidades de manera amplia y ordenada, que documenta los resultados y las recomendaciones en materia de seguridad informática, basado en todo el proceso realizado. Esto es lo que se pretende lograr con el presente proyecto, tener un análisis que permita a la Entidad, en este caso la Rama Judicial y en concreto a la Dirección Seccional de Administración Judicial de Armenia, tomar medidas y decisiones que propendan por la seguridad de la información que actualmente administra.

5.4 MARCO LEGAL

En Colombia, la normatividad relacionada con los delitos informáticos está tipificada en la ley 1273 de 2009. Esta ley realiza una modificación al Código Penal Colombiano, creando un nuevo bien jurídico tutelado el cual se denomina como "*de la protección de la información y de los datos*". Es a través de este que se habla sobre la preservación integral de los sistemas que hagan uso de tecnologías de la información y las comunicaciones[12].

Dicha ley, a través de sus 10 artículos, explica que puede ser considerado como un delito informático en Colombia y cuáles son las circunstancias de agravación punitiva relacionadas. De manera descriptiva, la ley está compuesta por los siguientes artículos:

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.*
Artículo 269C: *Interceptación de datos informáticos*.
Artículo 269E: *Uso de software malicioso*.
Artículo 269F: *Violación de datos personales*.
Artículo 269G: *Suplantación de sitios web para capturar datos personales*.
Artículo 269H: *Circunstancias de agravación punitiva*.
Artículo 269I: *Hurto por medios informáticos y semejantes*.
Artículo 269J: *Transferencia no consentida de activos*

Ahora bien, el hacking ético es una actividad que toca tangencialmente las prohibiciones expresas en la mencionada ley, con la diferencia de que se encuentra enmarcado por unas reglas y compromisos entre el hacker ético o pentester y la entidad a la cual se realizan las pruebas relacionadas, así las cosas, no existe un quebrantamiento de la ley, toda vez que existe un acuerdo de aceptación y confidencialidad que enmarca la realización de tal actividad.

Del mismo modo, en el año 2012 el Gobierno Nacional sancionó la Ley Estatutaria 1581, a través de la cual se dictan algunas disposiciones generales relacionadas con la protección de datos personales, definiendo como Dato personal “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”[13].

---

[12] LEY 1273 de 2009. (05 de enero de 2009). *Senad de la Republica.* Obtenido de Ministerio del Interior y de Justicia: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[13] LEY 1581. (17 de octubre de 2012). *Alcaldia de Bogotá*. Obtenido de Diario Oficial Alcaldia de Bogota: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Posteriormente, el 11 de abril de 2016 se publica el documento CONPES 3854, el cual establece la *Política Nacional de Seguridad Digital*. En dicho documento se habla sobre la seguridad y defensa de las entidades del Estado, contra posibles ataques cibernético, con un enfoque más preventivo que reactivo y basado en la gestión del riesgo en el entorno digital.

Como es posible observar, la anterior normativa descrita apalanca el proceso de realización de hacking ético a la infraestructura tecnológica de la Rama Judicial, entendiendo que esta Entidad debe garantizar la seguridad de la información almacenada y gestionada por sus sistemas de información, propendiendo por la protección de los datos personales y en alineación con el documento CONPES que se mencionó anteriormente.

6. DISEÑO METODOLOGICO

El presente trabajo está enfocado hacia la modalidad de *Proyecto Aplicado*, a través del cual se "permite al estudiante el diseño de proyectos para una trasferencia social de conocimiento que contribuya de manera innovativa a la solución de problemas focalizados"[14].

En cuanto a la metodología para la realización del presente proyecto, se basa en el Manual de la Metodología Abierta de Testeo de Seguridad, Open Source Security Testing Methodology Manual – OSSTMM[15].

6.1 METODOLOGÍA DE INVESTIGACIÓN

OSSTMM, es una metodología muy bien documentada, que a través de una correcta aplicación permite identificar las vulnerabilidades y debilidades en materia de seguridad informática que puedan presentarse en la Entidad, para este caso, la Rama Judicial, Dirección Seccional de Administración Judicial de Armenia, Quindío. Igualmente, con esta metodología es posible establecer causas para las vulnerabilidades identificadas. Lo cual ofrece unas bases consistentes que conllevan a la realización de las recomendaciones de seguridad pertinentes, de una manera objetiva y sustentada, lo cual redunda en la posibilidad de que la Rama Judicial establezca medidas y/o controles que impacten positivamente de seguridad informática, generando una mayor confianza en los usuarios y partes interesadas.

6.2 METODOLOGÍA DE DESARROLLO

El presente proyecto, se desarrolla a través de cuatro fases, que son: Planeación, Descubrimiento, Ataque, Reportes. Es a través de estas 4 fases que se pretende dar alcance y cumplimiento a los objetivos planteados en el presente proyecto. Estas cuatro fases, también conocidas como Planning, Discovery, Attack, and Reporting – PDAR, se encuentran alineadas con las fases del hacking ético[16].

---

[14] UNAD. (s.f.). *Universidad Nacionla Abierta y a Distancia - UNAD.* Obtenido de Alternativas para grado - ECBTI: https://academia.unad.edu.co/ecbti/oferta-academica/alternativas-para-grado

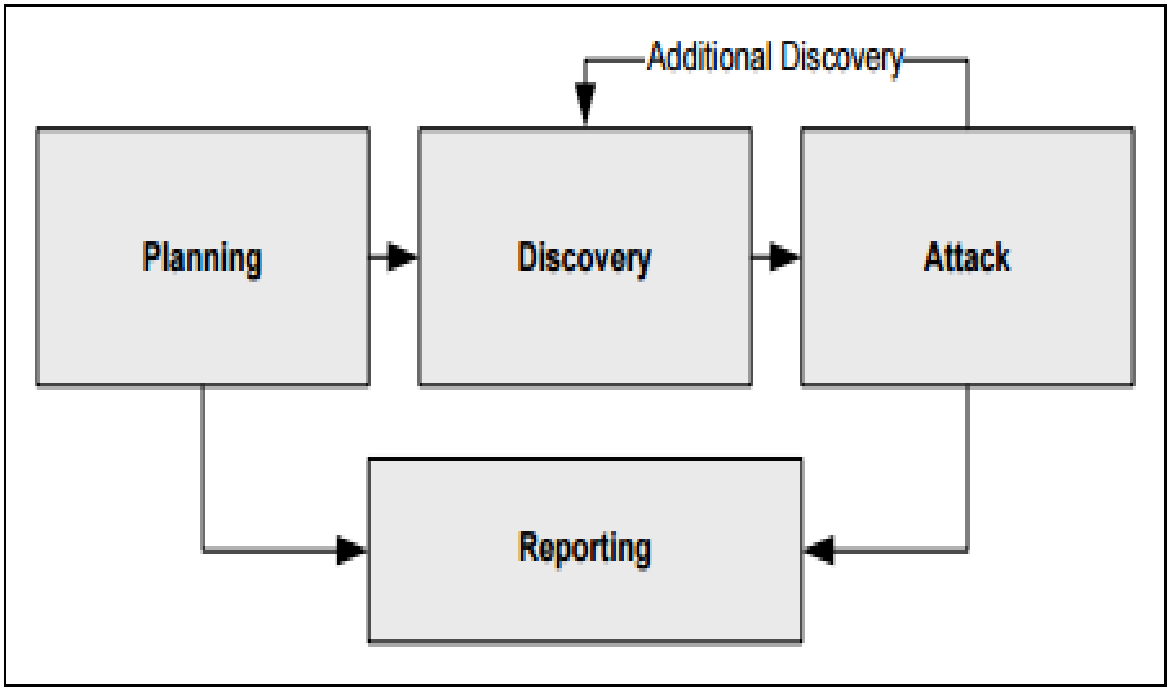
[15] JUNTA DE ANDALUCIA. (s.f.). *Marco de Desarrollo de la Junta de Andalucía*. Recuperado el 2017 de mayo de 20, de http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551

[16] NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY. (septiembre de 2008). *Technical Guide to Information Security Testing and Assessment*. Recuperado el 21 de mayo de 2017, de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

A continuación, se presenta una imagen que contiene un flujograma del PDAR (Planeación, Descubrimiento, Araque y Reportes), como se observa, su proceso inicial es la planeación y una vez culminada esta fase, es posible pasar a la fase de descubrimiento, para posteriormente continuar con el ataque, lo cual corresponde a la realización de las pruebas de penetración como tal; si durante esta fase se obtienen descubrimientos adicionales, estos deberán ser tratados como tal y realizar el ataque o explotación de los mismos, de ser pertinente. Todos los hallazgos obtenidos durante la fase de ataque deben ser documentados en los reportes destinados para tal fin.

A continuación, se presenta el flujograma de PDAR, según la NIST-SP 800-42

Figura 6. Flujograma PDAR



Fuente: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

En los siguientes párrafos, se presenta una descripción detallada de cada una de las fases que componen la presente metodología.

6.2.1 Planeación

En esta fase de define el alcance que tendrá el hacking ético, también se aprueba la realización de esta actividad y se establecen los acuerdos de confidencialidad.

Del lado del equipo de pruebas, se define la metodología a utilizar. Igualmente es necesario tener en cuenta las restricciones en cuanto a horarios y tiempos de pruebas y ataques, además de las restricciones legales que pueda requerir la Entidad.

6.2.2 Descubrimiento

La fase de descubrimiento es una de las fases más amplias en el proceso de hacking ético y es aquí donde empieza el trabajo recabando información sobre el objetivo a atacar. Se divide en 3 momentos:

- ✓ Footprinting
- ✓ Escaneo y enumeración
- ✓ Análisis de vulnerabilidades

6.2.2.1 Footprinting

Es la primera actividad que se debe realizar, es una tarea no intrusiva en donde se busca obtener el máximo de información sobre la organización y sus sistemas informáticos, componentes hardware y demás, aquí se aplican varias técnicas tales como:

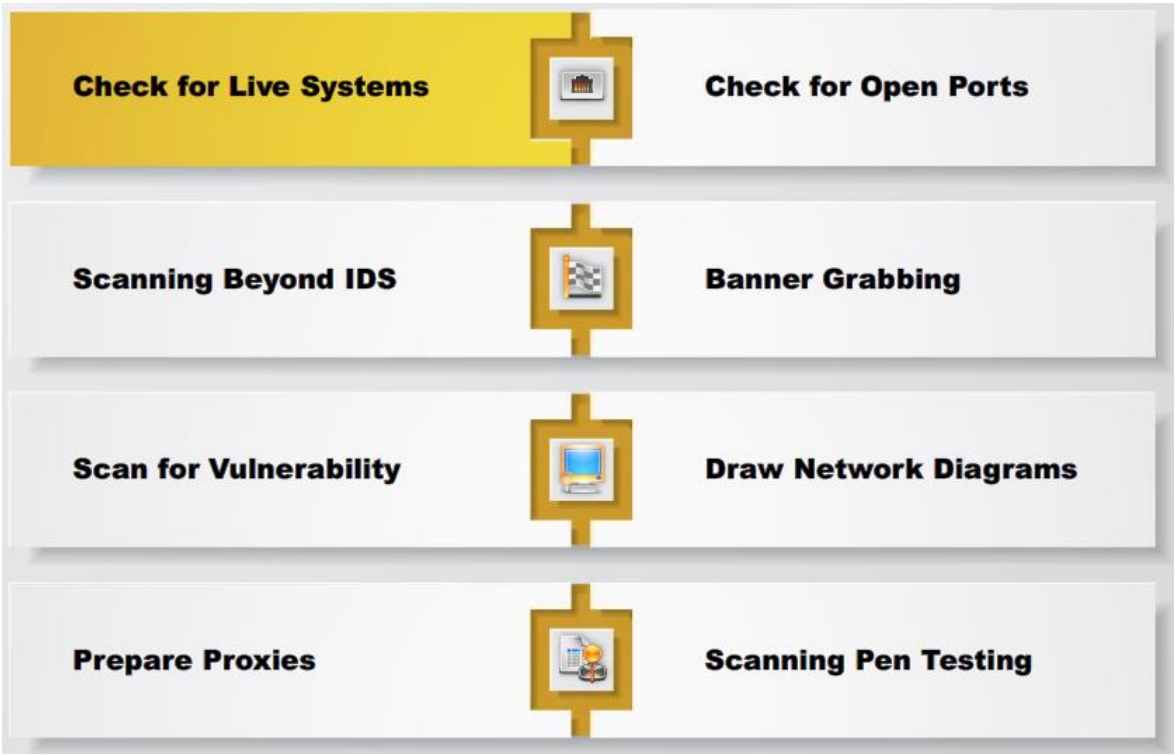
- Ingeniería Social
- Búsquedas avanzadas con Google
- Social Networking a través de sitios como LinkedIn, Twitter, Google plus, Facebook entre otros

6.2.2.2 Escaneo y enumeración

Durante esta etapa, se busca identificar sistemas activos, puertos abiertos y servicios activos y esto se realiza a través del escaneo de puertos, escaneo de redes y escaneo de vulnerabilidades.

En la siguiente imagen se observan los elementos a tener en cuenta durante el escaneo y la enumeración:

Figura 7. Elementos de Escaneo y Enumeración



Fuente: CEH V.9 Modulo Scanning Networks

Para la etapa de escaneo y enumeración existen se herramientas tales como Nmap, Angry IP Scanner, Hping, Xprof2, WinFingerprint, a través de las cuales es posible tener un primer acercamiento a lo que es la infraestructura y topología de red implementada por la Entidad, así como enumerar los puertos y servicios que se encuentran habilitados en los diferentes hosts que integran dicha red informática.

6.2.2.3 Análisis de vulnerabilidades

Una vez culminadas las etapas de escaneo y enumeración, es posible continuar con el análisis de vulnerabilidades, aquí se utilizan herramientas tales como Nessus, OpenVAS, Shadow Securtity Scanner, ISS Scanner. El funcionamiento de dichas herramientas se basa en inspeccionar los puertos y servicios habilitados en los distintos hosts de la red y realizar un análisis de vulnerabilidades, en comparación con las que se encuentran documentadas por el *Common Vulnerabilities and Exposures – CVE* y otras no documentadas pero conocidas. Estas son básicamente

debilidades en la configuración o implementación de servicios que se tienen implementados.

6.2.3 Ataque

Esta fase es el corazón de un hacking ético, es aquí donde toda la teoría se pone en práctica, donde la información recabada anteriormente se utiliza para explotar las vulnerabilidades encontradas y hackear los sistemas informáticos objetivo. Se divide principalmente en dos momentos:

- ✓ Explotación
- ✓ Elevación de privilegios

6.2.3.1 Explotación

En esta fase se explotan las vulnerabilidades encontradas anteriormente, para ello se hace uso de exploits que pueden ser buscados en una base de datos de estos o crear scripts que permitan realizar esta explotación. Es recomendable que el o los encargados de realizar esta fase, tengan conocimientos en lenguajes de scripting como lo son Phyton, Pearl o incluso Ruby.

Es necesario que esta fase se ejecute muy cuidadosamente, siendo pertinente determinar cuáles vulnerabilidades se van a comprobar a través de los diferentes exploits, pues algunos podrían afectar los sistemas que se encuentren en producción o que la Entidad pueda considerar críticos para su operación, e incluso llegar generar fallos que puedan poner en riesgo la disponibilidad de servicios ofrecidos por la Rama Judicial.

Existen bases de datos donde se pueden encontrar exploits los cuales se encuentran listos para ejecutar, aunque es altamente recomendad realizar pruebas de los exploits que se pretenden utilizar, en un ambiente controlado o de pruebas, antes de ejecutarlos la infraestructura en producción. Algunas de esas bases de datos de exploits son:

https://www.exploit-db.com/
http://www.hack0wn.com/
https://es.0day.today/

Igualmente existen marcos de trabajo o aplicaciones que permiten realizar estas tareas de explotación, tales como: Metasploit, Core Security, Immunity CANVAS, Exploit Pack, Armitage, Nexpose[17]. A traves de estos frameworks es posible facilitar

[17] ALTERNATIVE TO. (s.f.). *Crowedsourced Software Recomendations - Alternatives to Metasploit*. Recuperado el 21 de mayo de 2017, de http://alternativeto.net/software/metasploit-community-edition/

la explotación de ciertas vulnerabilidades, toda vez que contienen o permiten implementar los scripts que vulneran las debilidades encontradas, pudiendo confirmar la existencia de las mismas.
En ocasiones, algunos de estos exploits deben ejecutarse con privilegios elevados y es allí donde interviene la siguiente fase:

6.2.3.2 Elevación de Privilegios

En esta fase, el hacker o tester, debe adquirir un nivel de acceso que le permita realizar las actividades pertinentes, en este proceso ser necesario la utilización de software o ciertas herramientas que le permitan escalar privilegios de manera que pueda realizar su labor sin restricciones.

La elevación de privilegios no siempre se da a nivel de usuarios, a veces se da a niel de máquinas, cuando se utiliza una maquina como pivote, para poder acceder a otras, esto se conoce como *Daisy Chaining*

6.2.4 Reporte

Esta es la última etapa del proceso de hacking ético, en ella se registran todas las actividades desarrolladas, las vulnerabilidades encontradas y se realizan recomendaciones para solucionar estas vulnerabilidades y que contramedidas se pueden tomar.

Es recomendable guardar registro de las acciones realizadas, durante las fases anteriores (planeación, descubrimiento y ataque) esto ayuda a la construcción del reporte final.

El reporte debe contener aspectos técnicos de las tareas realizadas, en un lenguaje general que pueda entender la gerencia de la organización, además debe contener como mínimo, los siguientes elementos:

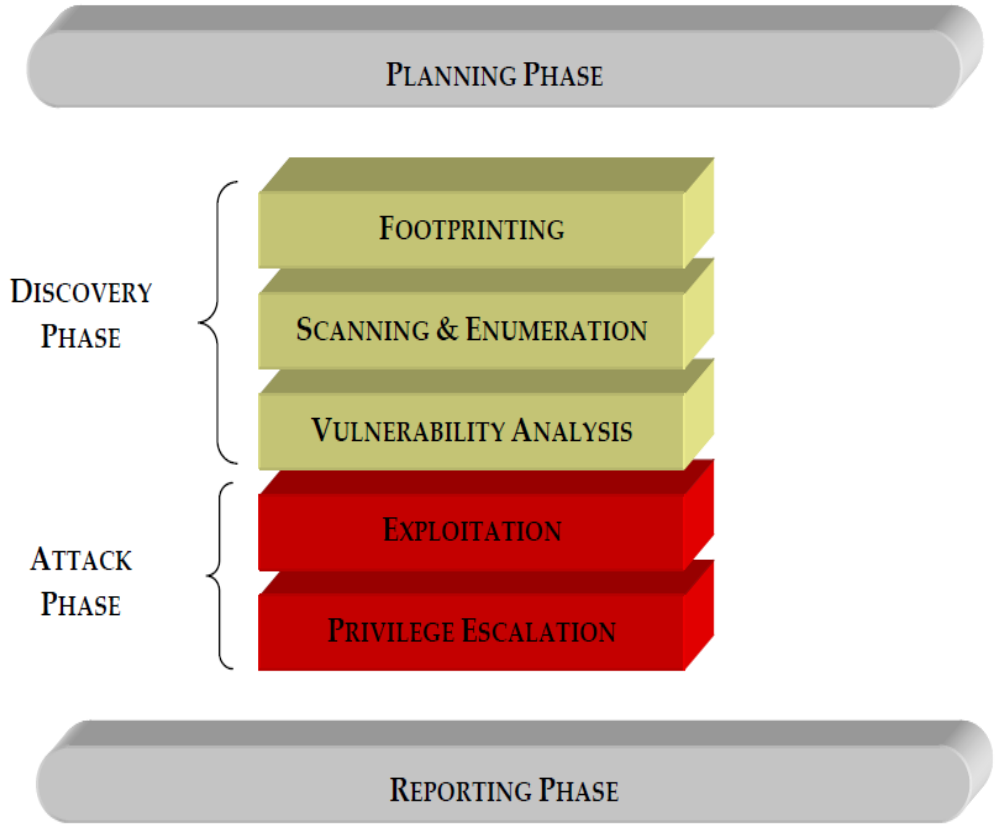
- Resumen ejecutivo
- Resultados detallados de las actividades realizadas
- Valoración vulnerabilidades encontradas (Nivel de riesgo)
- Impacto sobre la organización
- Recomendaciones

Es necesario mencionar, que OSSTMM cuenta con unas herramientas que permiten realizar la valoración de los niveles de riesgo a través de aplicaciones matemáticas,

que permiten no solo cualificar sino cuantificar tales niveles, para poder generar una evaluación en nivel de cumplimiento, en cuanto a seguridad informática se refiere.

De manera gráfica, las fases del presente proyecto pueden observarse a continuación, en Figura 8

Figura 8. Fases del proyecto



Fuente: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

6.3 UNIVERSO

El universo del presente proyecto corresponde a todos los activos de información con que cuenta la Dirección Ejecutiva Seccional de Administración Judicial de Armenia, los procesos, procedimientos y políticas relacionadas con la seguridad de la información de la Entidad.

6.4 MUESTRA

La muestra para el presente proyecto corresponde a los activos de información que sean considerados como críticos o de mayor relevancia, para la Entidad

6.5 FUENTES DE RECOLECCIÓN DE INFORMACIÓN

La información se recolecta a través de la observación directa, entrevistas y los informes y resultados que arrojen las herramientas de auditoria, escaneo, enumeración y análisis de vulnerabilidades empleadas durante el desarrollo del presente proyecto.

7. APLICACIÓN DE OSSTMM

Como ya se explicó, *Open Source Security Testing Methodology Manual – OSSTMM*, es una metodología que permite evaluar la seguridad operacional – OpSec (Operational Security), sobre diferentes factores como lo son el humano, físico, inalámbrico, telecomunicaciones, redes de datos y otros vectores, adaptados a auditorias de tipo pentesting y hacking ético, entre otros.

7.1 DEFINIENDO EL HACKING ÉTICO

OSSTMM, plantea la revisión de los siguientes 7 pasos para el establecimiento de la prueba de seguridad, en este caso del hacking ético.

7.1.1. Controles

Dentro de los controles a testear en el presente hacking ético, se definen los siguientes:

Autenticación: este control, que se encuentra enfocado en desafiar las credenciales de acceso a los diferentes activos y sistemas de información, a través de la ***identificación*** y la ***autorización***.

Subyugación: este control asegura que las actividades, acciones o interacciones sobre los activos y/o sistemas de información de la Rama Judicial, solo se realizan a través de los procedimientos establecidos para tal fin.

Continuidad: este control es sobre las acciones que permiten mantener los sistemas operativos, en caso de corrupción o falla.

No Repudiación: a través de este control se asegura que los actores de los sistemas de información de la Rama Judicial no pueden negar la ejecución de las diferentes actividades que ejecutan sobre dichos sistemas.

Confidencialidad: es un control para asegurar que un activo exhibido o intercambiado entre partes que interactúan no puede ser conocido fuera de esas partes.

Privacidad: es un control para asegurar que un recurso que se accede se muestra o se intercambia entre las partes no puede ser conocido fuera de esas partes.

Integridad: es un control para asegurar que las partes interactuantes sepan cuándo los activos y los procesos han cambiado

Los controles de ***indemnización***, ***resiliencia*** y ***alarma*** no serán tenidos en cuenta durante el presente hacking ético, puesto que algunos de ellos van asociados a la normatividad legal de la entidad que no está incluida dentro del alcance del presente proyecto, además que su testeo puede afectar la prestación del servicio de justicia.

7.1.2. Zona de compromiso

Esta ***engagement zone***, es un área alrededor de los activos de información que incluye los mecanismos de protección y los procesos o servicios construidos alrededor de los mismos.

7.1.3. Alcance del Hacking Ético

Dentro del alcance del presente hacking ético, se establece que el mismo se realiza a la organización que se describe a continuación:

Razón social: Dirección Ejecutiva Seccional de Administración Judicial de Armenia
Dirección: Carrera 12 # 20 - 63 Palacio de Justicia "Fabio Calderón Botero", Piso 3º Oficina 335T, Armenia, Quindío.
Teléfono: (+6) 741 47 13
Responsable: Julián Ochoa Arango
Cargo: Director Ejecutivo Seccional de Administración Judicial
Sede: Palacio de Justicia ***Fabio Calderón Botero***

La Dirección Ejecutiva Seccional de Administración Judicial, es un órgano administrativo y de gestión de recursos que hace parte de la Rama Judicial, el cual no ejerce ninguna actividad comercial, su enfoque es hacia el servicio, en este caso gestionar y administrar recursos físicos, tecnológicos, financieros y humanos, al servicio de los despachos judiciales y administrativos que componen el Distrito Judicial de Armenia[18]

7.1.4. Vectores

El presente hacking ético se realiza vectorizado de adentro hacia adentro, pues actualmente se cuenta con acceso, aunque limitado, a la infraestructura tecnológica de la Entidad. Igualmente, es pertinente realizar pruebas externas, pero buscando alcanzar o acceder a la infraestructura de la Dirección Ejecutiva Seccional de

[18] UNIDAD DE DESARROLLO Y ANÁLISIS ESTADÍSTICO - RAMA JUDICIAL. (2017). *Documento para la Elaboración del Contexto Institucional de la Rama Judicial.* Bogotá D.C.: UDAE.

Administración Judicial de Armenia, Quindío y no otras infraestructuras localizadas en otras ciudades o incluso en el nivel central (Bogotá).

La realización de las pruebas únicamente requiere del uso de computadores y herramientas relacionadas con la seguridad informática. Ningún otro tipo de hardware o equipos es requerido

7.1.5. Canales

Los canales son los medios a través de los cuales serán probados los vectores, para este Hacking Ético, los canales se definen en la siguiente tabla:

Tabla 3. Canales a testear

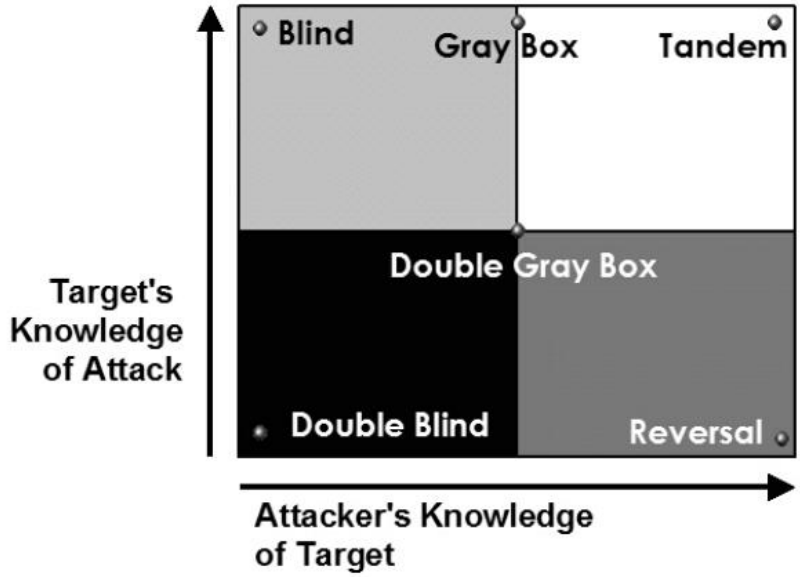
Clase	Canal	Descripción
Seguridad Física (Physical Security - PHYSSEC)	Humano	Comprende los factores humanos, en donde la interacción es física o posológica
	Físico	Es de naturaleza física y no electrónica. Comprende lo tangible de la seguridad donde la interacción requiere esfuerzo físico
Seguridad del Espectro (Spectrum Security – SPECSEC)	Redes inalámbricas	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético
Seguridad de Comunicaciones (Communications Security - COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicaciones, digitales o analógicas
	Redes de Datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción tiene lugar a través de cable

Fuente: Allen David Zuluaga Mateus

7.1.6. Tipo de Hacking Ético

OSSTMM tiene definidas 6 tipos de prueba, basadas en la cantidad de información que el tester, en este caso el hacker ético, conoce en cuanto a los objetivos o superficie de ataque y cuanto conoce la organización o Entidad, sobre el hacking ético a realizarse. Esto se observa en la siguiente imagen:

Figura 9. Tipos de hacking ético



Fuente: OSSTMM Cap. 2.3

El hacking ético a la Rama Judicial se realiza de acuerdo con lo establecido en las pruebas de doble caja gris o también conocidas como pruebas de caja blanca, aquí el hacker tiene un conocimiento limitado de las defensas de la Entidad y un pleno conocimiento de los canales. Igualmente, la Rama Judicial y el encargado de administrar la infraestructura tecnológica de dicha entidad, conocen el alcance y el plazo del ejercicio de Hacking Ético, pero no de los calanes probados ni vectores de prueba utilizados.

7.1.7. Reglas y Compromisos del Hacking Ético

Estas reglas definen las directrices de la realización de pruebas y manejo de los resultados de las mismas.

Lo anterior se encuentra definido en el ANEXO 3: Reglas y compromisos del hacking ético.

8. RESULTADOS

8.1 FASE DE PLANEACIÓN

8.1.1 Autorización para realización del hacking ético

El momento inicial para la planeación, parte de la aprobación o autorización, por parte de la organización a auditar u organización objetivo, para la realización de las actividades relacionadas con el hacking ético, en este caso, el Director Ejecutivo Seccional de Administración Judicial, aprueba dicha actividad, mediante oficio evidenciable en el 1ANEXO 2: Autorización a solicitud autorización hacking ético

8.1.2 Plan de pruebas

Este documento, se elabora de manera consensuada entre el tester y la organización, en este caso entre el tesista y la Rama Judicial, dicho documento contiene entre otros elementos

- ✓ La fecha de inicio y la duración
- ✓ El tipo de test
- ✓ El alcance
- ✓ La metodología a utilizar (canales, vectores y controles)
- ✓ Restricciones o limitaciones
- ✓ Acuerdo de confidencialidad

Dicho plan de pruebas se encuentra disponible en el ANEXO 4: Plan de pruebas.

8.2 FASE DE DESCUBRIMIENTO

8.2.1 Entrevista al coordinador de soporte tecnológico

Como primera etapa para recabar información, se realiza entrevista al Ingeniero Alexander Moreno Rojas, coordinador de soporte tecnológico de la Entidad, a fin de conocer de primera mano, el estado de la infraestructura tecnológica y de seguridad de la información de la Entidad.

Entrevista al Ing. Alexander Moreno Rojas.
Coordinador de soporte tecnológico de la Entidad
Realizada el 27/11/2017

¿Posee la Rama Judicial un documento que contenga las políticas de seguridad de la información?
RNo, no contamos con ese documento, sin embargo, existe una Unidad de Informática en el Nivel Central, en Bogotá, la cual se encarga de tomar las decisiones en materia de infraestructura tecnológica para la rama judicial; son ellos quienes elaboran los planes y programas que luego se hacen extensivos a las demás seccionales como la nuestra.
Existe un documento, que no tiene fecha de elaboración, pero que conozco hace más de 5 años, este documento contiene las directrices para hacer el nombramiento de máquinas, la generación de nombres de usuario y recalca la importancia de la realización de las copias de seguridad, pero dicho documento nunca se ha actualizado.

¿Se ha realizado un análisis de riesgo a la infraestructura tecnológica?
RSi, en nuestro Sistema de Gestión de Calidad, existe un proceso denominado "Gestión tecnológica" el cual tiene como objetivo administrar y mantener los recursos informáticos y de comunicaciones.
En el marco de dicho sistema de gestión de calidad, se analizan anualmente los riesgos que puedan impactar el cumplimiento de tal objetivo.

¿Cuántas aplicaciones se tienen consideradas críticas para cumplir los objetivos de la Entidad?
R1, contamos con un sistema de información denominado justicia XXI, el cual está integrado por varios módulos que se instalan según el tipo de despacho o dependencia, esto de acuerdo con las necesidades del servicio.
Justicia XXI es un sistema de información en ambiente cliente-servidor.

¿Qué sistemas operativos utiliza en sus servidores?
REn todos nuestros servidores corren sistemas operativos Windows Server, en alguna versión 2003 y en otra versión 2008 r2

¿Qué motor de Bases de datos se utiliza?
RNuestro motor de base de datos es SQL Server 2005

¿Cuántos usuarios se tienen en la red tanto LAN?
RActualmente tenemos en Armenia, 3 sedes judiciales interconectadas y con acceso al sistema de información Justicia XXI.
En la sede Edificio Cervantes hay aproximadamente 180 usuarios, en la sede Edificio Bolívar, son aproximadamente 120 usuarios y en el Palacio de Justicia estamos cerca de los 450 usuarios.

¿Por favor indique las marcas de dispositivos utilizados en la red?
RLos equipos activos de nuestra red son de marcas Lucent, HP y Cisco.

¿Cuentan con estándares de configuración, es decir todos los equipos están configurados con cierta uniformidad?
RHay un estándar para el nombramiento de equipos y también para la creación de usuarios en el directorio activo. Esto se ve afectado en la práctica debido a la alta rotación de personal.

¿Tienen procedimientos para la realización de actividades criticas relacionadas con TI? (Generación de copias de seguridad, ataques informáticos, continuidad del negocio, planes de contingencia)
RNo, no existen tales procedimientos

¿Se ha realizado algún estudio referente a planes de continuidad del negocio, recuperación ante desastres o planes de contingencia?
RNo, nunca se han realizado tales estudios.

¿Con qué elementos de seguridad de la información cuenta la Entidad?
RContamos con un firewall a nivel de hardware, el cual es administrado por el Nivel Central.
A nivel seccional contamos con consolas de antivirus en cada sede judicial a fin de asegurar que la actualización de los sistemas antivirus se haga a través de la LAN y no tengan que salir a Internet los equipos.
Igualmente contamos con un servidor WSUS (Windows Server Update Services) para proveer las actualizaciones de seguridad para los sistemas operativos.

8.2.2 Clasificación de activos de información

Otra actividad que se adelanta en esta fase de descubrimiento es realizar un levantamiento y clasificación de los activos de información, esto servirá para orientar las pruebas hacia los objetivos correctos, en donde los resultados del Hacking Ético generen un mayor valor agregado a la Entidad. La clasificación de los activos relevantes se hace conforme a lo establecido en la metodología MAGERIT. Es necesario aclarar que la metodología permite realizar una aproximación iterativa, aplicando la metodología de una manera amplia y posteriormente con base en las revisiones, entrar en más detalles[19].

A continuación, se presentan una serie de tablas que corresponden a la clasificación de los activos de información existentes en la Entidad, conforme a lo establecido en el catálogo de elementos de la metodología MAGERIT.

[19] MAGERIT. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En M. d. Públicas, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* (pág. 13). Madrid: Subdirección General de Información, Documentación y Publicaciones.

Activos Esenciales

Tabla 4. Codificación de los activos esenciales

Código Grupo de Activo	Nombre Grupo de Activo	Código Rama Judicial	Nombre Rama Judicial
[vr] [A] [R]	Datos vitales, de alto carácter personal, con difusión limitada	JXXI_Info	Datos almacenados en los sistemas de información de la Entidad, para la gestión judicial
[service]	servicio	KACTUS_Info	Datos almacenados en el sistema de información, para gestión RRHH
[service]	servicio	SICOF_Info	Datos almacenados en el sistema de información, para gestión inventarios
[service]	Servicio	MPLS_1	Servicio de internet MPLS que interconecta las diferentes sedes judiciales

Fuente: Allen David Zuluaga Mateus

[D] Datos/Información

Tabla 5. Codificación de los datos e información

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
D01	[files]	Ficheros	DB_Consejo	Archivo de base de datos del Sistema Justicia XXI
D02	[files]	Ficheros	DB_SARJ	Archivo de base de datos del Sistema Automatizado de Reparto Judicial
D03	[files]	Ficheros	DB_Titulos	Archivo de base de datos del Sistema Justicia XXI, módulo de depósitos judiciales
D04	[files]	Ficheros	ARCH_Financiera	Archivos con información financiera y presupuestal de la Entidad
D05	[files]	Ficheros	ARCH_Contratos	Archivos con información relacionada con la contratación de la entidad
D06	[conf]	Datos de configuración	CONF_JXXI	Archivos con la configuración del sistema de información Justicia XXI
D07	[backup]	Copias de respaldo	BK_JXXI	Archivo de copia de seguridad del servidor JXXI
D08	[backup]	Copias de respaldo	BK_Cervantes	Archivo de copia de seguridad del servidor Cervantes
D09	[backup]	Copias de respaldo	BK_Audiencias	Copias de seguridad de las audiencias realizadas
D10	[log]	Registro de actividad	LOG_Palacio	Registros de actividad en sistemas de información del Palacio de Justicia
D11	[log]	Registro de actividad	LOG_Cervantes	Registros de actividad en sistemas de información del edificio Cervantes

Fuente: Allen David Zuluaga Mateus

[K] Claves criptográficas

Tabla 6. Codificación MAGERIT de las claves criptográficas

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
K01	[x509]	Certificados de clave publica	TOKEN_Finan	Certificados para la firma digital en el Sistema Integrado de Información Financiera

Fuente: Allen David Zuluaga Mateus

[S] Servicios

Tabla 7. Codificación MAGERIT de los servicios

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
S01	[www]	World Wide Web	INTERNET	Servicio de internet para los servidores judiciales y usuarios en los terminales de consulta
S02	[email]	Correo electrónico	EMAIL	Servicio de correo electrónico institucional para todos los servidores judiciales
S03	[file]	Almacenamiento de ficheros	STORAGE	Sistema de almacenamiento y custodia de archivos en datacenter

Fuente: Allen David Zuluaga Mateus

[SW] Software y aplicaciones

Tabla 8. Codificación MAGERIT de software y aplicaciones

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
SW01	[sub]	Desarrollo a la medida	JXXI	Sistema de información Justicia XXI
SW02	[prp]	Desarrollo propio	JXXIWEB	Sistema de información Justicia XXI Web
SW03	[sub]	Desarrollo a la medida	KACTUS	Sistema de gestión de RRHH
SW04	[sub]	Desarrollo a la medida	SICOF	Sistema de gestión de inventarios
SW05	[std] [dbms]	Sistema de Gestión de Base de Datos	SQL	SGBD SQL Server para Justicia XXI

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
SW06	[std] [dbms]	Sistema de Gestión de Base de Datos	MySQL	SGBD MySQL Server para el sistema de gestión de turnos
SW07	[std] [office]	Ofimatica	MSOFFICE	Microsoft Office 2013
SW08	[std] [av]	Anti virus	NOD	ESSET NOD32 Antivirus 4
SW09	[std] [os]	Sistema operativo	WIN8	Windows 8.1
SW10	[std] [os]	Sistema operativo	WINSERV2003	Windows Server 2003 SE
SW11	[std] [os]	Sistema operativo	WINSERV2008	Windows Server 2008 R2
SW12	[std] [hypervisor]	Gestor de máquina virtual	HYPERV	Hyper-V Microsoft rol

Fuente: Allen David Zuluaga Mateus

[HW] Hardware - Equipos Informáticos

Tabla 9. Codificación MAGERIT de equipos informáticos

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
HW01	[host]	Servidor de aplicaciones	DIRACT	Servidor para el Active Directory Domain Services
HW02	[host]	Servidor de aplicaciones	JXXI	Servidor para el despliegue del sistema de información justicia XXI
HW03	[host]	Servidor de aplicaciones	ARMENIA2	Servidor para el despliegue del WSUS, consola de antivirus local
HW04	[host]	Servidor de aplicaciones	SERVPALACIO	Servidor para del sistema de gestión de turnos y sistema de salas de audiencia
HW05	[pc]	Informática personal	PCUSER	Equipos de cómputo para usuarios
HW06	[vhost]	Equipo virtual	PCVIRTUAL	Máquina virtual Ubuntu server para el sistema de gestión de turnos
HW07	[peripheral] [print]	Medios de impresión	IMPRE	Impresoras
HW08	[peripheral] [print]	Escáneres	ESCAN	Escáneres
HW09	[network] [switch]	Conmutadores	SWITCH01	Switch Force10
HW10	[network] [switch]	Conmutadores	SWITCH02	Switch HP
HW11	[network] [router]	Enrutadores	ROUTER	Router Cisco 2800 Series
HW12	[network] [wap]	Punto de acceso inalámb.	WIFI	Access Point inalámbrico

Fuente: Allen David Zuluaga Mateus

[COM] Redes de comunicaciones

Tabla 10. Codificación MAGERIT de redes de comunicaciones

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
COM01	[PSTN]	Red telefónica	TELEFONIA	Red de telefonía análoga
COM02	[wifi]	Red inalámbrica	WIFISIID	Red inalámbrica para servidores judiciales
COM03	[LAN]	Red local	LAN	Red LAN de la Rama Judicial, Palacio de Justicia
COM04	[Internet]	Internet	Internet	Red de Internet MPLS

Fuente: Allen David Zuluaga Mateus

[Media] Soportes de Información

Tabla 11. Codificación MAGERIT de soportes de información

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
Media01	[electronic] [vdisk]	Discos virtuales	VDISK	Disco duro virtual VHD para máquina virtual Linus Ubuntu server
Media02	[electronic] [cd]	CD – ROM	CD	CDs
Media03	[electronic] [dvd]	DVD	DVD	DVDs
Media04	[electronic] [tape]	Cinta magnética	TAPEBK	Tape Back UP para generación de copias de seguridad
Media05	[non_electronic] [printed]	Material impreso	PROCESOS	Procesos Judiciales
Media06	[non_electronic] [printed]	Material impreso	HDV	Hojas de Vida
Media07	[non_electronic] [printed]	Material impreso	CONTRATOS	contratos

Fuente: Allen David Zuluaga Mateus

[AUX] Equipamiento auxiliar

Tabla 12. Codificación MAGERIT de equipos auxiliares

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
AUX01	[ups]	Sistemas de alimentación ininterrumpida	UPS01	UPS TripLite 40KVA

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
AUX02	[ups]	Sistemas de alimentación ininterrumpida	UPS02	UPS PowerCom 2KVA
AUX03	[ups]	Sistemas de alimentación ininterrumpida	UPS03	UPS ASTEI 10KVA
AUX04	[gen]	Generadores eléctricos	PLANTA	Planta generadora de energía
AUX05	[ac]	Equipos de climatizacino	AC	Aires acondicionados
AUX06	[cabling] [wire]	Cable eléctrico	CABLE	Cableado estructurado
AUX07	[cabling] [fiber]	Fibra Óptica	FIBRA	Enlaces de fibra óptica entre centros de cableado

Fuente: Allen David Zuluaga Mateus

[L] Instalaciones

Tabla 13. Codificación MAGERIT de instalaciones

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
L01	[building]	Edificio	PALACIO	Palacio de Justicia *Fabio Calderón Botero*

Fuente: Allen David Zuluaga Mateus

[P] Personal

Tabla 14. Codificación MAGERIT para el personal

Código	Código Grupo de Activo MAGERIT	Nombre Grupo de Activo MAGERIT	Código Rama Judicial	Nombre Rama Judicial
P01	[ue]	Usuarios externos	USUARIOS	Usuarios del sistema de justicia
P02	[ui]	Usuarios internos	SERVIDOREJ	Funcionarios y empleados judiciales
P03	[adm]	Administradores de sistemas	ADMIN	Administrador de los sistemas informáticos de la Rama Judicial
P04	[com]	Administradores de comunicaciones	ADMINCOM	Administrador de los sistemas informáticos de telecomunicaciones de la Rama Judicial
P05	[dba]	Administradores de DDBB	ADMINDB	Administrador de los sistemas informáticos de bases de datos de la Rama Judicial
P06	[prov]	Proveedores	PROVEEDOR	Proveedores de la Rama Judicial

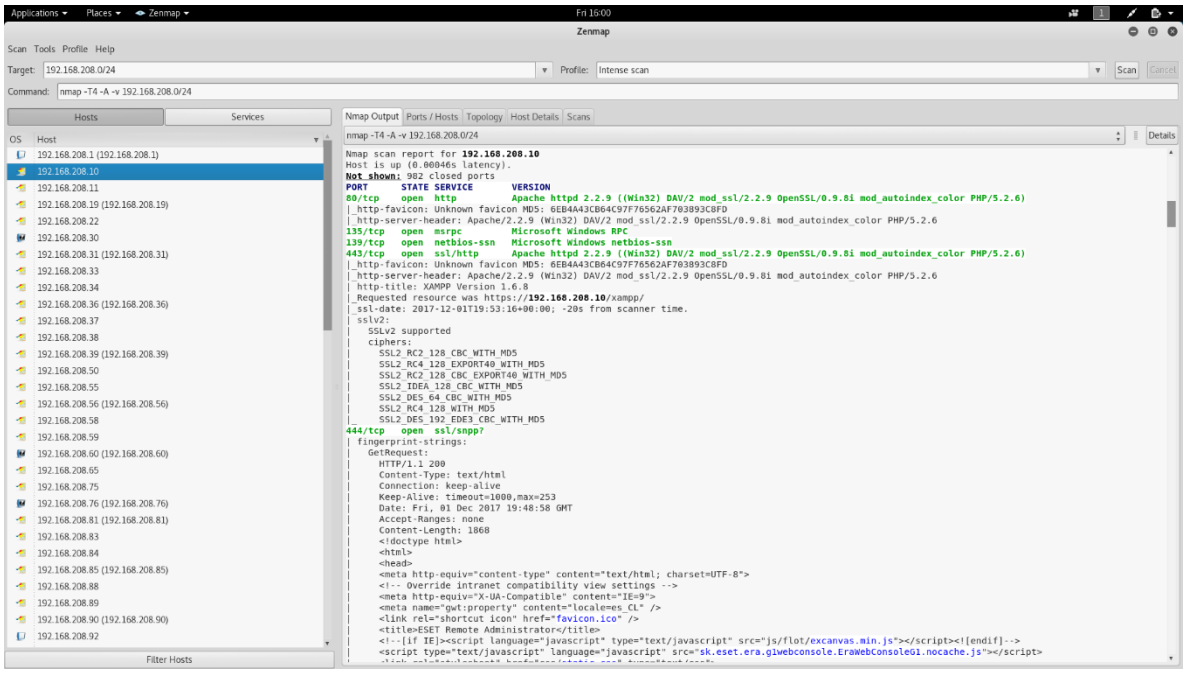
Fuente: Allen David Zuluaga Mateus

8.2.3 Escaneo y enumeración

Se procede a realizar un escaneo de host y puertos abiertos en la red 192.168.208.0/24 con el fin de identificar algún sistema o servicio critico o de valor importante, los resultados de dicho escaneo se encuentran disponibles en el ANEXO 5: Resultados escaneo con Nmap.

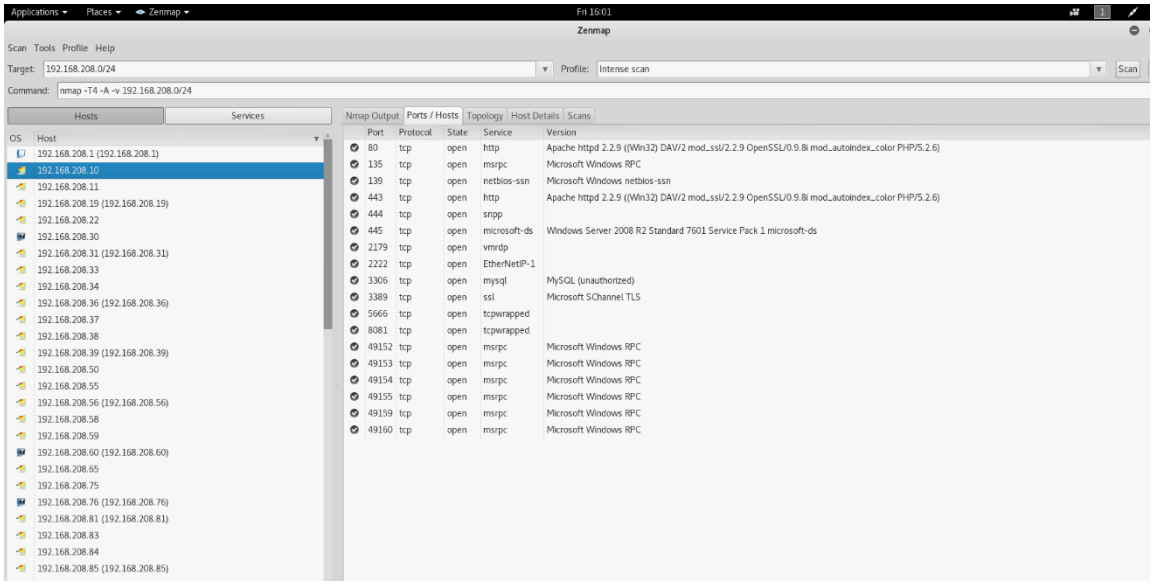
El escaneo se realiza a través de la herramienta Zenmap, que corresponde a la GUI o interface gráfica de Nmap. Dicho escaneo arroja como resultado que prácticamente todos los host tienen los mismos servicios habilitados, a excepción del host 192.168.208.10 que cuenta con otros servicios tales como apache, mysql, php, tal como se observa en la siguiente imagen:

Figura 10. Escaneo con Zenmap



Fuente: Allen David Zuluaga Mateus

Figura 11. Puertos abiertos en 192.168.208.10



Fuente: Allen David Zuluaga Mateus

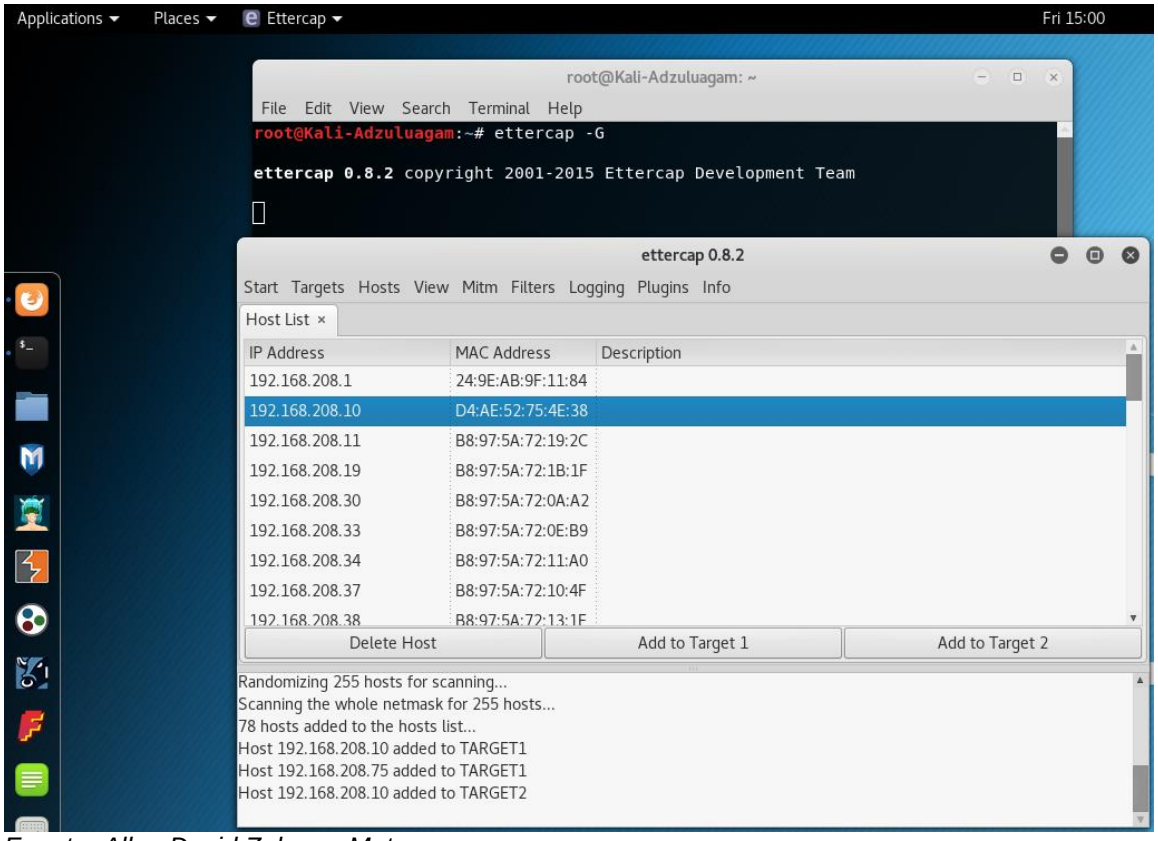
8.3 FASE DE ATAQUE

8.3.1 Ataque MiTM a 192.168.208.10

Después de analizar con wireshark el tráfico de red hacia la IP 192.168.208.10, se determina que una de las IP que más solicitudes realiza a dicho host es la 192.168.208.75, por lo cual se implementa un ataque de ARL Spoofing y ataque de hombre en el medio, a través de la aplicación Ettercap, con el fin capturar información entre ambas maquinas.

Se prepara el ataque con la aplicación Ettercap, con objetivos 192.168.208.10 y 192.138.208.75. Se selecciona la IP 192.168.208.75 como el *Target* 1 y la IP 192.168.208.10 como el *Target 2,* tal como se muestra en la siguiente imagen:

Figura 12. Agregando objetivos del ataque

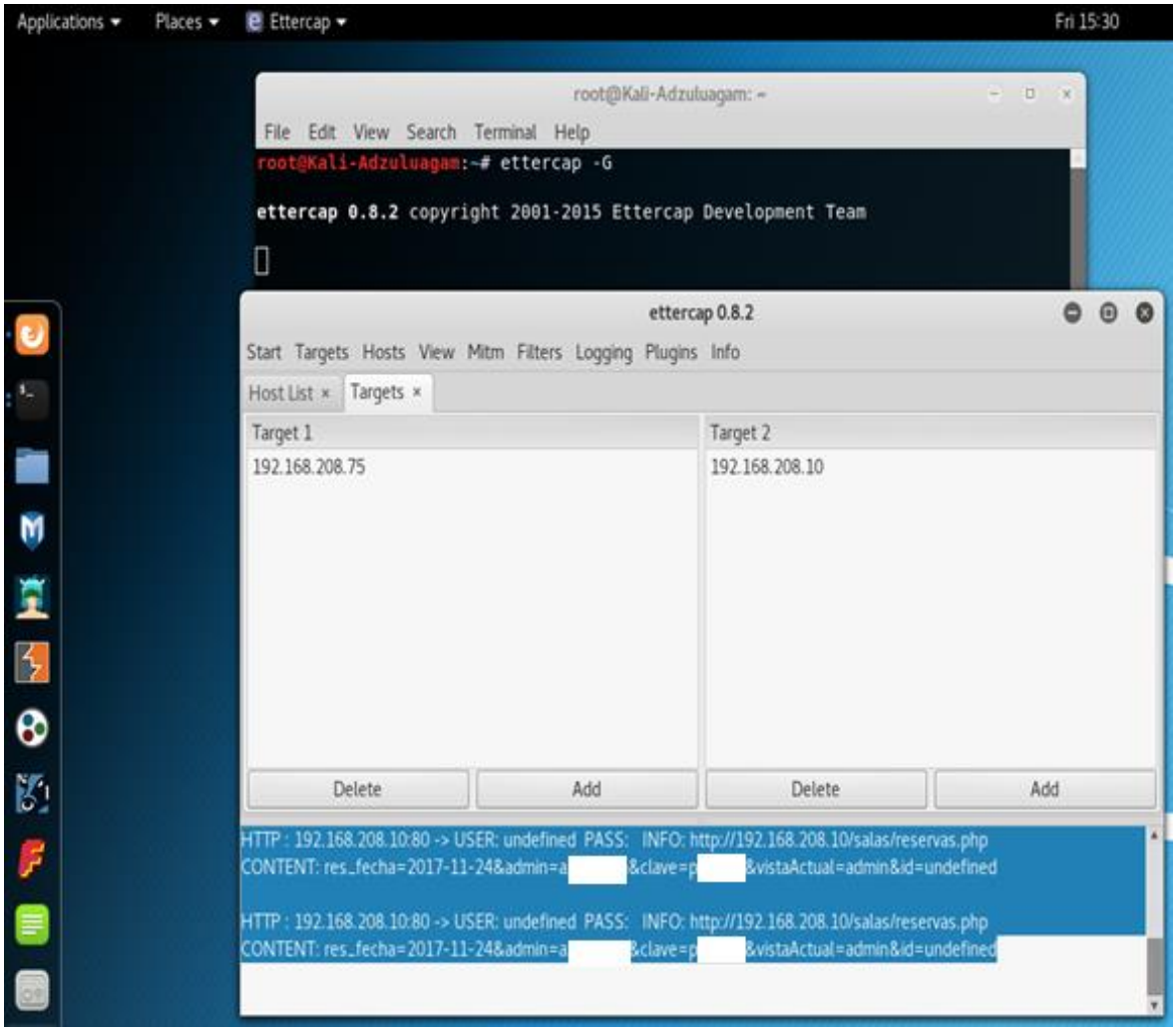


Fuente: Allen David Zuluaga Mateus

Una vez hecho esto se puede iniciar con el ataque habilitando el ARP poisoning, quedando el ataque lanzado, solo se necesita esperar a que se presente tráfico entre ambas máquinas y este sea capturado por Ettercap

Después de unos minutos, se observa que Ettercap ha capturado el siguiente tráfico:

Figura 13. Ataque spoofing perpetrado



Fuente: Allen David Zuluaga Mateus

Como se observa en la anterior imagen, a través de un ARP Spoofing y un IP Spoofing se logra capturar el usuario y la contraseña con los cuales se realizó la autenticación en el sitio web. El usuario y contraseña se encuentran ocultos para respetar el acuerdo de confidencialidad.

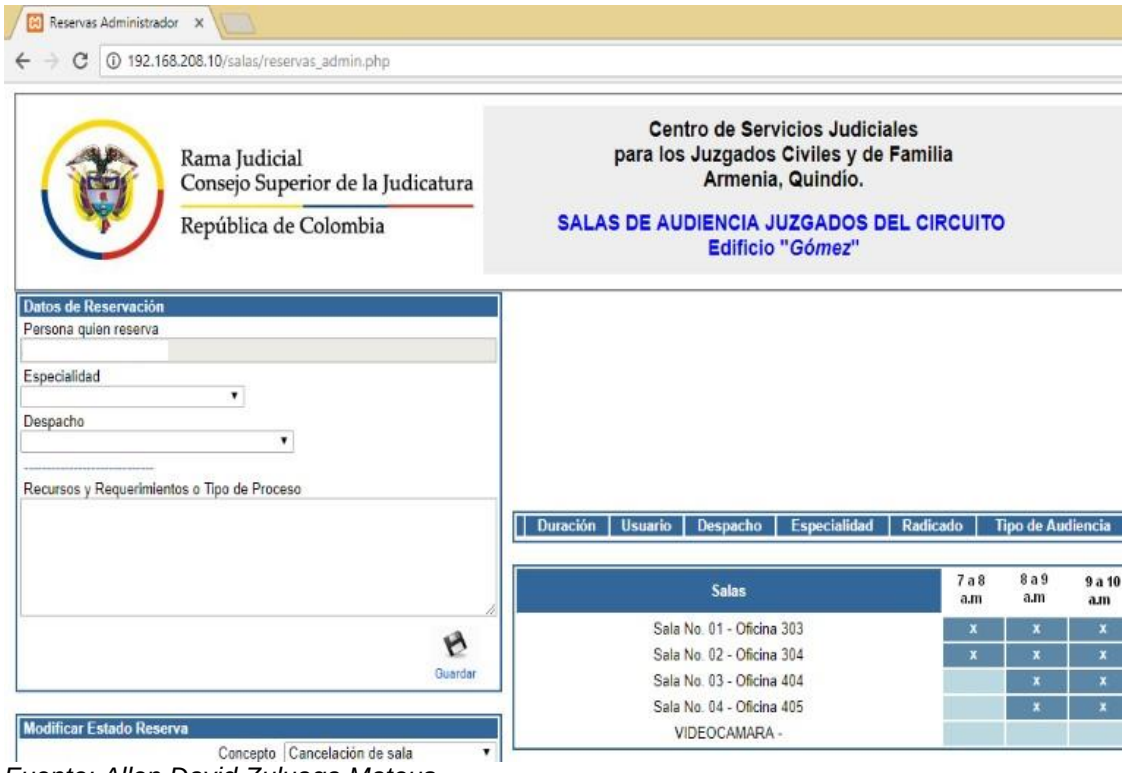
8.4 FASE DE EXPLOTACIÓN

Con las credenciales de acceso, caputradas por Ettercap, se pureba el acceso al sitio http://192.168.208.10/salas/reservas.php

Figura 14. Sitio web alojado en servidor

Fuente: Allen David Zuluaga Mateus

Figura 15. Credenciales de sitio web vulneradas



Fuente: Allen David Zuluaga Mateus

9. RECOMENDACIONES

La principal recomendación resultante del ejercicio de hacking ético realizado a la Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío, es la documentación e implementación de un Sistema de Gestión de Seguridad de la Información – SGSI, basado en los principios de la NTC ISO 27001, para lo cual se ha desarrollado en el ANEXO 6: Statement of Applicability SoA – Declaración de aplicabilidad. Con este documento se pretende tener una referencia para que la Entidad pueda aplicar medidas de protección de la información, a través de la implementación de controles establecidos en la mencionada norma técnica procurando por que no se estén dejando de lado, aquellas medidas de seguridad que posiblemente no hayan sido tenidas en cuenta por la Entidad.

Ademas de lo anterior, se recomienda hacer un amplio despliegue de los controles definidos en dicha norma y muy especialmente los asociados a los dominios:

5. Políticas de seguridad, en lo relacionado con el objetivo de control *"Directrices de la Dirección en seguridad de la información*", pues a través de ello es posible que la Entidad defina las políticas de seguridad de la información, en relación con los activos informáticos que se consideren indispensables para el cumplimiento de su misión.

9. Control de accesos, en lo relacionado con los objetivos de control "*gestión de acceso de usuario*" y "*Control de acceso a las aplicaciones*", pues la correcta implementación de estos controles permitirá a la Entidad endurecer su seguridad informática en cuanto a las políticas de autorización y de acceso.

10. Cifrado, en lo relacionado con los "*Controles criptográficos*" que debe implementar la Rama Judicial, para asegurarse que la información se encuentre protegida de accesos no autorizados, pues el presente hacking ético reveló que las credenciales de acceso viajan en texto plano, encontrándose expuestas a ataques como el realizado.

Esto, debido a que los mencionados dominios fueron directamente impactados de una manera negativa, con la realización del presente ejercicio de hacking ético, lo anterior sin menosprecio de los demás dominios, objetivos de control y controles especificados en dicha norma.

10. CONCLUSIONES

- ✓ La metodología abierta de testeo de seguridad – OSSTMM, permite determinar eficazmente, vulnerabilidades a la seguridad informática a través de un modelo estructurado y con un análisis cuantitativo.

- ✓ A través de un hacking ético es posible recabar información sobre un objetivo, además de identificar y explotar vulnerabilidades o fallas en la seguridad informática de una entidad.

- ✓ La herramienta de reportes STAR, implementada en OSSTMM, permite cuantificar el nivel de seguridad de una organización, a traves de formulas matemáticas basadas en la aplicación de la metodología.

- ✓ A partir de la identificación y cuantificación de amenazas, es posible tomar decisiones e implementar mecanismos de mitigación que contribuyan al fortalecer el nivel de seguridad de las organizaciones

BIBLIOGRAFÍA

ALARCÓN SALVATIERRA, P. A., BARRIGA DÍAZ, R. A., & ALARCÓN SALVATIERRA, J. A. (2016). La Importancia de la Seguridad Informática en las Instituciones Gubernamentales. *Revista Caribeña de Ciencias Sociales - ISSN: 2257-7630*.

ALTERNATIVE TO. (s.f.). *Crowedsourced Software Recomendations - Alternatives to Metasploit*. Recuperado el 21 de mayo de 2017, de http://alternativeto.net/software/metasploit-community-edition/

AMBITO JURIDICO. (20 de junio de 2014). *Noticias Juridicas y Analisis de Nuevas Leyes*. Obtenido de Sentencia “cero papel” restituye predios a víctimas del conflicto: https://www.ambitojuridico.com/BancoConocimiento/Civil-y-Familia/noti-142006-05-sentencia-cero-papel-restituye-predios-a-victimas-del-conflicto

COLEGIATURA COLOMBIANA. (2016). *Colegiatura Colombiana.* Obtenido de http://www.colegiatura.edu.co/images/contenidos/admisiones/EscalaSalarial2016RedEnlaceProfesional.pdf

CONSEJO SUPERIOR DE LA JUDICATURA. (2015). *Rama Judicial.* Obtenido de Plan Sectorial de Desarrollo: https://www.ramajudicial.gov.co/documents/1513685/5113559/Plan_Sectorial_de_Desarrollo_Rama_Judicial_2015-2018+%283%29.pdf/a7b785e1-fb02-4ff6-905b-c16ac93df312

CONSEJO SUPERIOR DE LA JUDICATURA. (s.f.). *Corporación Exelencia en la Justicia.* Obtenido de Presente y Futuro de las TICS en la Rama Judicial: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0ahUKEwjD9uOwwInUAhVMJCYKHaQnDOsQFgg1MAQ&url=http%3A%2F%2Fwww.cej.org.co%2Findex.php%2Fcomponent%2Fdocman%2Fdoc_download%2F393-presentacion-consejo-superior-de-la-judicatura%3FItemid%3

CONSEJO SUPERIOR DE LA JUDICATURA. (s.f.). *Sistema Integrado de Gestión de Calidad y Medio Ambiente - SIGMA*. Recuperado el 29 de marzo de 2017, de Mapa de procesos: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/portal/index.php?idcategoria=8

CORONEL SUÁREZ, I. A. (2016). *Aplicar Hackeo Ético para Detección de Vulnerabildiades Mediante Herramientas Open Source en las Aplicaciones Web de una Institución de Educación Superior.* Obtenido de Escuela Superior Politecnica del Litoral: http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/37397/D-103391.pdf

CRUZ SAAVEDRA, W. G. (02 de junio de 2014). *Universdidad Privada del Norte.* Obtenido de Repositori Institucional: http://repositorio.upn.edu.pe/bitstream/handle/11537/10239/Cruz%20Saavedra%20Walter%20Gonzalo.pdf?sequence=1&isAllowed=y

JUNTA DE ANDALUCIA. (s.f.). *Marco de Desarrollo de la Junta de Andalucía*. Recuperado el 2017 de mayo de 20, de http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551

LEY 1273 de 2009. (05 de enero de 2009). *Senad de la Republica.* Obtenido de Ministerio del Interior y de Justicia: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

LEY 1581. (17 de octubre de 2012). *Alcaldia de Bogotá*. Obtenido de Diario Oficial Alcaldia de Bogota: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

LOPEZ SANTOYO, R. (junio de 2015). *Repositorio Universidad Autónoma de Madrid.* Obtenido de Universidad Autónoma de Madrid: https://repositorio.uam.es/bitstream/handle/10486/668900/Lopez_Santoyo_Roberto_tfg.pdf?sequence=1&isAllowed=y

MAGERIT. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En M. d. Públicas, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* (pág. 13). Madrid: Subdirección General de Información, Documentación y Publicaciones.

MINTIC. (s.f.). *Ministerio de Tecnologias de la Informacion y las Comunicaciones*. Obtenido de Fortalecimiento de la gestion en el Estado: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6206.html

MUÑOZ DE FRUTOS, A. (31 de octubre de 2015). *ComputerHoy*. Obtenido de ¿Qué es un hacker y qué tipos de hacker existen?: http://computerhoy.com/noticias/software/que-es-hacker-que-tipos-hacker-existen-36027

NATIONAL INSTITUTE FOR STANDARS AND TECHNOLOGY. (septiembre de 2008). *Technical Guide to Information Security Testing and Assessment*. Recuperado el 21 de mayo de 2017, de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

PEDRAZA, H. (21 de noviembre de 2014). *Hector Pedraza 10*. Recuperado el 30 de marzo de 2017, de Fases del Hacking Ético: https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/

RACCIATTI, H. M. (13 de diciembre de 2010). *Infosec Island*. Obtenido de Tiempos de Cambio: OSSTMM 3 - Una Introducción: http://www.infosecisland.com/blogview/10215-Tiempos-de-Cambio-OSSTMM-3-Una-Introduccin-.html

RAMA JUDICIAL DEL PODER PÚBLICO. (s.f.). *Sistema de Gestión y Control de la Calidad y el Medio Ambiente.* Obtenido de Rama Judicial: http://sistemagestioncalidad.ramajudicial.gov.co/ModeloCSJ/results_busqueda.php?proceso=13&tipos=0

UNAD. (s.f.). *Universidad Nacionla Abierta y a Distancia - UNAD.* Obtenido de Alternativas para grado - ECBTI: https://academia.unad.edu.co/ecbti/oferta-academica/alternativas-para-grado

UNIDAD DE DESARROLLO Y ANÁLISIS ESTADÍSTICO - RAMA JUDICIAL. (2017). *Documento para la Elaboración del Contexto Institucional de la Rama Judicial.* Bogotá D.C.: UDAE.

ZULUAGA MATEUS, A. D. (2014). *Analisis Infraestructura de la Entidad - Rama Judicial.* Armenia.

ANEXOS

ANEXO 1: Solicitud autorización hacking ético

Rama Judicial del Poder Público
Centro de Servicios para los Juzgados Civiles y de Familia
Armenia – Quindío.

DIRECCIÓN SECCIONAL ADMINISTRACIÓN JUDICIAL
SECRETARIA
RECIBE: Beatriz Raver
FECHA: 15 NOV 2017
HORA: 5:00pm FOLIOS: 1

10 de noviembre de 2017
Armenia, Quindío.

Doctor:
Julián Ochoa Arango
Director Ejecutivo Seccional de Administración Judicial
Ciudad

Asunto: Autorización para realizar pruebas de penetración y evaluar la seguridad informática en la Dirección Ejecutiva Seccional de Administración Judicial de Armenia

Respetado Dr. Julián,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de Especialización en Seguridad Informática. Para culminar este proceso académico, es mi intención desarrollar un trabajo de grado aplicado en la Dirección Ejecutiva Seccional de Administración Judicial, de manera que pueda revertir los conocimientos adquiridos en dicha especialización y generar un impacto positivo en la Entidad, en lo relacionado con los temas de seguridad informática.

Así las cosas, muy comedidamente solicito su autorización para realizar un "Hacking Ético Basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM", tal como lo indica el título del proyecto que pretendo adelantar.

OSSTMM, es una metodología que permite realizar una prueba a la seguridad informática, obteniendo una medida del nivel de la misma y una serie de reportes que permitirán a la Dirección Ejecutiva Seccional de Administración Judicial, tomar decisiones de manera preventiva, generando soluciones en materia de ciberseguridad, que permitan eliminar las posibles vulnerabilidades encontradas, antes de que estas sean explotadas por un atacante.

La realización del mencionado hacking ético, indudablemente genera un impacto positivo en las políticas de seguridad de la información de la Rama Judicial, pues se constituye en un elemento de entrada que permite la toma de decisiones basadas en hechos, en pro de la seguridad de la información. Esto a su vez redunda en un beneficio para los usuarios del aparato judicial, pues la información asociada a sus procesos judiciales, se encontrará mejor protegida, generando una mayor confianza en la Entidad.

De obtener esta autorización, se elaborará un documento consensuado sobre las reglas y compromisos del hacking ético, entre los cuales se destacan:

- Se prohíbe la realización de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por la Rama Judicial
- Las pruebas de seguridad a sistemas obviamente inseguros o inestables, locaciones y procesos que se tengan algún grado de inestabilidad, se encuentran prohibidas.
- El analista de seguridad, encargado de realizar las pruebas enmarcadas en el presente hacking ético, en este caso el Tesista, debe proporcionar confidencialidad y no revelación de la información de la Rama Judicial y los resultados de las pruebas realizadas.
- El Tesista debe respetar y mantener la seguridad, la salud, el bienestar y la privacidad del público tanto dentro como fuera del alcance.

Carrera 20A N° 14 15 Oficina 504 Edificio Gómez
Tel: (+6) 744 2949 csejforalarm@cendoj.ramajudicial.gov.co
Armenia, Quindío.

- El Tesista siempre debe operar dentro de la ley y demás de las regulaciones establecidas por la Entidad.
- Se debe respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

Adicionalmente y como valor agregado, se realizaran recomendaciones y se plantearan soluciones prácticas que permitan minimizar el riesgo asociado a las posibles vulnerabilidades encontradas.

Es necesario informar que el Ingeniero Alexander Moreno Rojas, ya se encuentra enterado del proyecto y con disposición para colaborar con el desarrollo del mismo y la implementación de las soluciones planteadas.

Cordialmente,

Allen David Zuluaga Mateus
Soporte tecnológico para la oralidad
Centro de Servicios para los
Juzgados Civiles y de Familia

VoBo: **Ing. Alexander Moreno Rojas**
Coordinador de Soporte Tecnológico
Dirección Ejecutiva Seccional de Administración Judicial
Armenia, Quindío.

1ANEXO 2: Autorización a solicitud autorización hacking ético

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

Consejo Superior de la Judicatura
Dirección Ejecutiva Seccional de Administración Judicial
Armenia – Quindío

DESAJARO17-2207

Armenia jueves, 23 de noviembre de 2017

Ingeniero
ALLEN DAVID ZULUAGA MATEUS
Técnico en sistemas
Dirección Seccional
Armenia Q.

Asunto: *"RE: Autorización para realizar pruebas de penetración y evaluar la seguridad informática en la Dirección Ejecutiva Seccional de Administración Judicial de Armenia Q."*

Cordial saludo, Ingeniero Zuluaga Mateus,

En atención a su oficio sin número, recibido el día 15 de noviembre del presente año, en el cual solicita autorización de realizar un "Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM", el cual resultaría positivo en las políticas de seguridad de la Rama Judicial, de manera atenta me permito informarle que esta Dirección Ejecutiva Seccional de Administración le autoriza realizar las pruebas de seguridad indicadas por usted en el oficio del 15 de noviembre de 2017.

Atentamente,

JULIAN OCHOA ARANGO
Director Ejecutivo Seccional

Elaboró: Beatriz Rave R.

ANEXO 3: Reglas y compromisos del hacking ético

Reglas y Compromisos

Hacking Ético a la Rama Judicial Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío

Hacking Ético Basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM, Aplicado a La Rama Judicial, Seccional Armenia, Quindío

Noviembre de 2017

Universidad Nacional Abierta y a Distancia - UNAD
Especialización en Seguridad Informática

Tabla de contenido

Información del proyecto

Datos

Empresa / Organización	Rama Judicial - Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío
Proyecto	Hacking Ético Basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM, Aplicado a La Rama Judicial, Seccional Armenia

Gerente del proyecto

Nombre	Cargo	Departamento / División
Alexander Moreno Rojas	Coordinador de Soporte Tecnológico	Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío

Patrocinador del proyecto

Nombre	Cargo	Departamento / División
MBA. Julián Ochoa Arango	Director Ejecutivo Seccional de Administración Judicial	Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío

Equipo de trabajo

Nombre	Cargo	Departamento / División
Allen David Zuluaga Mateus	Tesista – Universidad Nacional Abierta y a Distancia UNAD	Universidad Nacional Abierta y a Distancia - Escuela de Ciencias Básicas y Tecnológicas – Especialización en Seguridad Informática

Reglas y compromisos del Hacking Ético

En el presente documento, se definen las reglas y los compromisos para realizar el hacking ético a la Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío, conforme a lo establecido en 2.4 de la Metodología Abierta para el Testeo de Seguridad - OSSTMM.

A. Ventas y marketing

Este literal queda excluido del presente documento, toda vez la realización del presente hacking ético, no representa una actividad comercial o de ventas y mercadeo, sin embargo se debe respetar que:

- La Rama Judicial, debe ser informada y sinceramente aconsejada en cuanto a sus medidas de seguridad.

B. Evaluación y entrega estimada

- Se prohíbe la realización de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por la Rama Judicial
- Las pruebas de seguridad a sistemas obviamente inseguros o inestables, locaciones y procesos que se tengan algún grado de inestabilidad, se encuentran prohibidas.

C. Contratos y negociaciones

A pesar de que para el presente hacking ético, no existe un contrato comercial entre la Universidad Nacional Abierta y a Distancia – UNAD, la Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío y el Tesista Ing. Allen David Zuluaga Mateus, se deben respetar los siguientes requerimientos y prohibiciones:

- El analista de seguridad, encargado de realizar las pruebas enmarcadas en el presente hacking ético, en este caso el Tesista, debe proporcionar confidencialidad y no revelación de la información de la Rama Judicial y los resultados de las pruebas realizadas.
- La Rama Judicial – Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío, debe proporcionar una declaración firmada que autorice el permiso de las pruebas de seguridad a realizar.
- La anterior autorización debe incluir permisos claros y específicos para pruebas que impliquen fallas de supervivencia, denegación de servicio, pruebas de proceso e ingeniería social y delimitar si estas se encuentran prohibidas o autorizadas.

D. Definición del alcance

- El alcance debe estar claramente definido antes de realizar las pruebas de verificación de servicios y vulnerabilidades
- Se deben explicar claramente los límites de cualquier prueba de seguridad a realizar, de acuerdo con el alcance.

E. Plan de pruebas

- El plan de pruebas no puede contener planes, procesos, técnicas o procedimientos que estén fuera del nivel de competencia del Tesista.

F. Proceso de pruebas

- El Tesista debe respetar y mantener la seguridad, la salud, el bienestar y la privacidad del público tanto dentro como fuera del alcance.
- El Tesista siempre debe operar dentro de la ley y demás de las regulaciones establecidas por la Entidad.
- De ser necesario realizar pruebas privilegiadas, la Rama Judicial debe proporcionar dos credenciales de acceso diferentes, ya sean contraseñas, certificados, números de identificación seguros, distintivos, etc. y deben ser típicas para los usuarios de los privilegios que se están probando en lugar de estar especialmente vacíos o accesos seguros.
- Cuando la prueba incluye privilegios conocidos, el Tesista debe primero probar sin privilegios (como en un entorno de caja negra) antes de probar de nuevo con privilegios.
- El Tesista debe conocer sus herramientas software o hardware a utilizar durante el test, de dónde provienen las herramientas, cómo funcionan, además de hacer que las prueben en un área de pruebas restringida antes de usar las herramientas en la Rama Judicial.
- La realización de pruebas destinadas a probar la denegación de un servicio o recuperación ante desastres sólo puede hacerse con permiso explícito de la Rama Judicial y sólo al ámbito en el que no se produzca ningún daño a los equipos de la Entidad ni afectaciones en la prestación del servicio
- Tanto las vulnerabilidades verificadas, así como las brechas de seguridad descubiertas, que pueden explotarse a través de un acceso completo, no vigilado o no rastreable, y que puedan poner en peligro vidas o la operación de la Entidad, deben ser comunicadas inmediatamente a la Rama Judicial, acompañadas de una solución práctica que impida su explotación.

G. Reportes

- Se debe respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.
- Los informes derivados del hacking ético deben ser objetivos, sin falsedades, ni malicia dirigida personalmente.
- Se debe notificar a la Rama Judicial cuando el Tesista deba cambiar el plan o lugar de pruebas, así como cuando ocurra algún problema durante la realización de las mismas. Se deben realizar notificaciones antes de ejecutar pruebas nuevas, peligrosas o de alto tráfico.
- Cuando se incluyan recomendaciones y/o soluciones en el informe, estas deben ser válidas y prácticas.
- El informe debe indicar claramente tanto las medidas de seguridad y controles que se cataloguen como exitosos y fallidos.
- Los informes deben utilizar únicamente indicadores cuantitativos para medir la seguridad. Estas métricas deben basarse en hechos y evitar interpretaciones subjetivas.
- La Rama Judicial debe ser notificada cuando se envía el informe para esperar su llegada y para confirmar la recepción de la entrega.
- Los canales de comunicación para la entrega del informe deben ser confidenciales de extremo a extremo.
- Los resultados y los informes nunca pueden utilizarse para obtener beneficios comerciales o afectar la imagen y otros factores de la Entidad

Firmas,

_____
Julián Ochoa Arango
Director Ejecutivo Seccional de Administración Judicial

_____
Alexander Moreno Rojas
Profesional Universitario G-11
Director del Proyecto

_____
Allen David Zuluaga Mateus
Tesista Especialización en seguridad informática

ANEXO 4: Plan de pruebas

Plan de Pruebas

Hacking Ético a la Rama Judicial Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío

Hacking Ético Basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM, Aplicado a La Rama Judicial, Seccional Armenia, Quindío

Noviembre de 2017

Universidad Nacional Abierta y a Distancia - UNAD
Especialización en Seguridad Informática

Tabla de contenido

Plan de Pruebas

El presente documento tiene como objetivo determinar de manera consensuada, las pruebas a realizar, en el marco del Hacking Ético Basado en la Metodología Abierta de Testeo de Seguridad – OSSTMM, Aplicado a La Rama Judicial, Seccional Armenia, Quindío

FECHA DEL ANÁLISIS

27/nov/2017 al 11/dic/2017

DURACIÓN

2 semanas

NOMBRE DEL AUDITOR

Allen David Zuluaga Mateus

TIPO DE TEST

De caja blanca, bajo los siguientes roles:

Tester/Auditor:
Tiene conocimiento limitado de las defensas de la Entidad y un pleno conocimiento de los canales.

Entidad/Auditado:
Conoce el alcance y el plazo del Hacking Ético, pero no de los calanes probados ni vectores de prueba utilizados.

ALCANCE DE LAS PRUEBAS

Razón social:
Dirección Ejecutiva Seccional de Administración Judicial de Armenia

Dirección:
Carrera 12 # 20 - 63 Palacio de Justicia "Fabio Calderón Botero", Piso 3º Oficina 335T, Armenia, Quindío.

Teléfono:
(+6) 741 47 13

Responsable:
Julián Ochoa Arango

Cargo:
Director Ejecutivo Seccional de Administración Judicial

Sede:
Palacio de Justicia ***Fabio Calderón Botero***

CANALES ANALIZADOS

Con base en lo establecido en la metodología OSSTMM, se analizan los siguientes canales:

- ✓ Humano
- ✓ Físico
- ✓ Redes inalámbricas
- ✓ Telecomunicaciones
- ✓ Redes de Datos

VECTORES ANALIZADOS

El presente hacking ético se realiza vectorizado de adentro hacia adentro, pues actualmente se cuenta con acceso, aunque limitado, a la infraestructura tecnológica de la Entidad. Igualmente, es pertinente realizar pruebas externas, pero buscando alcanzar o acceder a la infraestructura de la Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío y no otras infraestructuras localizadas en otras ciudades o incluso en el nivel central (Bogotá).

La realización de las pruebas únicamente requiere del uso de computadores y herramientas relacionadas con la seguridad informática. Ningún otro tipo de hardware o equipos es requerido

CONTROLES

Dentro de los controles a testear en el presente hacking ético, se definen los siguientes:

Autenticación
Este control, que se encuentra enfocado en desafiar las credenciales de acceso a los diferentes activos y sistemas de información, a través de la ***Identificación*** y la ***autorización***.

Subyugación
Este control asegura que las actividades, acciones o interacciones sobre los activos y/o sistemas de información de la Rama Judicial, solo se realizan a través de los procedimientos establecidos para tal fin.

Continuidad
Este control es sobre las acciones que permiten mantener los sistemas operativos, en caso de corrupción o falla.

No Repudiación
A través de este control se asegura que los actores de los sistemas de información de la Rama Judicial no pueden negar la ejecución de las diferentes actividades que ejecutan sobre dichos sistemas.

Confidencialidad
Es un control para asegurar que un activo exhibido o intercambiado entre partes que interactúan no puede ser conocido fuera de esas partes.

Privacidad
Es un control para asegurar que un recurso que se accede se muestra o se intercambia entre las partes no puede ser conocido fuera de esas partes.

Integridad
Es un control para asegurar que las partes interactuantes sepan cuándo los activos y los procesos han cambiado

LIMITACIONES

Los controles de ***Indemnización***, ***resiliencia*** y ***alarma*** no serán tenidos en cuenta durante el presente hacking ético, puesto que algunos de ellos van asociados a la normatividad legal de la entidad que no está incluida dentro del alcance del presente proyecto, además que su testeo puede afectar la prestación del servicio de justicia

De igual manera, se encuentran prohibidas las pruebas y/o explotación de vulnerabilidades que puedan poner en riesgo la operatividad de los sistemas informáticos de la entidad.

Las pruebas que impliquen fallas de supervivencia y/o denegación de servicio, se encuentran prohibidas.

POLÍTICA DE CONFIDENCIALIDAD

Toda la información obtenida durante cualquiera de las fases del hacking ético realizado a la Dirección Ejecutiva Seccional de Administración Judicial de Armenia, y que pueda poner en riesgo la seguridad de la información de la Entidad, de los procesos que allí se ejecutan, de las personas que allí laboran, de los usuarios del servicio de justicia, no podrá ser divulgada, bajo ningún criterio.
La información genérica, relacionada con los resultados del mencionado hacking ético, y que no ponga en riesgo la seguridad de la información de la Entidad, de los procesos que allí se ejecutan, de las personas que allí laboran, de los usuarios del servicio de justicia, podrá ser divulgada con fines académicos, investigativos, no comerciales y en busca de mejorar la seguridad de la información de la entidad, para lo cual se debe contar con la autorización ya sea del Director Ejecutivo Seccional o del Coordinador de Soporte Tecnológico de la Entidad.

Firmas,

_____
Alexander Moreno Rojas
Profesional Universitario G-11
Director del Proyecto

_____
Allen David Zuluaga Mateus
Tesista Especialización en seguridad informática

ANEXO 5: Resultados escaneo con Nmap

Nmap Scan Report - Scanned at Fri Dec 1 14:32:09 2017

Scan Summary

| 192.168.208.0
| 192.168.208.1 (192.168.208.1)
| 192.168.208.2
| 192.168.208.3
| 192.168.208.4
| 192.168.208.5
| 192.168.208.6
| 192.168.208.7
| 192.168.208.8
| 192.168.208.9
| 192.168.208.10
| 192.168.208.11
| 192.168.208.12
| 192.168.208.13
| 192.168.208.14
| 192.168.208.15
| 192.168.208.16
| 192.168.208.17
| 192.168.208.18
| 192.168.208.19 (192.168.208.19)
| 192.168.208.20
| 192.168.208.21
| 192.168.208.22
| 192.168.208.23
| 192.168.208.24
| 192.168.208.25
| 192.168.208.26
| 192.168.208.27
| 192.168.208.28
| 192.168.208.29
| 192.168.208.30
| 192.168.208.31 (192.168.208.31)
| 192.168.208.32
| 192.168.208.33
| 192.168.208.34
| 192.168.208.35
| 192.168.208.36 (192.168.208.36)
| 192.168.208.37
| 192.168.208.38
| 192.168.208.39 (192.168.208.39)
| 192.168.208.40
| 192.168.208.41
| 192.168.208.42
| 192.168.208.43
| 192.168.208.44
| 192.168.208.45

192.168.208.46
192.168.208.47
192.168.208.48
192.168.208.49
192.168.208.50
192.168.208.51
192.168.208.52
192.168.208.53
192.168.208.54
192.168.208.55
192.168.208.56 (192.168.208.56)
192.168.208.57
192.168.208.58
192.168.208.59
192.168.208.60 (192.168.208.60)
192.168.208.61
192.168.208.62
192.168.208.63
192.168.208.64
192.168.208.65
192.168.208.66
192.168.208.67
192.168.208.68
192.168.208.69
192.168.208.70
192.168.208.71
192.168.208.72
192.168.208.73
192.168.208.74
192.168.208.75
192.168.208.76 (192.168.208.76)
192.168.208.77
192.168.208.78
192.168.208.79
192.168.208.80
192.168.208.81 (192.168.208.81)
192.168.208.82
192.168.208.83
192.168.208.84
192.168.208.85 (192.168.208.85)
192.168.208.86
192.168.208.87
192.168.208.88
192.168.208.89
192.168.208.90 (192.168.208.90)
192.168.208.91
192.168.208.92
192.168.208.93
192.168.208.94 (192.168.208.94)
192.168.208.95 (192.168.208.95)
192.168.208.96

192.168.208.97
192.168.208.98
192.168.208.99
192.168.208.100
192.168.208.101 (192.168.208.101)
192.168.208.102
192.168.208.103
192.168.208.104
192.168.208.105
192.168.208.106
192.168.208.107
192.168.208.108
192.168.208.109
192.168.208.110
192.168.208.111 (192.168.208.111)
192.168.208.112 (192.168.208.112)
192.168.208.113
192.168.208.114
192.168.208.115
192.168.208.116 (192.168.208.116)
192.168.208.117
192.168.208.118 (192.168.208.118)
192.168.208.119
192.168.208.120
192.168.208.121
192.168.208.122
192.168.208.123
192.168.208.124
192.168.208.125
192.168.208.126
192.168.208.127
192.168.208.128
192.168.208.129
192.168.208.130
192.168.208.131
192.168.208.132
192.168.208.133
192.168.208.134
192.168.208.135
192.168.208.136
192.168.208.137
192.168.208.138 (192.168.208.138)
192.168.208.139 (192.168.208.139)
192.168.208.140 (192.168.208.140)
192.168.208.141 (192.168.208.141)
192.168.208.142 (192.168.208.142)
192.168.208.143
192.168.208.144 (192.168.208.144)
192.168.208.145 (192.168.208.145)
192.168.208.146 (192.168.208.146)
192.168.208.147 (192.168.208.147)

192.168.208.148 (192.168.208.148)
192.168.208.149
192.168.208.150 (192.168.208.150)
192.168.208.151
192.168.208.152 (192.168.208.152)
192.168.208.153 (192.168.208.153)
192.168.208.154 (192.168.208.154)
192.168.208.155
192.168.208.156 (192.168.208.156)
192.168.208.157
192.168.208.158
192.168.208.159
192.168.208.160 (192.168.208.160)
192.168.208.161 (192.168.208.161)
192.168.208.162
192.168.208.163 (192.168.208.163)
192.168.208.164 (192.168.208.164)
192.168.208.165 (192.168.208.165)
192.168.208.166
192.168.208.167 (192.168.208.167)
192.168.208.168
192.168.208.169
192.168.208.170 (192.168.208.170)
192.168.208.171
192.168.208.172
192.168.208.173
192.168.208.174
192.168.208.175
192.168.208.176
192.168.208.177
192.168.208.178
192.168.208.179
192.168.208.180
192.168.208.181
192.168.208.182
192.168.208.183
192.168.208.184
192.168.208.185
192.168.208.186
192.168.208.187
192.168.208.188
192.168.208.189
192.168.208.190
192.168.208.191
192.168.208.192
192.168.208.193
192.168.208.194
192.168.208.195
192.168.208.196
192.168.208.197
192.168.208.198

192.168.208.199
192.168.208.200 (192.168.208.200)
192.168.208.201 (192.168.208.201)
192.168.208.202 (192.168.208.202)
192.168.208.203 (192.168.208.203)
192.168.208.204
192.168.208.205
192.168.208.206
192.168.208.207
192.168.208.208
192.168.208.209
192.168.208.210
192.168.208.211
192.168.208.212
192.168.208.213
192.168.208.214
192.168.208.215
192.168.208.216
192.168.208.217
192.168.208.218
192.168.208.219
192.168.208.220
192.168.208.221
192.168.208.222
192.168.208.223
192.168.208.224
192.168.208.225
192.168.208.226
192.168.208.227
192.168.208.228
192.168.208.229
192.168.208.230
192.168.208.231
192.168.208.232
192.168.208.233
192.168.208.234
192.168.208.235
192.168.208.236
192.168.208.237
192.168.208.238
192.168.208.239
192.168.208.240
192.168.208.241
192.168.208.242
192.168.208.243
192.168.208.244
192.168.208.245
192.168.208.246
192.168.208.247
192.168.208.248
192.168.208.249

| **192.168.208.250**
| **192.168.208.251**
| **192.168.208.252**
| **192.168.208.253**
| **192.168.208.254**
| **192.168.208.255**

Scan Summary

Nmap 7.60 was initiated at Fri Dec 1 14:32:09 2017 with these arguments: *nmap -T4 -A -v 192.168.208.0/24*
Verbosity: 1; Debug level 0

192.168.208.0 **(click to expand)**

192.168.208.1 / 192.168.208.1

Address

192.168.208.1 - (ipv4)
24:9E:AB:9F:11:84 - Huawei Technologies (mac)

Hostnames

192.168.208.1 (PTR)

Ports

The 994 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [3])**	
23	tcp	open	
80	tcp	open	
443	tcp	open	

Remote Operating System Detection

Used port: 443/tcp (open)
Used port: 1/tcp (closed)
OS match: Huawei VRP 5.160 (98%)
OS match: Huawei VRP 3 switch (91%)
OS match: IBM AIX 4.3 (90%)
OS match: Apple Mac OS X 10.3.9 (Panther) (Darwin 7.9.0, PowerPC) (90%)
OS match: Huawei S9300 switch (90%)
OS match: IBM AIX 5.3 (89%)
OS match: IBM AIX 5.2 on Power5 (88%)
OS match: 3Com SuperStack 3 Switch 4500 (88%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.2 **(click to expand)**
192.168.208.3 **(click to expand)**
192.168.208.4 **(click to expand)**
192.168.208.5 **(click to expand)**
192.168.208.6 **(click to expand)**
192.168.208.7 **(click to expand)**
192.168.208.8 **(click to expand)**
192.168.208.9 **(click to expand)**

192.168.208.10

Address

192.168.208.10 - (ipv4)
D4:AE:52:75:4E:38 - Dell (mac)

Ports

The 982 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Product
80	tcp	open	http	syn-ack	Apache httpd

135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn
443	tcp	open	http	syn-ack	Apache httpd
444	tcp	open	snpp	syn-ack	
445	tcp	open	microsoft-ds	syn-ack	Windows Server 2008 R2 Standard 7601 Service Pack 1 mi ds
2179	tcp	open	vmrdp	syn-ack	
2222	tcp	open	EtherNetIP-1	syn-ack	
3306	tcp	open	mysql	syn-ack	MySQL
3389	tcp	open	ssl	syn-ack	Microsoft SChannel TLS
5666	tcp	open	tcpwrapped	syn-ack	
8081	tcp	open	tcpwrapped	syn-ack	
49152	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49153	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49159	tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49160	tcp	open	msrpc	syn-ack	Microsoft Windows RPC

Remote Operating System Detection

Used port: 80/tcp (open)
Used port: 1/tcp (closed)
Used port: 31987/udp (closed)
OS match: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (96%)
OS match: Microsoft Windows 7 or Windows Server 2008 R2 (96%)
OS match: Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%)
OS match: Microsoft Windows Server 2008 SP1 (96%)
OS match: Microsoft Windows Server 2008 SP2 (96%)
OS match: Microsoft Windows 7 (96%)
OS match: Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%)
OS match: Microsoft Windows 7 SP1 (96%)
OS match: Microsoft Windows 7 Ultimate (96%)
OS match: Microsoft Windows 7 Ultimate SP1 or Windows 8.1 Update 1 (96%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.11

Address

192.168.208.11 - (ipv4)
B8:97:5A:72:19:2C - Biostar Microtech Int'l (mac)

Ports

The 999 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
1688	tcp	open	msrpc

Remote Operating System Detection

Used port: 1688/tcp (open)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.12 **(click to expand)**

192.168.208.13 **(click to expand)**

192.168.208.14 **(click to expand)**

192.168.208.15 **(click to expand)**

192.168.208.16 **(click to expand)**

192.168.208.17 **(click to expand)**

192.168.208.18 **(click to expand)**

192.168.208.19 / 192.168.208.19

Address

192.168.208.19 - (ipv4)
B8:97:5A:72:1B:1F - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.19 (PTR)

Ports

The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
135	tcp	open	msrpc
1688	tcp	open	msrpc

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 or 2008 Beta 3 (100%)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows 8.1 R1 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.20 **(click to expand)**

192.168.208.21 **(click to expand)**

192.168.208.22

Address

192.168.208.22 - (ipv4)
B8:97:5A:72:0F:3D - Biostar Microtech Int'l (mac)

Ports

The 999 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
49156	tcp	open	msrpc

Remote Operating System Detection

Used port: 49156/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.23 **(click to expand)**

192.168.208.24 **(click to expand)**

192.168.208.25 **(click to expand)**

192.168.208.26 **(click to expand)**

192.168.208.27 **(click to expand)**

192.168.208.28 **(click to expand)**

192.168.208.29 **(click to expand)**

192.168.208.30

Address
192.168.208.30 - (ipv4)
B8:97:5A:72:0A:A2 - Biostar Microtech Int'l (mac)
Ports
The 1000 ports scanned but not shown below are in state: filtered
Remote Operating System Detection
Unable to identify operating system.

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.31 / 192.168.208.31
Address
192.168.208.31 - (ipv4)
C8:9C:DC:FB:75:B9 - Elitegroup Computer Systems (mac)
Hostnames
192.168.208.31 (PTR)
Ports
The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Pro
139	tcp	open	tcpwrapped	syn-ack	
445	tcp	open	tcpwrapped	syn-ack	Wir

Remote Operating System Detection
Used port: 445/tcp (open)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.32 **(click to expand)**

192.168.208.33
Address
192.168.208.33 - (ipv4)
B8:97:5A:72:0E:B9 - Biostar Microtech Int'l (mac)
Ports
The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason
135	tcp	open	msrpc	syn-ack
139	tcp	open	netbios-ssn	syn-ack
445	tcp	open	microsoft-ds	syn-ack
49155	tcp	open	msrpc	syn-ack

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.34
Address
192.168.208.34 - (ipv4)
B8:97:5A:72:11:A0 - Biostar Microtech Int'l (mac)
Ports
The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason
135	tcp	open	msrpc	syn-ack
139	tcp	open	netbios-ssn	syn-ack

445	tcp	open	microsoft-ds	syn-ack	Windows 8.1
49156	tcp	open	msrpc	syn-ack	Microsoft Wi

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.35 **(click to expand)**

192.168.208.36 / 192.168.208.36

Address
192.168.208.36 - (ipv4)
B8:97:5A:7B:F8:94 - Biostar Microtech Int'l (mac)

Hostnames
192.168.208.36 (PTR)

Ports
The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
135	tcp	open	msrpc
1688	tcp	open	msrpc

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 or 2008 Beta 3 (100%)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows 8.1 R1 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.37

Address
192.168.208.37 - (ipv4)
B8:97:5A:72:10:4F - Biostar Microtech Int'l (mac)

Ports
The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.38

Address
192.168.208.38 - (ipv4)
B8:97:5A:72:13:1F - Biostar Microtech Int'l (mac)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Pro
135	tcp	open	msrpc	syn-ack	Mic
139	tcp	open	netbios-ssn	syn-ack	Mic
445	tcp	open	microsoft-ds	syn-ack	Mic
49155	tcp	open	msrpc	syn-ack	Mic

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.39 / 192.168.208.39

Address

192.168.208.39 - (ipv4)
B8:97:5A:69:3A:ED - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.39 (PTR)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.40 **(click to expand)**
192.168.208.41 **(click to expand)**
192.168.208.42 **(click to expand)**
192.168.208.43 **(click to expand)**
192.168.208.44 **(click to expand)**
192.168.208.45 **(click to expand)**
192.168.208.46 **(click to expand)**
192.168.208.47 **(click to expand)**
192.168.208.48 **(click to expand)**
192.168.208.49 **(click to expand)**

192.168.208.50

Address

192.168.208.50 - (ipv4)
B8:97:5A:72:1A:6C - Biostar Microtech Int'l (mac)

Ports

The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
139	tcp	open	tcpwrapped
445	tcp	open	tcpwrapped

Remote Operating System Detection

Used port: 445/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.51 **(click to expand)**

192.168.208.52 **(click to expand)**

192.168.208.53 **(click to expand)**

192.168.208.54 **(click to expand)**

192.168.208.55

Address

192.168.208.55 - (ipv4)
B8:97:5A:69:3E:1E - Biostar Microtech Int'l (mac)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.56 / 192.168.208.56

Address

192.168.208.56 - (ipv4)
B8:97:5A:72:11:52 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.56 (PTR)

Ports

The 995 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
2869	tcp	open	http	syn-ack	M
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)

OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.57 **(click to expand)**

192.168.208.58

Address

192.168.208.58 - (ipv4)
B8:97:5A:69:39:AD - Biostar Microtech Int'l (mac)

Ports

The 999 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
135	tcp	open	msrpc

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.59

Address

192.168.208.59 - (ipv4)
B8:97:5A:69:3A:F9 - Biostar Microtech Int'l (mac)

Ports

The 994 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
80	tcp	open	http	syn-ack	
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
443	tcp	open	https	syn-ack	
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 80/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.60 / 192.168.208.60

Address

192.168.208.60 - (ipv4)
B8:97:5A:72:1A:44 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.60 (PTR)

Ports

The 1000 ports scanned but not shown below are in state: filtered

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.61 **(click to expand)**
192.168.208.62 **(click to expand)**
192.168.208.63 **(click to expand)**
192.168.208.64 **(click to expand)**

192.168.208.65

Address

192.168.208.65 - (ipv4)
B8:97:5A:69:37:80 - Biostar Microtech Int'l (mac)

Ports

The 995 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason
135	tcp	open	msrpc	syn-ack
139	tcp	open	netbios-ssn	syn-ack
445	tcp	open	microsoft-ds	syn-ack
3389	tcp	open	ms-wbt-server	syn-ack
49155	tcp	open	msrpc	syn-ack

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.66 **(click to expand)**
192.168.208.67 **(click to expand)**
192.168.208.68 **(click to expand)**
192.168.208.69 **(click to expand)**
192.168.208.70 **(click to expand)**
192.168.208.71 **(click to expand)**
192.168.208.72 **(click to expand)**
192.168.208.73 **(click to expand)**
192.168.208.74 **(click to expand)**

192.168.208.75

Address

192.168.208.75 - (ipv4)
B8:97:5A:72:04:17 - Biostar Microtech Int'l (mac)

Ports

The 994 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason
80	tcp	open	http	syn-ack
135	tcp	open	msrpc	syn-ack
139	tcp	open	netbios-ssn	syn-ack
443	tcp	open	https	syn-ack
445	tcp	open	microsoft-ds	syn-ack
49155	tcp	open	msrpc	syn-ack

Remote Operating System Detection

Used port: 80/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)

OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.76 / 192.168.208.76

Address
192.168.208.76 - (ipv4)

Hostnames
192.168.208.76 (PTR)

Ports
The 1000 ports scanned but not shown below are in state: closed

Remote Operating System Detection
Unable to identify operating system.
Used port: 1/tcp (closed)
Used port: 35577/udp (closed)

Misc Metrics (click to expand)

192.168.208.77 **(click to expand)**

192.168.208.78 **(click to expand)**

192.168.208.79 **(click to expand)**

192.168.208.80 **(click to expand)**

192.168.208.81 / 192.168.208.81

Address
192.168.208.81 - (ipv4)
64:31:50:42:66:C5 - Hewlett Packard (mac)

Hostnames
192.168.208.81 (PTR)

Ports
The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Pro
139	tcp	open	tcpwrapped	syn-ack	
445	tcp	open	tcpwrapped	syn-ack	Wir

Remote Operating System Detection
Used port: 445/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.82 **(click to expand)**

192.168.208.83

Address
192.168.208.83 - (ipv4)
2C:41:38:B1:2F:C6 - Hewlett Packard (mac)

Ports
The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason
139	tcp	open	tcpwrapped	syn-ack
445	tcp	open	tcpwrapped	syn-ack

Remote Operating System Detection
Used port: 445/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)

OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.84

Address

192.168.208.84 - (ipv4)
2C:41:38:B5:44:CC - Hewlett Packard (mac)

Ports

The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason
139	tcp	open	tcpwrapped	syn-ack
445	tcp	open	tcpwrapped	syn-ack

Remote Operating System Detection

Used port: 445/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.85 / 192.168.208.85

Address

192.168.208.85 - (ipv4)
B8:97:5A:72:18:B5 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.85 (PTR)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.86 **(click to expand)**

192.168.208.87 **(click to expand)**

192.168.208.88

Address

192.168.208.88 - (ipv4)
D4:85:64:BA:22:A0 - Hewlett Packard (mac)

Ports

The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Produc
139	tcp	open	tcpwrapped	syn-ack	
445	tcp	open	tcpwrapped	syn-ack	Windo

Remote Operating System Detection
Used port: 445/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.89

Address
192.168.208.89 - (ipv4)
C8:9C:DC:FB:75:C7 - Elitegroup Computer Systems (mac)

Ports
The 997 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Product
135	tcp	open	msrpc	syn-ack	Microsoft Windows
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows
445	tcp	open	microsoft-ds	syn-ack	Windows 7 Profess

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.90 / 192.168.208.90

Address
192.168.208.90 - (ipv4)
18:A9:05:23:B3:CC - Hewlett Packard (mac)

Hostnames
192.168.208.90 (PTR)

Ports
The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Produc
139	tcp	open	tcpwrapped	syn-ack	
445	tcp	open	tcpwrapped	syn-ack	Windo

Remote Operating System Detection
Used port: 445/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.91 **(click to expand)**

192.168.208.92

Address
192.168.208.92 - (ipv4)
00:21:B7:7A:66:73 - Lexmark International (mac)

Ports
The 986 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0]	filtered [0])**	Service	Reason	Product
21	tcp	open	ftp	syn-ack	Lexmark E360dn printer ftpd
79	tcp	open	finger	syn-ack	Lexmark E360dn printer fingerd
80	tcp	open	http	syn-ack	thttpd
515	tcp	open	printer	syn-ack	Lexmark lpd service
631	tcp	open	http	syn-ack	thttpd
5000	tcp	open	upnp	syn-ack	
5001	tcp	open	tcpwrapped	syn-ack	
6100	tcp	open	synchronet-db	syn-ack	
8000	tcp	open	http	syn-ack	thttpd
9000	tcp	open	telnet	syn-ack	Lexmark E360dn printer telnetd
9100	tcp	open	jetdirect	syn-ack	
9200	tcp	open	ir-alerts	syn-ack	Lexmark E360dn print server identific
9500	tcp	open	ismserver	syn-ack	
10000	tcp	open	printer-admin	syn-ack	Lexmark printer admin

Remote Operating System Detection
Used port: 21/tcp (open)
Used port: 1/tcp (closed)
Used port: 41521/udp (closed)
OS match: Dell 2350dn, IBM InfoPrint 1832; or Lexmark C544dn, T612, T650, or X464de printer (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.93

Address
192.168.208.93 - (ipv4)
D4:85:64:B8:74:FE - Hewlett Packard (mac)

Ports
The 989 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [8] | filtered [0])**	Service	Reason	Produc
135	tcp	open	tcpwrapped	syn-ack	
139	tcp	open	tcpwrapped	syn-ack	
445	tcp	open	tcpwrapped	syn-ack	Windo

Remote Operating System Detection
Used port: 445/tcp (open)
Used port: 7/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.94 / 192.168.208.94

Address
192.168.208.94 - (ipv4)
18:A9:05:B1:C7:4A - Hewlett Packard (mac)

Hostnames
192.168.208.94 (PTR)

Ports
The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Produc
139	tcp	open	tcpwrapped	syn-ack	
445	tcp	open	tcpwrapped	syn-ack	Windo

Remote Operating System Detection
Used port: 445/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)

OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.95 / 192.168.208.95

Address

192.168.208.95 - (ipv4)
00:1E:0B:26:E0:B9 - Hewlett Packard (mac)

Hostnames

192.168.208.95 (PTR)

Ports

The 997 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [1] | filtered [0])**	Service	Reason
139	tcp	open	tcpwrapped	syn-ack
445	tcp	open	tcpwrapped	syn-ack

Remote Operating System Detection

Used port: 445/tcp (open)
Used port: 3389/tcp (closed)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (99%)
OS match: Microsoft Windows 7 SP1 (96%)
OS match: Microsoft Windows 8 Enterprise (95%)
OS match: Microsoft Windows Server 2008 R2 (94%)
OS match: Microsoft Windows 7 SP1 or Windows Server 2008 R2 SP1 or Windows 8.1 Update 1 (92%)
OS match: Microsoft Windows Vista Home Premium SP1, Windows 7, or Windows Server 2008 (92%)
OS match: Microsoft Windows 10 build 14393 (92%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%)
OS match: Microsoft Windows Server 2012 R2 (90%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.96 **(click to expand)**

192.168.208.97 **(click to expand)**

192.168.208.98 **(click to expand)**

192.168.208.99 **(click to expand)**

192.168.208.100 **(click to expand)**

192.168.208.101 / 192.168.208.101

Address

192.168.208.101 - (ipv4)
00:21:B7:7A:8F:08 - Lexmark International (mac)

Hostnames

192.168.208.101 (PTR)

Ports

The 986 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Product
21	tcp	open	ftp	syn-ack	Lexmark E360dn prir
79	tcp	open	finger	syn-ack	Lexmark E360dn prir
80	tcp	open	http	syn-ack	thttpd
515	tcp	open	printer	syn-ack	Lexmark lpd service
631	tcp	open	http	syn-ack	thttpd
5000	tcp	open	upnp	syn-ack	
5001	tcp	open	tcpwrapped	syn-ack	
6100	tcp	open	synchronet-db	syn-ack	
8000	tcp	open	http	syn-ack	thttpd
9000	tcp	open	telnet	syn-ack	Lexmark E360dn prir

9100	tcp	open	jetdirect	syn-ack	
9200	tcp	open	ir-alerts	syn-ack	Lexmark E360dn print server identifi
9500	tcp	open	ismserver	syn-ack	
10000	tcp	open	printer-admin	syn-ack	Lexmark printer admin

Remote Operating System Detection
Used port: 21/tcp (open)
Used port: 1/tcp (closed)
Used port: 31189/udp (closed)
OS match: Dell 2350dn, IBM InfoPrint 1832; or Lexmark C544dn, T612, T650, or X464de printer (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.102 **(click to expand)**
192.168.208.103 **(click to expand)**
192.168.208.104 **(click to expand)**
192.168.208.105 **(click to expand)**
192.168.208.106 **(click to expand)**
192.168.208.107 **(click to expand)**
192.168.208.108 **(click to expand)**
192.168.208.109 **(click to expand)**
192.168.208.110 **(click to expand)**

192.168.208.111 / 192.168.208.111

Address
192.168.208.111 - (ipv4)
00:0D:60:41:6C:3D - IBM (mac)

Hostnames
192.168.208.111 (PTR)

Ports
The 992 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service	Reaso
7	tcp	open	echo	syn-ac
9	tcp	open	discard	syn-ac
13	tcp	open	daytime	syn-ac
17	tcp	open	qotd	syn-ac
19	tcp	open	chargen	syn-ac
135	tcp	open	msrpc	syn-ac
139	tcp	open	netbios-ssn	syn-ac
445	tcp	open	microsoft-ds	syn-ac

Remote Operating System Detection
Used port: 7/tcp (open)
Used port: 1/tcp (closed)
Used port: 31957/udp (closed)
OS match: Microsoft Windows XP SP2 or SP3, or Windows Server 2003 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.112 / 192.168.208.112

Address
192.168.208.112 - (ipv4)
00:0D:60:40:50:FA - IBM (mac)

Hostnames
192.168.208.112 (PTR)

Ports
The 997 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason
135	tcp	open	msrpc	syn-ack
139	tcp	open	netbios-ssn	syn-ack
445	tcp	open	microsoft-ds	syn-ack

Remote Operating System Detection
Used port: 135/tcp (open)
Used port: 1/tcp (closed)
Used port: 39710/udp (closed)
OS match: Microsoft Windows XP SP2 or SP3, or Windows Server 2003 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.113 **(click to expand)**

192.168.208.114 **(click to expand)**

192.168.208.115 **(click to expand)**

192.168.208.116 / 192.168.208.116

Address
192.168.208.116 - (ipv4)
2C:41:38:B4:87:4D - Hewlett Packard (mac)
Hostnames
192.168.208.116 (PTR)
Ports
The 1000 ports scanned but not shown below are in state: filtered
Remote Operating System Detection
Unable to identify operating system.

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.117 **(click to expand)**

192.168.208.118 / 192.168.208.118

Address
192.168.208.118 - (ipv4)
2C:41:38:B1:36:58 - Hewlett Packard (mac)
Hostnames
192.168.208.118 (PTR)
Ports
The 1000 ports scanned but not shown below are in state: filtered
Remote Operating System Detection
Unable to identify operating system.

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.119 **(click to expand)**

192.168.208.120 **(click to expand)**

192.168.208.121 **(click to expand)**

192.168.208.122 **(click to expand)**

192.168.208.123 **(click to expand)**

192.168.208.124 **(click to expand)**

192.168.208.125 **(click to expand)**

192.168.208.126 **(click to expand)**

192.168.208.127 **(click to expand)**

192.168.208.128 **(click to expand)**

192.168.208.129 **(click to expand)**

192.168.208.130 **(click to expand)**

192.168.208.131 **(click to expand)**
192.168.208.132 **(click to expand)**
192.168.208.133 **(click to expand)**
192.168.208.134 **(click to expand)**
192.168.208.135 **(click to expand)**
192.168.208.136 **(click to expand)**
192.168.208.137 **(click to expand)**

192.168.208.138 / 192.168.208.138

Address

192.168.208.138 - (ipv4)
B8:97:5A:72:08:76 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.138 (PTR)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)
Misc Metrics (click to expand)

192.168.208.139 / 192.168.208.139

Address

192.168.208.139 - (ipv4)
B8:97:5A:72:28:D7 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.139 (PTR)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)
Misc Metrics (click to expand)

192.168.208.140 / 192.168.208.140

Address
192.168.208.140 - (ipv4)
00:21:5A:1E:37:62 - Hewlett Packard (mac)
Hostnames
192.168.208.140 (PTR)
Ports
The 997 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [1] | filtered [0])**	Service	Reason
139	tcp	open	tcpwrapped	syn-ack
445	tcp	open	tcpwrapped	syn-ack

Remote Operating System Detection
Used port: 445/tcp (open)
Used port: 3389/tcp (closed)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.141 / 192.168.208.141
Address
192.168.208.141 - (ipv4)
B8:97:5A:72:0A:24 - Biostar Microtech Int'l (mac)
Hostnames
192.168.208.141 (PTR)
Ports
The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
135	tcp	open	msrpc
1688	tcp	open	msrpc

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 or 2008 Beta 3 (100%)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.142 / 192.168.208.142
Address
192.168.208.142 - (ipv4)
B8:97:5A:8E:74:80 - Biostar Microtech Int'l (mac)
Hostnames
192.168.208.142 (PTR)
Ports
The 995 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
1688	tcp	open	msrpc	syn-ack	M
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.143 (click to expand)

192.168.208.144 / 192.168.208.144

Address

192.168.208.144 - (ipv4)
C8:9C:DC:FB:75:46 - Elitegroup Computer Systems (mac)

Hostnames

192.168.208.144 (PTR)

Ports

The 997 ports scanned but not shown below are in state: filtered

Port		State (toggle closed [1] | filtered [0])	Service	Reason	Produc
139	tcp	open	tcpwrapped	syn-ack	
445	tcp	open	tcpwrapped	syn-ack	Windo

Remote Operating System Detection

Used port: 445/tcp (open)
Used port: 3389/tcp (closed)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.145 / 192.168.208.145

Address

192.168.208.145 - (ipv4)
F0:92:1C:EA:13:8E - Hewlett Packard (mac)

Hostnames

192.168.208.145 (PTR)

Ports

The 997 ports scanned but not shown below are in state: filtered

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Produ
135	tcp	open	msrpc	syn-ack	Micro
139	tcp	open	netbios-ssn	syn-ack	Micro
445	tcp	open	microsoft-ds	syn-ack	Micro

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows 10 build 10586 - 14393 (95%)
OS match: Microsoft Windows 7 Professional or Windows 8 (93%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (93%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (91%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (91%)
OS match: Microsoft Windows 10 build 14393 (90%)
OS match: Microsoft Windows 10 build 10586 (90%)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (90%)
OS match: Microsoft Windows Embedded Standard 7 (90%)
OS match: Microsoft Windows 7 (89%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.146 / 192.168.208.146

Address

192.168.208.146 - (ipv4)
B8:97:5A:69:3C:04 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.146 (PTR)

Ports

The 995 ports scanned but not shown below are in state: filtered

Port		State (toggle closed [0] | filtered [0])	Service	Reason
135	tcp	open	msrpc	syn-ack

139	tcp	open	netbios-ssn	syn-ack	Microsoft Wind
445	tcp	open	microsoft-ds	syn-ack	Windows 8.1 F
1688	tcp	open	msrpc	syn-ack	Microsoft Wind
49155	tcp	open	msrpc	syn-ack	Microsoft Wind

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.147 / 192.168.208.147

Address
192.168.208.147 - (ipv4)
B8:97:5A:69:3B:67 - Biostar Microtech Int'l (mac)

Hostnames
192.168.208.147 (PTR)

Ports
The 994 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
1688	tcp	open	msrpc	syn-ack	M
2869	tcp	open	http	syn-ack	M
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.148 / 192.168.208.148

Address
192.168.208.148 - (ipv4)
B8:97:5A:7C:08:B2 - Biostar Microtech Int'l (mac)

Hostnames
192.168.208.148 (PTR)

Ports
The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.149 **(click to expand)**

192.168.208.150 / 192.168.208.150

Address

192.168.208.150 - (ipv4)
B8:97:5A:69:37:58 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.150 (PTR)

Ports

The 999 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
135	tcp	open	msrpc

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows 8.1 R1 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.151 **(click to expand)**

192.168.208.152 / 192.168.208.152

Address

192.168.208.152 - (ipv4)
B8:97:5A:D5:CA:1A - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.152 (PTR)

Ports

The 995 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
3389	tcp	open	ssl	syn-ack	M
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.153 / 192.168.208.153

Address

192.168.208.153 - (ipv4)
B8:97:5A:72:06:75 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.153 (PTR)

Ports

The 995 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W

2869	tcp	open	http	syn-ack	Microsoft HTTPA
49155	tcp	open	msrpc	syn-ack	Microsoft Window

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.154 / 192.168.208.154

Address

192.168.208.154 - (ipv4)
B8:97:5A:72:28:52 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.154 (PTR)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0]	filtered [0])**	Service	Reason	Pro
135	tcp	open	msrpc	syn-ack	Mic
139	tcp	open	netbios-ssn	syn-ack	Mic
445	tcp	open	microsoft-ds	syn-ack	Mic
49155	tcp	open	msrpc	syn-ack	Mic

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.155 **(click to expand)**

192.168.208.156 / 192.168.208.156

Address

192.168.208.156 - (ipv4)
B8:97:5A:72:18:EC - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.156 (PTR)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0]	filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Embedded Standard 7 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.157 **(click to expand)**

192.168.208.158 **(click to expand)**

192.168.208.159 **(click to expand)**

192.168.208.160 / 192.168.208.160

Address

192.168.208.160 - (ipv4)
00:1D:92:97:25:68 - Micro-star Int'l (mac)

Hostnames

192.168.208.160 (PTR)

Ports

The 998 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service
139	tcp	open	netbios-ssn
445	tcp	open	microsoft-ds

Remote Operating System Detection

Used port: 139/tcp (open)
OS match: Microsoft Windows 2000 SP4 (100%)
OS match: Microsoft Windows XP SP2 or SP3 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.161 / 192.168.208.161

Address

192.168.208.161 - (ipv4)
B8:97:5A:72:09:2E - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.161 (PTR)

Ports

The 991 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Pro
135	tcp	open	msrpc	syn-ack	Mic
139	tcp	open	netbios-ssn	syn-ack	Mic
445	tcp	open	microsoft-ds	syn-ack	Mic
5357	tcp	open	http	syn-ack	Mic
49152	tcp	open	msrpc	syn-ack	Mic
49153	tcp	open	msrpc	syn-ack	Mic
49154	tcp	open	msrpc	syn-ack	Mic
49155	tcp	open	msrpc	syn-ack	Mic
49156	tcp	open	msrpc	syn-ack	Mic

Remote Operating System Detection

Used port: 135/tcp (open)
Used port: 1/tcp (closed)
Used port: 31079/udp (closed)
OS match: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.162 **(click to expand)**

192.168.208.163 / 192.168.208.163

Address

192.168.208.163 - (ipv4)
B8:97:5A:72:09:61 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.163 (PTR)

Ports

The 995 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Pro
135	tcp	open	msrpc	syn-ack	Mic
139	tcp	open	netbios-ssn	syn-ack	Mic
445	tcp	open	microsoft-ds	syn-ack	Mic
1688	tcp	open	msrpc	syn-ack	Mic
49155	tcp	open	msrpc	syn-ack	Mic

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.164 / 192.168.208.164

Address

192.168.208.164 - (ipv4)
C8:9C:DC:EE:57:A0 - Elitegroup Computer Systems (mac)

Hostnames

192.168.208.164 (PTR)

Ports

The 997 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Produ
135	tcp	open	msrpc	syn-ack	Micro
139	tcp	open	netbios-ssn	syn-ack	Micro
445	tcp	open	microsoft-ds	syn-ack	Micro

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.165 / 192.168.208.165

Address

192.168.208.165 - (ipv4)
B8:97:5A:72:0D:F9 - Biostar Microtech Int'l (mac)

Hostnames

192.168.208.165 (PTR)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Pro
135	tcp	open	msrpc	syn-ack	Mic
139	tcp	open	netbios-ssn	syn-ack	Mic
445	tcp	open	microsoft-ds	syn-ack	Mic
49155	tcp	open	msrpc	syn-ack	Mic

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)
OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.166 **(click to expand)**

192.168.208.167 / 192.168.208.167

Address

192.168.208.167 - (ipv4)
00:21:B7:7A:8C:21 - Lexmark International (mac)

Hostnames

192.168.208.167 (PTR)

Ports

The 986 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Product
21	tcp	open	ftp	syn-ack	Lexmark E360dn prir
79	tcp	open	finger	syn-ack	Lexmark E360dn prir
80	tcp	open	http	syn-ack	thttpd
515	tcp	open	printer	syn-ack	Lexmark lpd service
631	tcp	open	http	syn-ack	thttpd
5000	tcp	open	upnp	syn-ack	
5001	tcp	open	tcpwrapped	syn-ack	
6100	tcp	open	synchronet-db	syn-ack	
8000	tcp	open	http	syn-ack	thttpd
9000	tcp	open	telnet	syn-ack	Lexmark E360dn prir
9100	tcp	open	jetdirect	syn-ack	
9200	tcp	open	ir-alerts	syn-ack	Lexmark E360dn prir
9500	tcp	open	ismserver	syn-ack	
10000	tcp	open	printer-admin	syn-ack	Lexmark printer adm

Remote Operating System Detection

Used port: 21/tcp (open)
Used port: 1/tcp (closed)
Used port: 40903/udp (closed)
OS match: Dell 2350dn, IBM InfoPrint 1832; or Lexmark C544dn, T612, T650, or X464de printer (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.168 **(click to expand)**

192.168.208.169 **(click to expand)**

192.168.208.170 / 192.168.208.170

Address

192.168.208.170 - (ipv4)
00:08:54:6A:CA:5D - Netronix (mac)

Hostnames

192.168.208.170 (PTR)

Ports

The 997 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [1] | filtered [0])**
139	tcp	open
445	tcp	open

Remote Operating System Detection

Used port: 445/tcp (open)
Used port: 3389/tcp (closed)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.171 **(click to expand)**

192.168.208.172 **(click to expand)**
192.168.208.173 **(click to expand)**
192.168.208.174 **(click to expand)**
192.168.208.175 **(click to expand)**
192.168.208.176 **(click to expand)**
192.168.208.177 **(click to expand)**
192.168.208.178 **(click to expand)**
192.168.208.179 **(click to expand)**
192.168.208.180 **(click to expand)**
192.168.208.181 **(click to expand)**
192.168.208.182 **(click to expand)**
192.168.208.183 **(click to expand)**
192.168.208.184 **(click to expand)**
192.168.208.185 **(click to expand)**
192.168.208.186 **(click to expand)**
192.168.208.187 **(click to expand)**
192.168.208.188 **(click to expand)**
192.168.208.189 **(click to expand)**
192.168.208.190 **(click to expand)**
192.168.208.191 **(click to expand)**
192.168.208.192 **(click to expand)**
192.168.208.193 **(click to expand)**
192.168.208.194 **(click to expand)**
192.168.208.195 **(click to expand)**
192.168.208.196 **(click to expand)**
192.168.208.197 **(click to expand)**
192.168.208.198 **(click to expand)**
192.168.208.199 **(click to expand)**

192.168.208.200 / 192.168.208.200

Address

192.168.208.200 - (ipv4)
00:25:36:4E:F9:86 - Oki Electric Industry (mac)

Hostnames

192.168.208.200 (PTR)

Ports

The 995 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
139	tcp	open	microsoft-ds
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection

Used port: 80/tcp (open)
Used port: 1/tcp (closed)
Used port: 38384/udp (closed)
OS match: Oki network printer (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.201 / 192.168.208.201

Address

192.168.208.201 - (ipv4)
00:25:36:EE:AF:C9 - Oki Electric Industry (mac)

Hostnames

192.168.208.201 (PTR)

Ports

The 994 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
139	tcp	open	microsoft-ds
443	tcp	open	tcpwrapped
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection

Used port: 80/tcp (open)
Used port: 1/tcp (closed)
Used port: 40480/udp (closed)
OS match: Samsung CLP-770ND printer (94%)
OS match: Samsung SMT-i5220 or SMT-i3100 VoIP phone (94%)
OS match: Samsung CLP-620ND, CLX-3185, CLX-6220FX, ML-1865W, ML-2580N, or ML-3312ND; or Xerox Phaser 3300MFP printer (92%)
OS match: Xerox Phaser 3435 printer (92%)
OS match: Enterasys B5 switch (91%)
OS match: Rockwell Automation Logix EtherNet/IP module (91%)
OS match: Dell PowerConnect 6248, or Enterasys B3 BG3124 or D2 D2G124 switch (91%)
OS match: Dell PowerConnect 6248, Enterasys C3 C3G124 or Netgear GSM7328Sv2 switch (91%)
OS match: Dell PowerConnect 8024F switch (91%)
OS match: Allen-Bradley 1756-EN2T/C programmable logic controller (90%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.202 / 192.168.208.202

Address

192.168.208.202 - (ipv4)
00:25:36:EE:1F:D6 - Oki Electric Industry (mac)

Hostnames

192.168.208.202 (PTR)

Ports

The 994 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
139	tcp	open	microsoft-ds
443	tcp	open	tcpwrapped
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection

Used port: 80/tcp (open)
Used port: 1/tcp (closed)
Used port: 36570/udp (closed)
OS match: Samsung CLP-770ND printer (94%)
OS match: Samsung SMT-i5220 or SMT-i3100 VoIP phone (94%)
OS match: Samsung CLP-620ND, CLX-3185, CLX-6220FX, ML-1865W, ML-2580N, or ML-3312ND; or Xerox Phaser 3300MFP printer (92%)

OS match: Xerox Phaser 3435 printer (92%)
OS match: Dell PowerConnect 8024F switch (91%)
OS match: Enterasys B5 switch (91%)
OS match: Rockwell Automation Logix EtherNet/IP module (91%)
OS match: Fuji Xerox ApeosPort IV C2275 printer (91%)
OS match: Dell PowerConnect 6248, or Enterasys B3 BG3124 or D2 D2G124 switch (91%)
OS match: Dell PowerConnect 6248, Enterasys C3 C3G124 or Netgear GSM7328Sv2 switch (91%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.203 / 192.168.208.203

Address

192.168.208.203 - (ipv4)
00:25:36:EE:4F:56 - Oki Electric Industry (mac)

Hostnames

192.168.208.203 (PTR)

Ports

The 994 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
139	tcp	open	microsoft-ds
443	tcp	open	tcpwrapped
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection

Used port: 80/tcp (open)
Used port: 1/tcp (closed)
Used port: 30591/udp (closed)
OS match: Samsung CLP-770ND printer (94%)
OS match: Samsung SMT-i5220 or SMT-i3100 VoIP phone (94%)
OS match: Samsung CLP-620ND, CLX-3185, CLX-6220FX, ML-1865W, ML-2580N, or ML-3312ND; or Xerox Phaser 3300MFP printer (92%)
OS match: Xerox Phaser 3435 printer (92%)
OS match: Dell PowerConnect 8024F switch (91%)
OS match: Enterasys B5 switch (91%)
OS match: Rockwell Automation Logix EtherNet/IP module (91%)
OS match: Fuji Xerox ApeosPort IV C2275 printer (91%)
OS match: Dell PowerConnect 6248, or Enterasys B3 BG3124 or D2 D2G124 switch (91%)
OS match: Dell PowerConnect 6248, Enterasys C3 C3G124 or Netgear GSM7328Sv2 switch (91%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.204

Address

192.168.208.204 - (ipv4)
B8:97:5A:72:17:79 - Biostar Microtech Int'l (mac)

Ports

The 995 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	W
7070	tcp	open	realserver	syn-ack	
49155	tcp	open	msrpc	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: Microsoft Windows Server 2008 R2 or Windows 8.1 (100%)
OS match: Microsoft Windows 7 Professional or Windows 8 (100%)
OS match: Microsoft Windows Phone 7.5 or 8.0 (100%)

OS match: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (100%)
OS match: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.205

Address

192.168.208.205 - (ipv4)
00:25:36:BE:CC:13 - Oki Electric Industry (mac)

Ports

The 994 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
139	tcp	open	microsoft-ds
443	tcp	open	tcpwrapped
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection

Used port: 80/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.206

Address

192.168.208.206 - (ipv4)
00:25:36:BE:CC:F3 - Oki Electric Industry (mac)

Ports

The 995 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
443	tcp	open	tcpwrapped
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection

Used port: 80/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.207

Address

192.168.208.207 - (ipv4)
C8:9C:DC:FB:76:47 - Elitegroup Computer Systems (mac)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	P
135	tcp	open	msrpc	syn-ack	M
139	tcp	open	netbios-ssn	syn-ack	M
445	tcp	open	microsoft-ds	syn-ack	M
2869	tcp	open	http	syn-ack	M

Remote Operating System Detection

Used port: 135/tcp (open)

OS match: iPXE 1.0.0+ (100%)
OS match: Tomato 1.28 (Linux 2.4.20) (100%)
OS match: Tomato firmware (Linux 2.6.22) (100%)
OS match: Sony Ericsson U8i Vivaz mobile phone (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.208 **(click to expand)**

192.168.208.209

Address

192.168.208.209 - (ipv4)
44:87:FC:E2:65:B7 - Elitegroup Computer Systems (mac)

Ports

The 997 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Produ
135	tcp	open	msrpc	syn-ack	Micro
139	tcp	open	netbios-ssn	syn-ack	Micro
445	tcp	open	microsoft-ds	syn-ack	Micro

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: iPXE 1.0.0+ (100%)
OS match: Tomato 1.28 (Linux 2.4.20) (100%)
OS match: Tomato firmware (Linux 2.6.22) (100%)
OS match: Sony Ericsson U8i Vivaz mobile phone (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.210 **(click to expand)**

192.168.208.211

Address

192.168.208.211 - (ipv4)
00:25:36:BE:CC:A4 - Oki Electric Industry (mac)

Ports

The 995 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
23	tcp	open	telnet
80	tcp	open	http
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection

Used port: 23/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.212

Address

192.168.208.212 - (ipv4)
00:25:36:BE:CC:E4 - Oki Electric Industry (mac)

Ports

The 993 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
23	tcp	open	telnet
80	tcp	open	http
139	tcp	open	microsoft-ds

443	tcp	open	tcpwrapped	s
515	tcp	open	printer	s
631	tcp	open	ipp	s
9100	tcp	open	jetdirect	s

Remote Operating System Detection
Used port: 23/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.213

Address
192.168.208.213 - (ipv4)
00:25:36:BE:CC:64 - Oki Electric Industry (mac)

Ports
The 994 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
139	tcp	open	microsoft-ds
443	tcp	open	tcpwrapped
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection
Used port: 80/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.214

Address
192.168.208.214 - (ipv4)
00:25:36:BE:CC:14 - Oki Electric Industry (mac)

Ports
The 995 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
80	tcp	open	http
443	tcp	open	tcpwrapped
515	tcp	open	printer
631	tcp	open	ipp
9100	tcp	open	jetdirect

Remote Operating System Detection
Used port: 80/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.215 **(click to expand)**

192.168.208.216

Address
192.168.208.216 - (ipv4)
B8:97:5A:72:0C:EB - Biostar Microtech Int'l (mac)

Ports
The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0]	filtered [0])**	Service	Reason	Product
135	tcp	open	msrpc	syn-ack	Microsoft Windows
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows
49155	tcp	open	msrpc	syn-ack	Microsoft Windows

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: iPXE 1.0.0+ (100%)
OS match: Tomato 1.28 (Linux 2.4.20) (100%)
OS match: Tomato firmware (Linux 2.6.22) (100%)
OS match: Sony Ericsson U8i Vivaz mobile phone (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.217 **(click to expand)**

192.168.208.218 **(click to expand)**

192.168.208.219 **(click to expand)**

192.168.208.220 **(click to expand)**

192.168.208.221

Address
192.168.208.221 - (ipv4)
C8:9C:DC:EE:58:66 - Elitegroup Computer Systems (mac)

Ports
The 1000 ports scanned but not shown below are in state: filtered

Remote Operating System Detection
Unable to identify operating system.

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.222 **(click to expand)**

192.168.208.223 **(click to expand)**

192.168.208.224 **(click to expand)**

192.168.208.225 **(click to expand)**

192.168.208.226 **(click to expand)**

192.168.208.227 **(click to expand)**

192.168.208.228 **(click to expand)**

192.168.208.229 **(click to expand)**

192.168.208.230 **(click to expand)**

192.168.208.231 **(click to expand)**

192.168.208.232

Address
192.168.208.232 - (ipv4)
8C:89:A5:89:9F:21 - Micro-Star INT'L (mac)

Ports
The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0]	filtered [0])**	Service	Reason	Prod
135	tcp	open	msrpc	syn-ack	Micr
139	tcp	open	netbios-ssn	syn-ack	Micr
445	tcp	open	microsoft-ds	syn-ack	Micr
1688	tcp	open	msrpc	syn-ack	Micr

Remote Operating System Detection
Used port: 135/tcp (open)
OS match: iPXE 1.0.0+ (100%)
OS match: Tomato 1.28 (Linux 2.4.20) (100%)

OS match: Tomato firmware (Linux 2.6.22) (100%)
OS match: Sony Ericsson U8i Vivaz mobile phone (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.233 **(click to expand)**

192.168.208.234 **(click to expand)**

192.168.208.235 **(click to expand)**

192.168.208.236 **(click to expand)**

192.168.208.237 **(click to expand)**

192.168.208.238 **(click to expand)**

192.168.208.239 **(click to expand)**

192.168.208.240 **(click to expand)**

192.168.208.241 **(click to expand)**

192.168.208.242 **(click to expand)**

192.168.208.243 **(click to expand)**

192.168.208.244 **(click to expand)**

192.168.208.245 **(click to expand)**

192.168.208.246

Address

192.168.208.246 - (ipv4)
A0:1E:0B:01:AD:A2 - Minix Technology Limited (mac)

Ports

The 999 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service
7999	tcp	open	nagios-

Remote Operating System Detection

Used port: 7999/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.247 **(click to expand)**

192.168.208.248

Address

192.168.208.248 - (ipv4)
00:15:5D:D0:EF:00 - Microsoft (mac)

Ports

The 995 ports scanned but not shown below are in state: closed

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Product
22	tcp	open	ssh	syn-ack	OpenSSH
80	tcp	open	http	syn-ack	Apache httpd
443	tcp	open	http	syn-ack	Apache httpd
8000	tcp	open	http-alt	syn-ack	
8080	tcp	open	http	syn-ack	Apache Tomcat/Co

Remote Operating System Detection

Used port: 22/tcp (open)
Used port: 1/tcp (closed)
OS match: Fortinet FortiGate 100D firewall (87%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.249 **(click to expand)**

192.168.208.250 **(click to expand)**

192.168.208.251

Address

192.168.208.251 - (ipv4)
64:31:50:45:61:E7 - Hewlett Packard (mac)

Ports

The 996 ports scanned but not shown below are in state: filtered

Port		State **(toggle closed [0] | filtered [0])**	Service	Reason	Pro
135	tcp	open	msrpc	syn-ack	Mic
139	tcp	open	netbios-ssn	syn-ack	Mic
445	tcp	open	microsoft-ds	syn-ack	Mic
3389	tcp	open	ms-wbt-server	syn-ack	Mic

Remote Operating System Detection

Used port: 135/tcp (open)
OS match: iPXE 1.0.0+ (100%)
OS match: Tomato 1.28 (Linux 2.4.20) (100%)
OS match: Tomato firmware (Linux 2.6.22) (100%)
OS match: Sony Ericsson U8i Vivaz mobile phone (100%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

192.168.208.252 **(click to expand)**

192.168.208.253 **(click to expand)**

192.168.208.254 **(click to expand)**

192.168.208.255 **(click to expand)**

Go to top
Toggle Closed Ports
Toggle Filtered Ports

ANEXO 6: Statement of Applicability SoA – Declaración de aplicabilidad

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
5. POLÍTICAS DE SEGURIDAD	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de políticas para la seguridad de la información.	SI	Se requiere un conjunto de políticas y medidas que permitan gestionar la seguridad de la información de la Entidad	Se emitió acuerdo No. PSAA14-10279 Por el cual se aprueban las políticas y procedimientos de Seguridad de la Información para la Rama Judicial				X
		5.1.2 Revisión de las políticas para la seguridad de la información.	SI	Es necesario que dichas políticas sean revisadas y socializadas con la Entidad y partes interesadas	Se emitió acuerdo No. PSAA14-10279 Por el cual se aprueban las políticas y procedimientos de Seguridad de la Información para la Rama Judicial. Las políticas se encuentran publicadas sistema de relatoría de la Rama Judicial				X
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización interna	6.1.1 Asignación de responsabilidades para la seguridad de la información.	SI	Es pertinente tener asignadas las responsabilidades, de acuerdo a los cargos y perfiles de los servidores judiciales encargados de la administración de la infraestructura	Manuales de funciones			X	
		6.1.2 Segregación de tareas.	SI	Por políticas de gestión del talento humano, es necesario la segregación de taras, de acuerdo a los cargos y perfiles de los servidores judiciales encargados de la administración de la infraestructura	Planes operativos por proceso			X	
		6.1.3 Contacto con las autoridades.	SI	Dentro de los principios de la administración de justicia se incluye la cooperación interinstitucional y con autoridades del estado	Acuerdos de cooperación interinstitucional	X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		6.1.4 Contacto con grupos de interés especial.	SI	Se evidencia cooperación interinstitucional con otras entidades del Estado, sin embargo el intercambio de información se realiza de una manera formal y no sistematizada o a través de webservices	Acuerdos de cooperación interinstitucional	X			
		6.1.5 Seguridad de la información en la gestión de proyectos.	NO	A nivel de la Seccional Armenia, no se gestionan proyectos relacionados con la infraestructura tecnológica, debido a la contratación no delegable, establecida desde el nivel central	N/A			X	
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad.	SI	Se debe garantizar la seguridad que requiere el tratamiento de la información susceptible de ser transmitida mediante el uso de las Tecnologías de la información y las comunicaciones (TIC), cuando se utilizan equipos o dispositivos de comunicación móvil para realizar funciones o actividades de teletrabajo y cumplimiento de funciones extra despacho en la Rama Judicial	Política de dispositivos móviles, teletrabajo y cumplimiento de funciones por fuera de las redes y sistemas de la rama judicial Política de uso de dispositivos móviles	X			
		6.2.2 Teletrabajo.	SI	Ley 1221 de 2008 “por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones” Guía Jurídica de Implementación	Política de dispositivos móviles, teletrabajo y cumplimiento de funciones por fuera de las redes y sistemas de la rama judicial	X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
				del Teletrabajo de mayo de 2013, Ministerio del trabajo y la seguridad social					
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	7.1 Antes de la contratación	7.1.1 Investigación de antecedentes.	SI	La Entidad debe procurar por contratar personal idóneo, competente y con altos niveles de ética e integridad	Lista de chequeo para contratación, que incluye certificaciones sobre antecedentes	X			
		7.1.2 Términos y condiciones de contratación.	SI	Los términos de los procesos contractuales, deben ser claros y trasparentes	Proceso de administración de la carrera judicial Proceso de adquisición de bienes y servicios	X			
	7.2 Durante la contratación	7.2.1 Responsabilidades de gestión.	SI	Es necesario tener responsabilidades completamente definidas para cada uno de los servidores judiciales	Procedimientos y caracterizaciones del SIGC Manual de políticas de seguridad de la información	X			
		7.2.2 Concienciación, educación y capacitación en seguridad de la información	SI	Es obligación de la Rama Judicial, formar a los servidores judiciales en las competencias relacionadas con su cargo	Plan de desarrollo de competencias	X			
		7.2.3 Proceso disciplinario.	SI	La entidad debe procurar por el buen comportamiento y la honorabilidad de todos sus servidores judiciales Ley 734 de 2002, Por la cual se expide el Código Disciplinario Único. "Artículo 34, Deberes. Numeral 4 Utilizar los bienes y recursos asignados para el	Procedimiento Sala disciplinaria del Consejo Seccional de la Judicatura	X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
				desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos."					
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo.	SI	La Entidad debe definir las pautas generales para asegurar una adecuada gestión del acceso a la información y prevenir accesos no autorizados a los sistemas de información y servicios de la Rama Judicial cuando se produce desvinculación, cambios de función, ausencias temporales o vacaciones de los usuarios de los sistemas de información.	Política de desvinculación cambio de funciones, ausencia temporal o vacaciones			X	
8. GESTIÓN DE ACTIVOS	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos.	SI	Se debe guardar registro de todos los activos y bienes devolutivos en custodia de los servidores judiciales	Sistema de inventario de bienes y activos SICOF ERP				X
		8.1.2 Propiedad de los activos.	SI	Todos los activos con que cuenta la Rama Judicial, son propiedad de la Nación	Sistema de inventario de bienes y activos SICOF ERP				X
		8.1.3 Uso aceptable de los activos.	SI	Se debe garantizar el uso responsable de los activos al servicio de la administración de justicia	Procedimiento para la administración de bienes y servicios				X

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		8.1.4 Devolución de activos.	SI	Los activos en custodia de los servidores judiciales, deben ser reintegrados cuando dicho servidor cambie de cargo o deje la Entidad	Procedimiento baja de bienes inservibles y obsoletos Procedimiento para la salida de elementos de almacén por requerimientos Formato acta de traspaso entre empleados elementos de inventario individual				X
	8.2 Clasificación de la información	8.2.1 Directrices de clasificación.	SI	Asegurar que la información recibe un nivel de protección apropiado de acuerdo con su importancia para la Rama Judicial. Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	Política de clasificación de la información	X			
		8.2.2 Etiquetado y manipulado de la información.	SI			X			
		8.2.3 Manipulación de activos.	SI			X			
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles.	SI	Medidas necesarias para evitar que la información reservada de la Rama Judicial se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos ajenos a la entidad.	Política Trae tu propio dispositivo (BYOD, Bring Your Own Device)			X	
		8.3.2 Eliminación de soportes.	SI	Se debe asegurar la disposición final segura de todos los elementos o dispositivos que contengan información de la Rama Judicial, cuando se den de baja o sean reutilizados.	Política para la eliminación y destrucción de medios			X	

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		8.3.3 Soportes físicos en tránsito.	SI	Es necesario proteger la información para que esta no sea extraída de manera ilegal, fuera de la Entidad Mantener la seguridad de la información cuando se autoriza el intercambio de la misma dentro de la Rama Judicial y con cualquier entidad externa.	Política Trae tu propio dispositivo (BYOD, Bring Your Own Device) Política de Transferencia de Información			X	
9. CONTROL DE ACCESOS	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos.	SI	Definir las pautas generales para asegurar un acceso seguro y controlado a la información de la Rama Judicial, impidiendo los accesos no autorizados. Ley 1712 de 6 de marzo de 2014, Por medio de la cual se crea la ley de transparencia y acceso a la información pública nacional y se dictan otras disposiciones	Política de control de acceso a la información Política de control de acceso físico				X
		9.1.2 Control de acceso a las redes y servicios asociados.	SI	Definir las pautas generales para asegurar un acceso controlado a los componentes de tecnología de información de la Rama Judicial	Control de Acceso a Componentes de tecnología de Información y Comunicaciones				X
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios.	SI	Definir las pautas generales para asegurar el uso controlado y seguro de las cuentas para el acceso a los Sistemas de información y Servicios de la Rama Judicial	Cuentas para acceso a sistemas de información				X
		9.2.2 Gestión de los derechos de acceso	SI						X

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		asignados a usuarios.							
		9.2.3 Gestión de los derechos de acceso con privilegios especiales.	SI						X
		9.2.4 Gestión de información confidencial de autenticación de usuarios.	SI						X
		9.2.5 Revisión de los derechos de acceso de los usuarios.	SI	Definir las pautas generales para asegurar un acceso seguro y controlado a la información de la Rama Judicial, impidiendo los accesos no autorizados.	Política de control de acceso a la información				X
		9.2.6 Retirada o adaptación de los derechos de acceso	SI	Definir las pautas generales para asegurar una adecuada gestión del acceso a la información y prevenir accesos no autorizados a los sistemas de información y servicios de la Rama Judicial cuando se produce desvinculación, cambios de función, ausencias temporales o vacaciones de los usuarios de los sistemas de información.	Política de desvinculación cambio de funciones, ausencia temporal o vacaciones				X

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación.	SI	Asegurar que la información recibe un nivel de protección apropiado de acuerdo con su importancia para la Rama Judicial. En cumplimiento a lo dispuesto en la Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013 sobre protección de datos, la Rama Judicial establece la siguiente política de tratamiento de datos personales con el propósito de que todas las personas puedan conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en las bases de datos o archivos a cargo de esta entidad.	Política de clasificación de la información Política de tratamiento de datos personales	X			
	9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información.	SI	Definir las pautas generales para asegurar el uso controlado y seguro de las cuentas para el acceso a los Sistemas de información y Servicios de la Rama Judicial	Cuentas para acceso a sistemas de información			X	
		9.4.2 Procedimientos seguros de inicio de sesión.	SI					X	

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		9.4.3 Gestión de contraseñas de usuario.	SI	Se deben Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, usando claves fuertes Ley 1273 de 2009, "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".	Política de claves			X	
		9.4.4 Uso de herramientas de administración de sistemas.	SI	Asegurar que el software sea adquirido o desarrollado con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información.	Política de adquisición, desarrollo y mantenimiento de software			X	
		9.4.5 Control de acceso al código fuente de los programas	SI					X	
10. CIFRADO	10.1 Controles criptográficos	10.1.1 Política de uso de los controles criptográficos.	SI	Definir la gestión de controles criptográficos para el envío o recepción de información en medios electrónicos protegiendo la confidencialidad, integridad y trazabilidad de la información.	Política de controles criptográficos				X

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		10.1.2 Gestión de claves.	SI	Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, usando claves fuertes.	Política de claves				X
11. SEGURIDAD FÍSICA Y AMBIENTAL	11.1 Áreas seguras	11.1.1 Perímetro de seguridad física.	SI	Evitar el acceso físico no autorizado de personal, el daño o la interferencia de las instalaciones y la información de la organización.	Política de control de acceso físico	X			
		11.1.2 Controles físicos de entrada.	SI			X			
		11.1.3 Seguridad de oficinas, despachos y recursos.	SI			X			
		11.1.4 Protección contra las amenazas externas y ambientales.	SI	Toda vez que el Quindío se encuentra en un área geográfica susceptible a desastres naturales, es necesario tomas las medidas de salvaguarda al respecto	Política de respaldo de la información	X			
		11.1.5 El trabajo en áreas seguras.	SI	Es necesario velar por la integridad de los servidores judiciales	Manual de espacios físicos saludables Contrato ARL	X			
		11.1.6 Áreas de acceso público, carga y descarga.	SI	Es necesario velar por la integridad de publico y visitantes	Proceso de administración de la seguridad Proceso de mantenimiento y mejoramiento de la infraestructura física	X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
	11.2 Seguridad de los equipos	11.2.1 Emplazamiento y protección de equipos.	SI	Se debe contar con las medidas de protección de equipos, para evitar que estos sufran daño por falta de condiciones optimas de funcionamiento	Revisión periódica a los elementos de protección de equipos que se tienen establecidos tales como pico protectores, ups, líneas a tierra Contrato de seguro de todos los activos de la Entidad	X			
		11.2.2 Instalaciones de suministro.	SI	Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso los proveedores o terceros que prestan sus servicios para la Rama Judicial	Política de seguridad de la información para relaciones con proveedores	X			
		11.2.3 Seguridad del cableado.	SI	Se debe garantizar la seguridad y no exposición de la infraestructura LAN y demás cableado estructurado que soporta el funcionamiento de la Entidad	Directrices para la construcción, mantenimiento y adecuación de cableado estructurado	X			
		11.2.4 Mantenimiento de los equipos.	SI	La Rama Judicial, debe garantizar el buen funcionamiento de los equipos tecnológicos con que cuenta	Contrato de mesa de ayuda Contrato de mantenimiento de equipos	X			
		11.2.5 Salida de activos fuera de las dependencias de la empresa.	NO	No se contempla la utilización de equipos por fuera de la Entidad	N/A	X			
		11.2.6 Seguridad de los equipos y activos fuera de	NO			X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		las instalaciones.							
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	SI	Definir las medidas necesarias para evitar que la información reservada de la Rama Judicial se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos ajenos a la entidad.	Política Trae tu propio dispositivo (BYOD, Bring Your Own Device)	X			
		11.2.8 Equipo informático de usuario desatendido.	SI	Pautas generales para asegurar una adecuada gestión del acceso a la información y prevenir accesos no autorizados a los sistemas de información y servicios de la Rama Judicial cuando se produce desvinculación, cambios de función, ausencias temporales o vacaciones de los usuarios de los sistemas de información.	Política de desvinculación cambio de funciones, ausencia temporal o vacaciones	X			
		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	SI	Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida o daño de la información disponible de los puestos de trabajo durante y fuera del horario trabajo normal de los funcionarios, contratistas y terceros que prestan sus servicios a la Rama Judicial	Política de escritorio limpio y pantalla limpia	X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
12. SEGURIDAD EN LA OPERATIVA	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.	SI	Definir las pautas generales para asegurar un acceso seguro y controlado a la información de la Rama Judicial, impidiendo los accesos no autorizados.	Política de control de acceso a la información			X	
		12.1.2 Gestión de cambios.	SI	Garantizar que los cambios sobre la infraestructura de tecnología de información, los servicios por terceras partes, procedimientos, controles y comunicaciones en la Rama Judicial se realicen e implementen adecuadamente siguiendo procedimientos estándar	Política de Gestión de Cambios			X	
		12.1.3 Gestión de capacidades.	SI	Pautas generales para asegurar un acceso controlado a los componentes de tecnología de información de la Rama Judicial	Control de Acceso a Componentes de tecnología de Información y Comunicaciones			X	
		12.1.4 Separación de entornos de desarrollo, prueba y producción.	SI	Asegurar que el software sea adquirido o desarrollado con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información.	Política de adquisición, desarrollo y mantenimiento de software				X
	12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso.	SI	Definir las pautas generales para asegurar una adecuada protección de la información de la Rama Judicial contra software malicioso.	Política de Antivirus				X

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
	12.3 Copias de seguridad	12.3.1 Copias de seguridad de la información.	SI	Definir las pautas generales para garantizar en la Rama Judicial la ejecución, preservación, mantenimiento y verificación de copias de respaldo de la información. El respaldo de la información busca reducir los impactos de los riesgos generados por la pérdida de información y es un mecanismo para soportar los planes de contingencia, recuperación ante desastres y atención a incidentes de seguridad de la información adoptados por la Entidad.	Política de respaldo de información				X
	12.4 Registro de actividad y supervisión	12.4.1 Registro y gestión de eventos de actividad.	SI	Definir las pautas generales para asegurar un adecuado uso y administración de los activos informáticos de la Rama Judicial por parte del personal a cargo de su administración.	Política Uso aceptable de los Activos	X			
		12.4.2 Protección de los registros de información.	SI	Definir las pautas generales para asegurar un acceso seguro y controlado a la información de la Rama Judicial, impidiendo los accesos no autorizados. Definir las pautas generales para garantizar en la Rama Judicial la ejecución, preservación, mantenimiento y verificación de	Política de control de acceso a la información Política de respaldo de la información	X			
		12.4.3 Registros de actividad del administrador y operador del sistema.	SI			X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
				copias de respaldo de la información. El respaldo de la información busca reducir los impactos de los riesgos generados por la pérdida de información y es un mecanismo para soportar los planes de contingencia, recuperación ante desastres y atención a incidentes de seguridad de la información adoptados por la Entidad.					
		12.4.4 Sincronización de relojes.	SI	Pautas generales para asegurar un acceso controlado a los componentes de tecnología de información de la Rama Judicial	Control de Acceso a Componentes de tecnología de Información y Comunicaciones	X			
	12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción.	SI	Asegurar que el software sea adquirido o desarrollado con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información.	Política de adquisición, desarrollo y mantenimiento de software				X
	12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas.	SI	Asegurar que el software sea adquirido o desarrollado con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información.	Política de adquisición, desarrollo y mantenimiento de software				X
		12.6.2 Restricciones en la instalación de software.	SI						X

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información	SI	Se debe garantizar el funcionamiento y operatividad de los sistemas de información con que cuenta la Entidad, así como bloquear su uso no autorizado	Auditorias internas MECI Política de claves	X			
13. SEGURIDAD EN LAS TELECOMUNICACIONES	13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red.	SI	pautas generales para asegurar un acceso seguro y controlado a la información de la Rama Judicial, impidiendo los accesos no autorizados pautas generales para asegurar una adecuada protección de la información de la Rama Judicial en el uso del servicio de Internet por parte de los usuarios autorizados	Política de control de acceso a la información Política de uso de servicios de acceso a Internet			X	
		13.1.2 Mecanismos de seguridad asociados a servicios en red.	SI					X	
		13.1.3 Segregación de redes.	SI					X	
	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información.	SI	pautas generales para asegurar una adecuada protección de la información de la Rama Judicial cuando se usa el servicio de correo electrónico por parte de los usuarios autorizados Asegurar que todos los funcionarios, contratistas, contratistas y terceros que prestan sus servicios a la Rama Judicial mejoran continuamente su conciencia en seguridad de la información y de cómo sus actividades diarias contribuyen al	Política de uso de correo electrónico Política de Formación y toma de conciencia en seguridad de la información	X			
		13.2.2 Acuerdos de intercambio.	SI			X			
		13.2.3 Mensajería electrónica.	SI			X			
		13.2.4 Acuerdos de confidencialidad y secreto.	SI			X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
				logro de los objetivos de la seguridad de la información					
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad.	SI	Ley 734 de 2002, Por la cual se expide el Código Disciplinario Único. "Artículo 34, Deberes. Numeral 4 Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos." Componentes de Elementos Transversales del manual 3.1 Gobierno en Línea, actividad 3, el cual dice "Implementar un sistema de Gestión de TI, el cual establece la sostenibilidad y mejoramiento que permita articular el uso de la tecnología con los objetivos misionales de las entidades. Así mismo, se requiere una estrategia de monitoreo, de forma tal que se puedan establecer avances y correctivos que permitan la adopción de buenas prácticas y tendencias tanto locales como globales".	Política de adquisición, desarrollo y mantenimiento de software			X	

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	SI	pautas generales para asegurar una adecuada protección de la información de la Rama Judicial cuando se usa el servicio de correo electrónico por parte de los usuarios autorizados Asegurar que todos los funcionarios, contratistas, contratistas y terceros que prestan sus servicios a la Rama Judicial mejoran continuamente su conciencia en seguridad de la información y de cómo sus actividades diarias contribuyen al logro de los objetivos de la seguridad de la información	Política de uso de correo electrónico Política de Formación y toma de conciencia en seguridad de la información			X	
		14.1.3 Protección de las transacciones por redes telemáticas.	SI					X	
	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro de software.	SI	Asegurar que el software sea adquirido o desarrollado con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información. Componentes de Elementos Transversales del manual 3.1 Gobierno en Línea, actividad 3, el cual dice “Implementar un sistema de Gestión de TI, el cual establece la sostenibilidad y mejoramiento que permita articular el uso de la tecnología con los objetivos misionales de las entidades. Así	Política de adquisición, desarrollo y mantenimiento de software			X	
		14.2.2 Procedimientos de control de cambios en los sistemas.	SI					X	
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el	SI					X	

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		sistema operativo.		mismo, se requiere una estrategia de monitoreo, de forma tal que se puedan establecer avances y correctivos que permitan la adopción de buenas prácticas y tendencias tanto locales como globales".					
		14.2.4 Restricciones a los cambios en los paquetes de software.	SI					X	
		14.2.5 Uso de principios de ingeniería en protección de sistemas.	SI					X	
		14.2.6 Seguridad en entornos de desarrollo.	SI					X	
		14.2.7 Externalización del desarrollo de software.	SI					X	
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	SI					X	
		14.2.9 Pruebas de aceptación.	SI					X	
	14.3 Datos de prueba	14.3.1 Protección de	SI	Asegurar que el software sea adquirido o desarrollado con los	Política de adquisición, desarrollo y mantenimiento de software				X

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		los datos utilizados en pruebas.		controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información					
15. RELACIONES CON SUMINISTRADORES	15.1 Seguridad de la información en las relaciones con suministradores	15.1.1 Política de seguridad de la información para suministradores .	SI	Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso los proveedores o terceros que prestan sus servicios para la Rama Judicial	Política de seguridad de la información para relaciones con proveedores	X			
		15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores .	SI			X			
		15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones .	SI	Asegurar que el software sea adquirido o desarrollado con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información.	Política de adquisición, desarrollo y mantenimiento de software	X			
	15.2 Gestión de la prestación del servicio por suministradores	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	SI	Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso los proveedores o terceros que prestan sus servicios para la Rama Judicial	Política de seguridad de la información para relaciones con proveedores Procedimiento para evaluación y reevaluación de proveedores Manual de supervisión de contratos	X			
		15.2.2 Gestión de cambios en los servicios	SI			X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		prestados por terceros.							
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos.	SI	Proteger la integridad, disponibilidad y confidencialidad de la información de la Rama Judicial, prevenir la perdida de servicios y cumplir con requerimientos legales. Esta política establece los mecanismos de coordinación para dar respuesta a los incidentes de seguridad de la información y habilita a la Rama Judicial para una remediación rápida, recopilación de datos y reporte de los eventos que afectan la infraestructura de información y tecnología	Política de gestión de incidentes de seguridad de la información			X	
		16.1.2 Notificación de los eventos de seguridad de la información.	SI					X	
		16.1.3 Notificación de puntos débiles de la seguridad.	SI					X	
		16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	SI					X	
		16.1.5 Respuesta a los incidentes de seguridad.	SI					X	
		16.1.6 Aprendizaje de los incidentes de	SI					X	

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		seguridad de la información.							
		16.1.7 Recopilación de evidencias	SI					X	
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	17.1 Continuidad de la seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información.	SI	Definir los lineamientos para la identificación, análisis y remediación de las vulnerabilidades en los componentes de la infraestructura tecnológica de la Rama Judicial.	Política para la gestión de vulnerabilidades sobre los componentes de la infraestructura tecnológica			X	
		17.1.2 Implantación de la continuidad de la seguridad de la información.	SI	El respaldo de la información busca reducir los impactos de los riesgos generados por la pérdida de información y es un mecanismo para soportar los planes de contingencia, recuperación ante desastres y atención a incidentes de seguridad de la información adoptados por la Entidad.	Política de respaldo de la información			X	
		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	Se debe procurar por el cumplimiento de las políticas establecidas en cuando a la seguridad y respaldo de la información	Auditorias internas MECI			X	

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
	17.2 Redundancias	17.2.1 Disponibilidad	SI	Componentes de Elementos Transversales del manual 3.1 Gobierno en Línea, actividad 3, el cual dice "Implementar un sistema de Gestión de TI, el cual establece la sostenibilidad y mejoramiento que permita articular el uso de la tecnología con los objetivos misionales de las entidades. Así mismo, se requiere una estrategia de monitoreo, de forma tal que se puedan establecer avances y correctivos que permitan la adopción de buenas prácticas y tendencias tanto locales como globales".	Política de respaldo de la información			X	
18. CUMPLIMIENTO	18.1 Cumplimiento de los requisitos legales y contractuales	18.1.1 Identificación de la legislación aplicable.	SI	Es preciso que la entidad conozca la legislación que la regula, en todos sus campos	Pirámide documental Códigos de procedimiento para todas las especialidades Acuerdos del Consejo Superior de la Judicatura	X			
		18.1.2 Derechos de propiedad intelectual (DPI).	SI	No aplica la propiedad intelectual en la Entidad.	La entidad en su marco normativo, vela por la protección y el cumplimiento de la propiedad intelectual y utilización de elementos software debidamente licenciados	X			
		18.1.3 Protección de los registros de la organización.	SI	La organización debe procurar por que la evidencia de la realización de sus actividades, sea retenida y	Comité de Archivo Tablas de Retención Documental Política de Respaldo de la Información	X			

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
				custodiada en los términos que exige la ley					
		18.1.4 Protección de datos y privacidad de la información personal.	SI	Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013 sobre protección de datos, la Rama Judicial establece la siguiente política de tratamiento de datos personales con el propósito de que todas las personas puedan conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en las bases de datos o archivos a cargo de esta entidad.	Política de tratamiento de datos personales	X			
		18.1.5 Regulación de los controles criptográficos.	SI	Definir la gestión de controles criptográficos para el envío o recepción de información en medios electrónicos protegiendo la confidencialidad, integridad y trazabilidad de la información.	Política de controles criptográficos	X			
	18.2 Revisiones de la seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información.	SI	La Entidad debe revisar de forma autónoma, el nivel de seguridad de la información tiene implementado	Pruebas de Pentesting realizadas Auditorias internas			X	
		18.2.2 Cumplimiento de las políticas y	SI					X	

Lista de Chequeo			Declaración de Aplicabilidad						
Dominios, Objetivos y Controles de ISO-IEC 27002:2013			Aplica	Justificación de la Selección	Declaración de Aplicabilidad	INDICE			
Dominio	Objetivo de Control	Control				Requerimientos Legales	Obligaciones Contractuales	Requerimientos del Negocio / Mejores Practicas	Resultados del Aseguramiento de Riesgos
		normas de seguridad.							
		18.2.3 Comprobación del cumplimiento.	SI	Es pertinente garantizar el cumplimiento de las políticas de seguridad de la información, a través de un tercero	Auditorias externas			X	