UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

HACKING ÉTICO PARA DETERMINAR LOS NIVELES DE SEGURIDAD DE LA JUNTA PARROQUIAL DE RICAURTE.

EGRESADO:

BURGOS VILLEGAS GEAN CARLOS

TUTOR:

ING. JOFFRE LEÓN ACURIO S. MSC.

AÑO 2018

TEMA

HACKING ÉTICO PARA DETERMINAR LOS NIVELES DE SEGURIDAD DE LA JUNTA PARROQUIAL DE RICAURTE

INTRODUCCIÓN

Actualmente se observa que los GAD (Gobiernos Autónomos Descentralizados) o juntas parroquiales rurales, en el Ecuador están avanzan a pasos acelerados y tienen la necesidad de emplear nuevas tecnologías para la automatización de ciertos procesos que en ocasiones son tediosos y se hace muy complicado hacerlo de forma manual, además del tiempo que se toman. Es importante señalar el desarrollo que ha alcanzado la tecnología en la actualidad y que son de mucha ayuda para los mediante el uso de herramientas informáticas.

Uno de los principales problemas que se presentan en la junta parroquial de Ricaurte es la falta de conocimiento sobre la seguridad que hay que tomar en cuenta al momento de adquirir e implementar infraestructura tecnológica ya que estos equipos manejaran información muy relevante.

Cabe recalcar que la junta parroquial de Ricaurte tiene información valiosa almacenada en sus ordenadores, de convenios con instituciones públicas la cual es muy utilizada para sus labores diarias, esta información no consta con las medidas de seguridad requeridas para su protección, lo que la hace vulnerable a ataques cibernéticos internos y externos que pueden llegar a la sustracción o alteración no autorizada de ella.

La metodología de investigación usada en este caso fue la descriptiva, este tema está enmarcado en la sublinea de investigación de redes y seguridad, en la línea de investigación de facultad de administración finanzas e informática F.A.F.I, para realizar el caso de estudio se enmarca en el desarrollo de sistemas de comunicación e información y emprendimiento empresariales y tecnológicos.

DESARROLLO

La junta parroquial o Gobierno Autónomo Descentralizado, es el encargado de la realización de labores sociales con la comunidad y de las principales obras dentro de las áreas rurales de Ricaurte, en convenio con el municipio cantonal y la prefectura y otros ministerios para lograr cumplir sus metas.

En los últimos años el avance de la tecnología ha logrado un fuerte crecimiento en el área informática el uso de internet que es algo primordial y vía principal para que los sistemas informáticos estén interconectados, los cuales disponen de una gran variedad de beneficios para las distintas áreas de la junta parroquial de Ricaurte.

El MINTEL, es el ministerio que en convenio con el Gobierno Autónomo Descentralizado de Ricaurte, complementen los aportes importantes y necesarios que permitan avanzar a Ricaurte como territorio digital y tecnológico, considerando que los que se beneficiaran serán sus habitantes (MINTEL, 2013).

El trabajo coordinado entre la junta parroquial de Ricaurte y el MINTEL, permite avanzar en el uso de las (TIC), que se relacionadas al uso de Hardware y Software, Internet, contenidos, que están para servir a los habitantes de la parroquia Ricaurte (MINTEL, 2013).

Sin embargo, los ordenadores e información que es muy valiosa para la junta parroquial de Ricaurte, no tienen medidas de seguridad necesarias para proteger dicha información.

El objetivo principal de este estudio es lograr determinar los niveles de seguridad en la red y ordenadores que posee el Gobierno Autónomo Descentralizado de Ricaurte desde el punto de vista interno, para poder encontrar los distintos fallos

de seguridad en su infraestructura tecnológica, y de esta manera aplicar un hacking ético para determinar sus niveles de seguridad y clasificarlos de acuerdo al número de vulnerabilidades encontradas.

Algunos de los problemas encontrados en la junta parroquial es el acceso que hay a los puntos de red libres fuera de los departamentos y los riesgos en la seguridad de la red, los ordenadores y la información que conlleva esto.

De acuerdo al libro de Karina Astudillo el Hacking ético (Ethical Hacking), los profesionales en seguridad informática e la información y en la aplicación del mismo es una manera de utilizar los conocimientos en esta rama de la informática, para realizar el análisis en la seguridad respectivo de las redes y la información que transita por ella, todo con fines únicamente éticos. La función o el punto del Ethical Hacking que se realizara en la junta parroquial de Ricaurte, es determinar que intrusos o personal no autorizado tenga acceso a la red y por consiguiente a la información de los computadores de los distintos departamentos, la parte final es velar por la protección de la información (Astudillo, 2013).

Para la realización del hacking ético se tuvo que tomar otros aspectos importantes como.

El proceso de Hacking posee distintas fases para su realización de acuerdo a lo investigación de la temática hay dos maneras de hacerlos, dichas fases se distinguen por su modo de operar

Las fases más usadas por los piratas informáticos.

1.- Reconocimiento 2.- Escaneo 3.- Obtener acceso 4.- Mantener acceso 5.- Borrar huellas (Astudillo, 2013).

Estas fases se las representa como un ciclo al que se lo llama comúnmente círculo.

A continuación (Figura 1) para enfatizar que el pirata informático luego de borrar sus huellas, no obstante, el auditor que ejecuta elservicio de hacking ético presenta un pequeño cambio en la ejecución de las fases de la siguiente forma (Astudillo, 2013):

1.- Reconocimiento 2.- Escaneo 3.- Obtener acceso 4.- Escribir Informe 5.- Reportar hallazgos en el Informe (Rodriguez, 2016).

El auditor que realiza el servicio de hacking ético se detiene en la fase 4 para reportar sus hallazgos en el informe y por consiguiente se hará las recomendaciones de seguridad (Rodriguez, 2016).

Por ende, las faces a utilizar son las del hacking ético.

FASES DEL HACKING ETICO-NOETICO

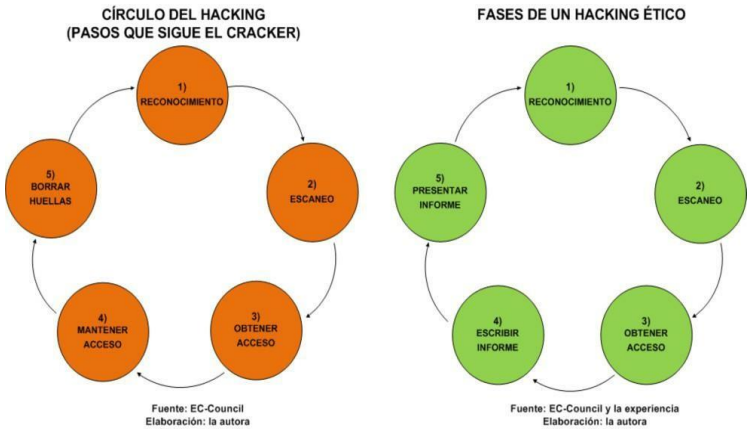

Grafico1 Fuente: (Astudillo, 2013)

Uno de los primeros aspectos que se tomó en cuenta de acuerdo al libro de Karina Astudillo al momento de realizar el servicio de hacking ético es necesario establecer su alcance, para poder elaborar un cronograma de trabajo que se ajuste a la necesidad y en base a él y realizar la propuesta de auditoria al gerente de la empresa donde se realizará la auditoria informática (Rodriguez, 2016).

Y para determinar el alcance se necesita conocer como mínimo tres cosas básicas: el **tipo de hacking** a realizar, **el modo de ataque** del mismo (MARTINEZ N. E., 2012).

Dependiendo de qué manera se harán las pruebas de intrusión, el hacking ético que usaremos es el hacking interno por tratarse de una auditoria interna (MARTINEZ N. E., 2012).

Como su nombre lo sugiere, este tipo de hacking se usó para ejecutaremos las pruebas internas dentro de la junta parroquial de Ricaurte (Astudillo, 2013).

En este tipo de pruebas suelen encontrarse más vulnerabilidades en la seguridad (MARTINEZ N. E., 2012).

Ya que los administradores de redes se preocupan en proteger solo del perímetro de su red, y no toman en cuenta al atacante interno. En esta última parte cometen un gran error, debido a que estudios más recientes nos demuestran que la mayoría de los ataques exitosos provienen del interior de alguna empresa (Rodriguez, 2016).

Según el libro de Karina Astudillo uno de los últimos aspectos a tomar en cuenta es el modo de ataque que vamos a usar, el servicio de hacking ético lo podemos ejecutar en una de las tres modalidades siguientes: hacking de caja negra, hacking de caja gris o hacking de caja blanca (Rodriguez, 2016).

En el ámbito profesional la modalidad escogida afectará los costos y que tiempo duraran las pruebas de intrusión (Astudillo, 2013).

La modalidad escogida fue el ataque White box hacking.

Que se denomina hacking de caja blanca, llamado también hacking transparente. En esta modalidad se aplicaran las pruebas de intrusión de manera interna, se llama de esta forma porque la junta parroquial de Ricaurte nos brindó información completa de las redes y los ordenadores a ser auditados (MARTINEZ N. E., 2012).

Además de brindarnos un punto para conectarnos a su red y posicionar la estación de auditoría, recibiremos información detallada como los listados de equipos con sus nombres, plataforma de los sistemas operativos, direcciones IP de cada ordenador, puesto que esto nos evitara tener que averiguar información por nuestra cuenta, este tipo de hacking suele realizarse en menos tiempo (Astudillo, 2013).

Finalmente, una vez que se obtuvo de la junta parroquial la información necesaria tipo de hacking que usaremos, modo de ataque, se pudo elaborar la propuesta que de auditoria y el alcance del servicio, el tiempo que demorara la ejecución del hacking ético, el informe entregable (opcional) (un informe de hallazgos y recomendaciones).

De acuerdo al libro de Karina Astudillo el reconocimiento es la primera fase en la ejecución del hacking, que consiste en recibir información importante para la auditoria (Astudillo, 2013).

Esto va a depender si existe o no conexión con el objetivo, las técnicas que podemos utilizar para el reconocimiento pueden ser activas o pasivas (Astudillo, 2013).

El tipo de reconocimiento que se uso fue el activo donde hay una interacción directamente con institución auditada que es la junta parroquial de Ricaurte (Astudillo, 2013).

En la actualidad existen muchos aplicativos y Herramientas que nos pueden ayudar a realizar un mapeo para el reconocimiento (Rodriguez, 2016).

Esta vendría hacer la segunda fase del hacking ético donde utilizamos una herramienta de escaneo y explotación de vulnerabilidades como es el sistema operativo Kali Linux que es una distribución basada en Debian GNU/Linux, que está diseñada para la auditoria y seguridad informática, que incluye muchas herramientas de escaneo, y la que utilizaremos es nmap (Rodriguez, 2016).

Esta herramienta de software libre que incluye Kali Linux se usó para realizar un mapeo de toda la red LAN y los ordenadores de la junta parroquial, para detecta las vulnerabilidades en los sistemas de los pc, los puertos abiertos por donde accederíamos cada uno de los ordenadores de la junta parroquial (Rodriguez, 2016).

Consola de nmap

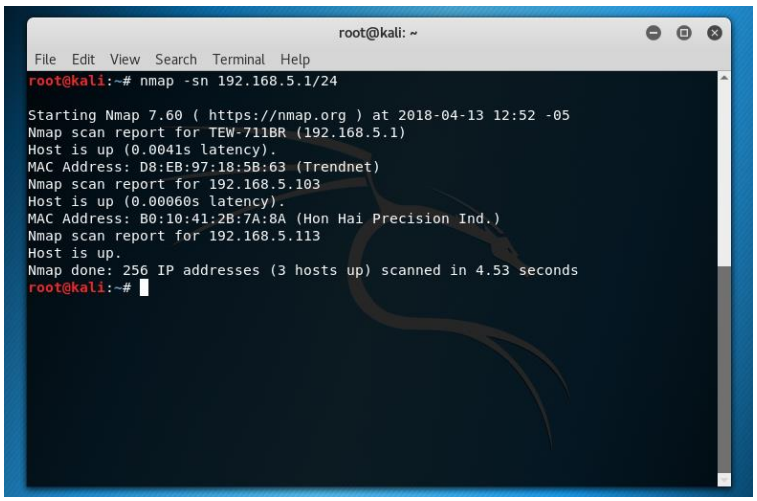

Figura 2 fuente: (elaboración propia)

Se clasifican en los siguientes riesgos: Riesgo bajo, riesgo medio y alto (MARTINEZ N. E., 2012).

Riesgo Alto: El riesgo es considerado alto cuando el ordenador escaneado tiene más de una vulnerabilidad crítica de seguridad, que pueden ser explotadas fácilmente por un atacante y que podrían conllevar a comprometer la seguridad de la información. Los ordenadores con este nivel de riesgo requieren acciones preventivas inmediatas (MARTINEZ N. E., 2012).

Riesgo Medio: el riesgo se considera medio cuando el ordenador escaneado tiene más de una vulnerabilidad severa de seguridad, que son de mayor complejidad y requieren tiempo para poder ser explotadas. Los ordenadores con este nivel de riesgo requieren acciones a corto plazo (Rodriguez, 2016).

Riesgo Bajo: El riesgo se considera bajo cuando el ordenador escaneado tiene una o más debilidades moderadas de seguridad, que podrían brindar información al atacante, la cual podría ser utilizada para realizar ataques posteriores. Los ordenadores con este nivel de riesgos deben ser mitigados adecuadamente, pero tienen un nivel de urgencia bajo (Astudillo, 2013).

En esta fase explotaremos algunas de las vulnerabilidades encontradas en la fase de escaneo para esto usaremos Metasploit y su Framework msfvenom, esta herramienta de código abierto que está incluida en las herramientas de explotación de vulnerabilidades de Kali Linux, con ella intentaremos acceder a cada uno de los 4 ordenadores los departamentos de la junta parroquial de Ricaurte, al no constar con sus antivirus respectivos y aquellos con licencia caducada, mediante el uso de la ingeniería social, que consta en ejecutar el sploit (el punto exe) o código malicioso creado con msfvenom, en cada uno de estos equipos

informáticos desprotegidos por medio del puerto 4444 para tener acceso total al sistema operativo y a la información almacenada en ellos (MARTINEZ N. E., 2012).

Consola de metasploit

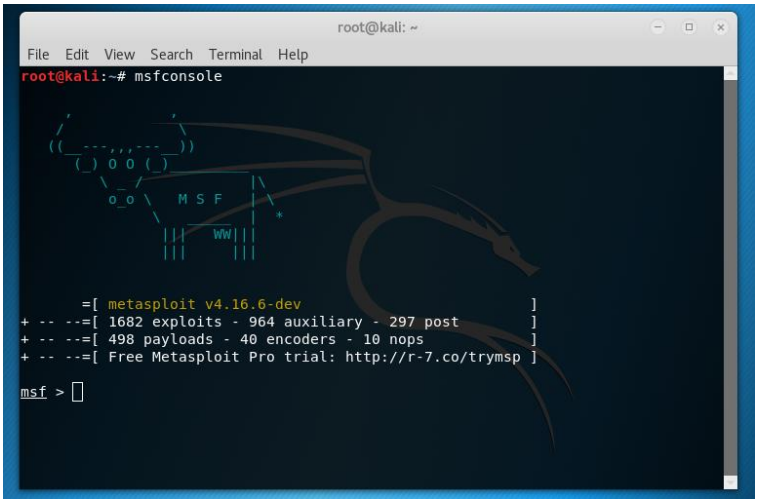

Figura 3 fuente: (elaboración propia)

En esta última fase se procedió a escribir el informe para detallar una a una las vulnerabilidades encontradas en la fase de escaneo y a la explotación de las mismas en la fase de obtener acceso, esta información va dirigida al encargado de sistema de la junta parroquial de Ricaurte para su revisión inmediata, y poder tomar o no medidas de corrección (MARTINEZ N. E., 2012).

En este caso veremos algunas de las medidas de prevención necesarias y el uso de la norma ISO 27001 que nos permite conocer la seguridad en la información gracias a que implanta un Sistema de Gestión de Seguridad de la Información (Peña, isotools, 2015).

También se utilizó la ISO 27002, que tiene los controles necesarios para determina un nivel de seguridad que se tiene que implantar, para lograr minimizar los riesgos y que los mismos se encuentren a niveles considerables (Peña, isotools, 2015).

Estos controles son los indicados que buscan estructurar el marco de seguridad eficiente mediante los roles, tareas, seguridad, como en los ordenadores (pmg-ssi, 2016).

Gestión de activos

Se centra en la protección que tiene que tener la información como activo y en cómo establecer las medidas de seguridad necesarias para su protección de las incidencias de seguridad y en la alteración no deseada de la misma (pmg-ssi, 2016).

Control de acceso

Se centra en que personas o personal está autorizado para acceder a la los equipos con información importante y cuales no deben tener acceso a ella (pmg-ssi, 2016).

Seguridad física y del entorno

La seguridad a nivel físico quiere decir, que la simple labor de no dejar desprotegidas las áreas de acceso a los ordenadores con información importante para personas no autorizadas, impresoras en zonas que sean fácilmente accesibles, (pmg-ssi, 2016).

Seguridad de las operaciones

Esta es la medida de protección y el uso de herramientas antivirus contra el software malicioso, copias de seguridad de la información, control de software en explotación y gestionar las vulnerabilidades (pmg-ssi, 2016).

Seguridad de las comunicaciones

La mayor parte del flujo e intercambio de información y de datos en distintas escalas se realiza mediante las redes sociales, para garantizar la seguridad y poder proteger de forma eficaz los medios de transmisión (pmg-ssi, 2016).

Gestión de incidentes de seguridad de la información

Esta es la parte más importante, los incidentes o quiebres de seguridad y que estar preparados para cuando estos incidentes ocurran, dando una respuesta rápida y eficiente para prevenirlos (pmg-ssi, 2016).

Tabla de vulnerabilidades y riesgos encontrados en los ordenadores de la junta parroquial de Ricaurte.					
Departamento	Equipos	Sistema operativo	Vulnerabilidades encontradas	Nivel de riesgo	Niveles de seguridad
Resección	Ordenador 1	Windows 10 pro de 64 bits	• Actualizaciones de sistema desactivadas. • Software antivirus sin licencia.	alto	bajo
Secretaria	Ordenador 2	Windows 10 pro de 64 bits	• Actualizaciones de sistema desactivadas. • Software antivirus sin licencia.	alto	bajo
Financiero	Ordenador 3	Windows 10 Home de 64 bits	• Actualizaciones de sistema desactivadas. • Software antivirus sin licencia.	alto	bajo

CONCLUSIONES

- En la fase de escaneo realizada con Nmap, se pudo encontrar muchas vulnerabilidades que se presentan en los sistemas Windows de Microsoft, una de esas es la apertura del puerto 4444 en el cual se puede tener acceso no autorizado al sistema operativo de cualquiera de los ordenadores de la junta parroquial de Ricaurte.
- En la tercera fase realizada que fue la de obtener acceso, se pudo evidenciar mediante el uso de metasploit la explotación de una de esas vulnerabilidades que es el puerto 4444, por el cual se pudo tener acceso a tres ordenadores de la junta parroquial entre estos están recepción, departamento de secretaria, departamento financiero.
- Dadas las vulnerabilidades encontradas en la junta parroquial y la explotación de cada una de ellas en los diferentes departamentos, se pudo determinar que los niveles de seguridad en la red LAN y tres de los cuatro ordenadores tienen un nivel de seguridad muy bajo.
- Dados los niveles bajos en la seguridad de la información de la junta parroquial de Ricaurte, y para que en un futuro no puedan ocurrir incidentes en la seguridad de sus ordenadores e información, se plantearon algunas medidas de seguridad preventiva, como el control de acceso de personas no autorizadas a los departamentos y la seguridad física del entorno, seguridad en las operaciones con el uso de herramientas antivirus uno de los recomendados es Eset Nod 32.

Bibliografía

Alonso, C. (26 de Octubre de 2016). *elladodelmal.* Obtenido de elladodelmal: www.elladodelmal.com/2016/10/descarga-el-libro-gratuito-de-seguridad.html

Astudillo, K. (2013). *Hacking Etico 101: Como Hackear Profesionalmente En 21 Dias O Menos.* guayaquil: Createspace Independent.

Benchimol, D. (2011). *Hacking.* Buenos Aires: Fox Andina.

Ecuador, C. d. (19 de Diciembre de 2017). *guiaosc.org*. Obtenido de guiaosc.org: https://guiaosc.org/cuales-son-las-competencias-de-los-gobiernos-autonomos-descentralizados/

Jimenez, J. R. (2015). *Pentesting con Kali 2.0.* Madrid: anonimo.

Marañón, G. Á. (2017). *Seguridad informática para empresas y particulares.* Madrid: Carmelo Sanchez Gonzalez.

MARTINEZ, N. E. (5 de Febrero de 2012). *uagraria.* Obtenido de uagraria: http://www.uagraria.edu.ec/documentos/posgrado/RECOMENDACIONES%20GENERALES%20PARA%20LA%20ELABORACION%20DE%20TESIS%20SIPUAE-2015.pdf

MARTINEZ, N. E. (5 de Febrero de 2012). *uagraria.* Obtenido de uagraria: http://www.uagraria.edu.ec/documentos/posgrado/RECOMENDACIONES%20GENERALES%20PARA%20LA%20ELABORACION%20DE%20TESIS%20SIPUAE-2015.pdf

MINTEL. (4 de Septiembre de 2013). *www.telecomunicaciones.gob.ec.* Obtenido de www.telecomunicaciones.gob.ec: https://www.telecomunicaciones.gob.ec/el-trabajo-coordinado-entre-el-mintel-y-los-gads-permitira-avanzar-hacia-los-territorios-digitales/#

MOTOS, V. (20 de Noviembre de 2015). *hackplayers*. Obtenido de hackplayers: http://www.hackplayers.com/2015/11/llega-la-version-7-de-nmap.html

ParaisoLinux. (29 de Marzo de 2010). *www.paraisolinux.com*. Obtenido de www.paraisolinux.com: https://paraisolinux.com/que-es-y-como-usar-nmap/

Peña, F. (5 de Enero de 2015). *isotools*. Obtenido de www.isotools.org: https://www.isotools.org/2015/01/05/iso-27001-seguridad-informatica-seguridad-informacion/

Peña, F. (5 de Enero de 2015). *isotools*. Obtenido de isotools: https://www.isotools.org/2015/01/05/iso-27001-seguridad-informatica-seguridad-informacion/

pmg-ssi. (14 de Junio de 2016). *pmg-ssi.com*. Obtenido de pmg-ssi.com: http://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/

Quesada, A. E. (2015). *Hacking con Kali Linux.* Lima: Anonimo.

Rmirez, A. T. (2016). *Sertificacion de seguridad ofensiva Nivel 1.* Mexico: Hackingmexico.

Rodriguez, C. F. (3 de Enero de 2016). *slideshare*. Obtenido de slideshare: https://www.slideshare.net/carlos141274/hacking-etico-101-56624376

Telefonica, F. (2016). *Ciberseguridad, la proteccion de la informacion en un mundo digital.* Madrid: Editorial Ariel, S.A.

Encuesta

DIRIGIDA: Al personal de la junta parroquial de Ricaurte.

OBJETIVO: obtener la información necesaria que permita analizar y conocer los diferentes puntos de vista.

Marque con una x la opción que considere correcta.

1.- ¿Qué opina usted acerca de la seguridad de las tic de la junta parroquial de Ricaurte?

Excelente ☐

Bueno ☐

Regular ☐

Malo ☐

Descripción	**Resultados**	
Excelente	0	0%
Bueno	0	0%
Regular	3	75%
Malo	1	25%
Total	4	100%

Análisis de Resultados.

La mayoría del personal administrativo del departamento de sistema, no consideran que la seguridad de las tic es buena.

2.- ¿cree usted que es necesario realizar una auditoria informática interna para medir los niveles de seguridad de las tic en la junta parroquial de Ricaurte?

Si ☐

No ☐

En ocasiones ☐

Descripción	**Resultados**	
Si	4	100%
No	0	0
En ocasiones	0	0
Total	4	100%

Análisis de Resultados.

En su totalidad, el personal administrativo del departamento de sistema, considera que la realización de una auditoria informática.

3.- ¿cree usted que al realizar la auditoria informática se encontraran problemas en la seguridad de las tic del GAD de Ricaurte?

Si ☐

No ☐

En ocasiones ☐

Descripción	Resultados	
Si	4	100%
No	0	0
En ocasiones	0	0
Total	4	100%

Análisis de Resultados.

En su totalidad, el personal administrativo del departamento de sistema, considera que la realizar la auditoria informática se van a encontrar vulnerabilidades.

4.- ¿considera necesario vulnerar la seguridad de la red t los sistemas para poder encontrar futuras soluciones?

Si ☐

No ☐

Descripción	Resultados	
Si	4	100%
No	0	0
En ocasiones	0	0
Total	34	100%

Análisis de Resultados.

En su totalidad, el personal administrativo del departamento de sistema, considera que necesario vulnerar la seguridad para encontrar solución a los problemas.

5.- ¿cree usted que después de realizarse la auditoria informática y encontrar posibles vulnerabilidades los directivos tomaran medidas en el asunto?

Si ☐

No ☐

Descripción	Resultados	
Si	3	75%
No	1	25
En ocasiones	0	0
Total	4	100%

Análisis de Resultados.

La mayoría del personal administrativo del departamento de sistema, consideran que al encontrar posibles vulnerabilidades en la seguridad tomarían cartas en el asunto.

6.- ¿Cómo califica usted la auditoria informática que se realizará en la junta parroquial?

Excelente ☐

Bueno ☐

Regular ☐

Malo ☐

Descripción	Resultados	
Excelente	0	0%
Bueno	3	75%
Regular	1	25%
Malo		0%
Total	4	100%

Análisis de Resultados.

La mayoría del personal administrativo del departamento de sistema, califican de buena la auditoria informática que se va a realizar.

Figura 3: Árbol de problemas (elaboración propia)

Escaneo por cada host con nmap

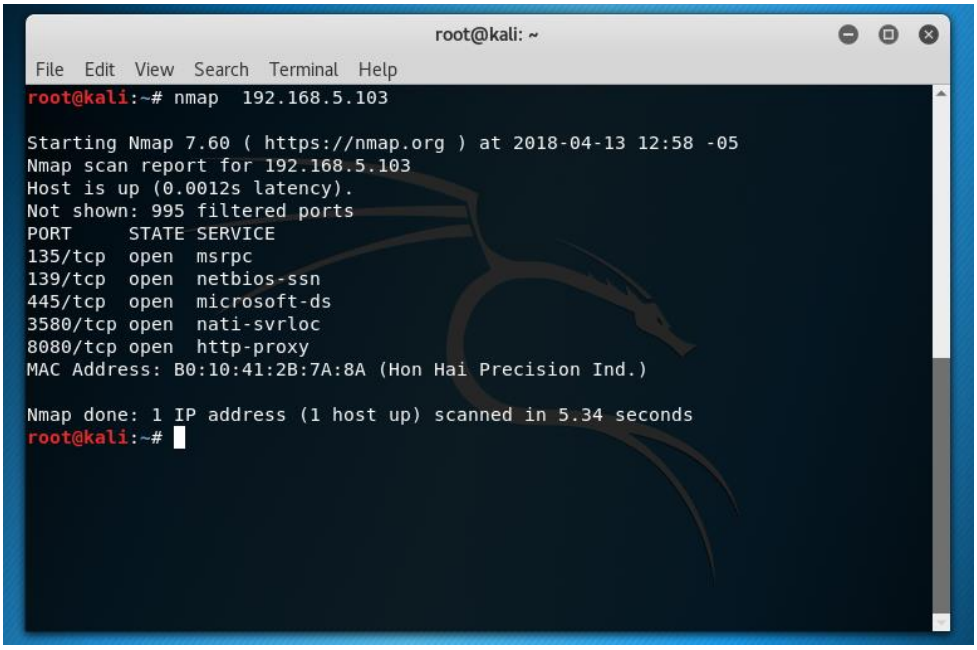

Figura 4 fuente: (elaboración propia)

Consola de msfvenom para crear el punto exe

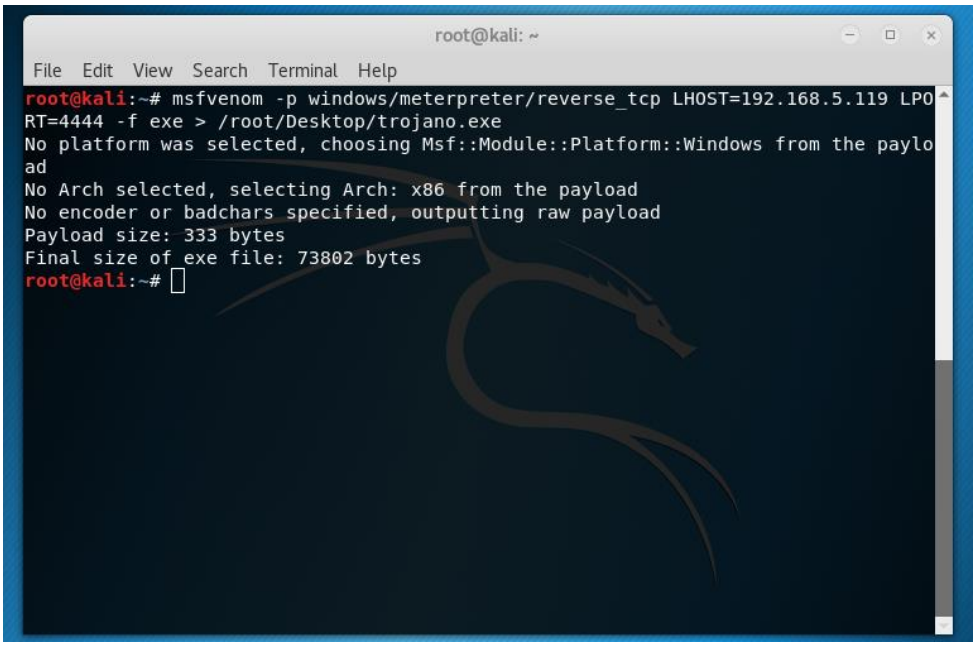

Figura 5 fuente: (elaboración propia)

Metasploit en espera que el punto exe sea ejecutado

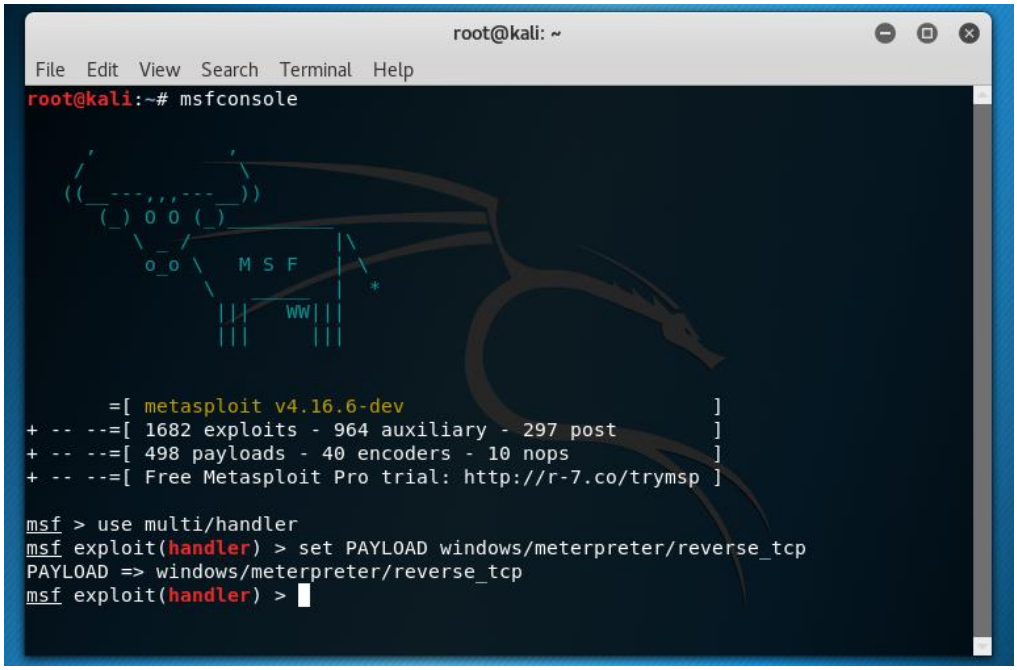

Figura 6 fuente: (elaboración propia)

Ventana de opciones de metasploit

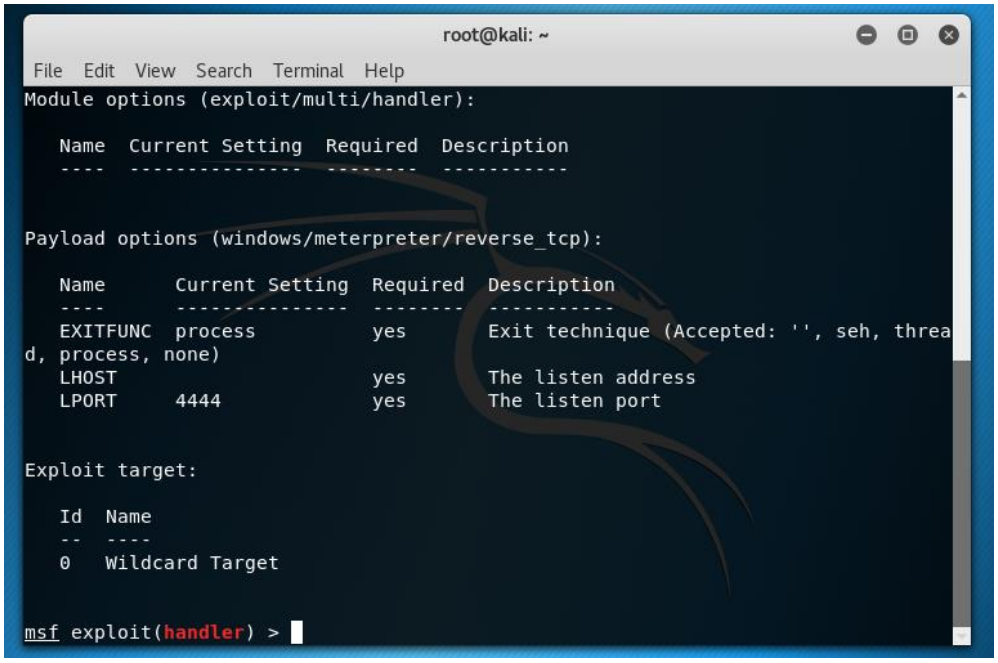

Figura 7 fuente: (elaboración propia)