FORMATO PARA LA PRESENTACIÓN DE PROYECTO DE INVESTIGACIÓN

CONVOCATORIA 2021

1. Nombre del proyecto de investigación

ANÁLISIS DEL COMPORTAMIENTO DE ATACANTES CIBERNÉTICOS MEDIANTE LA IMPLEMENTACIÓN DE UNA RED HONEYNET

2. Tipo de proyecto:

Proyecto de Investigación con componentes de Desarrollo e Innovación (I+D+I).

3. Grupo de investigación

Grupo de Investigación Sistemas y Aplicaciones Tecnológicas (GISAT)

4. Línea de investigación y Campos del Conocimiento

ff. Sistemas de Información

gg. Plataformas Tecnológicas

mm. Educación, ciencia, tecnología e innovación

Especialidad del campo

Campo Amplio	06 información y Comunicación (TIC)
Campo Específico	061 información y Comunicación (TIC)
Campo Detallado	0611 El uso del ordenador 0613 software y desarrollo y análisis de aplicativos

5. Director del Proyecto, integrantes internos y/o externos (coautores), ayudantes y/o semilleros de investigación, todos son participantes en la investigación

Ing. Milton Gabriel Del Hierro Mosquera

6. Fecha de entrega del perfil

20 de abril de 2021

7. Fecha planificada de finalización del proyecto

23 de diciembre 2022

8. Introducción

En los últimos tiempos y años los **ataques informáticos**, realizados por medio de la red se han incrementado de una forma exponencial. Este aumento se debe al incremento de las herramientas utilizadas por medios de los atacantes que casa vez se les hace más fácil invadir o penetrar a una red de datos existente.

Uno de los mayores culpables de que estos ataques sucedan con mas frecuencia son los **desarrolladores** ya que ellos crean sus propias herramientas, aplicaciones y códigos, para crear puertas traseras para penetrar en una **red de datos** a este tipo de desarrolladores se los conoce más comúnmente como hacker, y en palabras técnicas desarrolladores informáticos, debido a sus conocimientos son capaces de conectarse a un ordenador por más seguridades implementadas.

Esto genera que cada **intruso o hacker** tenga sus características muy definidas, creando un perfil de intruso, son muy **vulnerable**s aquellos equipos que contengan información valiosa, dichos ataques se desarrollan por millones a nivel mundial siendo un porcentaje muy pequeño los que se realizan a equipos con información útil o transcendental.

Los ataques que se realizan a diario no van dirigidos o tienen un objetivo determinado, mas bien tiene un objetivo principal que es determinar la víctima más débil en **seguridades informáticas**, donde la puerta de ingreso para la red será el equipo con muchas **vulnerabilidades** y brinde todas las facilidades para lograr el ingreso y se podrá aprovechar este portal para extraer información.

Después de haber desarrollado una pequeña introducción sobre como se realiza el proceso de extracción de información de la red, podemos darnos cuenta de que para poder desarrollar esta actividad debemos tener conocimientos extraordinarios y poder ingresar, pero también indagando un poco en internet ya podemos encontrar en la red miles de herramientas fáciles de realizar un manejo y ser más amigable para este tipo de personas dedicadas a este tipo de actividades ilícitas.

Durante los últimos años, la frecuencia de estos ataques sea dado cada vez más indiscriminada, que conlleva a tomar en cuenta las numerosas vulnerabilidades detectadas en los equipos informáticos y sistemas operativos, transformando o cualquier ordenador en una potencial víctima de penetración informático.

Por tanto, se genera una necesidad o requerimiento de implementar instrumentos que mitiguen las puertas ocultas de ingreso y se plantee una opción con técnica e instrumentos que permitan detectar dichas vulnerabilidades para robustecer nuestros sistemas conectados a la red.

9. El problema

Hoy en día los ataques cibernéticos en la red son más comunes de lo que uno espera, es así que se genera nuevas técnicas de ataques informáticos, a la par también se aumentan herramientas que contrarrestan dicha actividad ilícita.

La Universidad Politécnica Estatal Del Carchi cuenta con un sistema de seguridad informático moderado, la estructura de la red de la Institución cuenta con un software que limita el acceso al contenido, un **firewall** que permite salir al mundo por medio del internet y tener conexión a las redes externas, como toda red de datos es vulnerable a los ataques cibernéticos

Según conversación mantenida con el personal encargado de la parte de redes de la Universidad Politécnica Estatal del Carchi en especial con Javier Torres analista de redes y telecomunicaciones, menciona que en agosto del 2018 se recibió un ataque cibernético, después del análisis realizado se detectó que dicha acción se la realizo desde el continente de Asia con su posterior toma de correcciones bloqueando las direcciones IP de su procedencia. También se indicó que cotidianamente se reciben solicitudes de DOS con una toma de correctivo donde se bloquean los pines para que no puedan tener acceso a la red de la Universidad.

Por lo antes expuesto se propone fortalecer la red de la Institución para identificar la existencia de intrusos que estén tratando de ingresar o si estos han ingresado por medio de ataques a la red, por lo que se plantea implementar un sistema de identificación de arremetidas a través de **honeynet**.

10. Las variables

Variable Independiente:

Implementación de la red honeynet

Variable Dependiente:

Identificación y análisis de atacantes cibernéticos

11. Operacionalización de las variables de la investigación

La implementación de la red honeynet permitirá identificar y analizar a tiempo los atacantes cibernéticos

Tabla 1

Matriz de operacionalización de las variables

Variables	Dimensiones	Indicadores	Ítems
Identificación y análisis de atacantes cibernéticos **(Variable Dependiente)**	**Conocimiento**	Nivel de educación. Nivel de conocimiento técnico. Experiencia Técnica.	Encuesta Ficha técnica Entrevista
	Herramientas Tecnológicas	Número de herramientas utilizadas para el análisis de ataques	Selección de Herramientas
	Técnicas	Técnicas utilizadas para ataques cibernéticos	Ficha técnica
Implementación de la red honeynet **(Variable Dependiente)**	**Normativa**	Apegadas a la ley	Datos informativos ley de seguridad de la información
	Instrucciones	Instructivo	Datos informativos ley de seguridad de la información

Objetivos

Objetivo General

Identificar y analizar el comportamiento de atacantes cibernéticos mediante la implementación de una red honeynet en la Universidad Politécnica Estatal del Carchi

Objetivos específicos

- Diagnosticar las herramientas de detección de intrusos actuales sobre la arquitectura de red utilizada en la Universidad Politécnica Estatal del Carchi.
- Determinar políticas de seguridad que se podrían implementar en la red Universidad Politécnica Estatal del Carchi
- Diseñar un modelo honeynet que permita la recolección de información sobre los ataques informáticos, implementado en la nueva biblioteca institucional.
- Detectar los atacantes cibernéticos de la red de la Universidad Politécnica Estatal del Carchi para el análisis de datos obtenidos en la honeynet
- Elaborar un instructivo para mejorar las políticas de seguridad basadas en la información obtenida por la honeynet.

12. Justificación y alcance territorial

Al realizar la implementación de una red honeynet se relaciona el Objetivo 7 del plan nacional del Desarrollo que menciona: Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía, dentro de una generación de conocimientos participativos que permitirá realizar un detalle de todos los procesos implementados para impedir el ingreso de atacantes a la red de datos, Como expresa Campoverde (2018) “La importancia de estudiar los Honeypot se debe a que en la actualidad existe una gran dependencia de los sistemas informáticos, en los cuales, la información tecnológica adquiere un alto valor para la unidad de negocios en las organizaciones.”

En la Implantación de la red honeynet, se podrá colaborar a la unidad de tecnología de la Universidad Politécnica Estatal del Carchi ampliar las técnicas de protección y bloqueo a los atacantes cibernéticos y poder tomar mejores decisiones, para nuestra red institucional y poder proteger información primordial del sistema académico.

Al final de esta investigación se podrá realizar una capacitación a los integrantes de la unidad de tecnología en especial a los encargados de la red de datos de universidad, sobre temas inherentes y relacionados a la seguridad de la información y técnicas mas utilizadas por los atacantes o hackers, para blindar los ordenadores de los intrusos del exterior.

13. Marco Teórico

Los Honeypots de acuerdo con Torres (2016) es una herramienta de seguridad de la información, que ayuda a conocer los intrusos que ingresan a la red, así mismo en establecer qué tipo de ataque están realizando y las vulnerabilidades de la misma con el propósito de mejorar la seguridad. Por medio de esta herramienta se vigila los movimientos por parte de atacantes o hackers que quieren filtrarse en la información que se encuentra en la red.

Según Espí (2017) Una idea errada acerca de los Honeypots es pretender que son dispositivos diseñados para atraer a los atacantes, sin embargo, esto no es cierto, ya que los Honeypots no se anuncian para que cualquiera los ataque, sino que los mismos atacantes los encuentran por sus propios medios y con relativa facilidad. Un Honeypot debe cumplir una serie de funciones primordiales, entre ellas son:

• Desviar la atención del atacante para salvar al sistema principal y disuadirle de seguir adelante con la intrusión o ganar un tiempo muy valioso que nos permita reaccionar y tomar las medidas oportunas para frenar el ataque.

• Capturar nuevos tipos de malware para su posterior estudio.

• Poder obtener una base de datos con direcciones IP de atacantes y métodos de ataque desconocidos.

• Poder conocer nuevas vulnerabilidades y de esta manera poder aplicar medidas para que no afecten a la seguridad de nuestros sistemas. (pág 13)

Clasificación de los Honeypots

Lara y López (2013) mencionan que los Honeypots se pueden clasificar en: nivel de interacción, método de implantación y función. En el caso de utilizar la clasificación por el nivel de interacción se subdivide en Honeypots de baja interacción y Honeypots de alta interacción. Para el método de implantación se subdivide en Honeypots físicas y Honeypots virtualizadas. Por último, en la clasificación por función se subdivide en Honeypots de producción y Honeypots de investigación

Honeypots de baja interacción.

Son sistemas que aparentan ser sistemas operativos o tener servicios que en realidad no tienen, por ejemplo, pueden levantar el puerto 80 fingiendo tener algún tipo de servicio http y responder intentos de conexión con el mismo tipo de respuestas que

daría un servicio como apache.

Honeypots de alta interacción.

Son sistemas que tienen los servicios totalmente instalados, esto se refiere de instalaciones de sistemas operativos y servicios reales, totalmente operativos y configurados, a diferencia de la Honeypot de baja interacción nada en este tipo de Honeypot es emulado, en lo que a software se refiere, son de mayor interés para los atacantes y al mismo tiempo representan un nivel de riesgo mayor ya que un hacker puede llegar a tomar pleno 15 control de la máquina, reconfigurarla y ejecutar ataques desde ella hacia distintos nodos que están fuera del Honeypot.

En el nivel de interacción los Honeypot requieren de mayor control por los ataques que sufre la red, según Chinchaguano (2016) menciona las principales características de tienen los Honeypot de acuerdo al nivel de interacción con el atacante

Honeypots físicas.

Es aquella cuyos nodos son máquinas físicas, todos los elementos en ella son hardware real y nada en ella se emula. Como es de suponer involucra un costo mayor ya que se debe tener físicamente los equipos que la compongan y al mantenimiento se debe completar el cuidado de los componentes electrónicos que utilice, igualmente se puede incurrir en costos ya que con el tiempo el equipo físico puede dañarse y se requiera la adquisición de repuestos o contratos de mantenimiento que pueden suponer un impacto presupuestal a considerar de acuerdo al tamaño de la organización donde se implemente.

Honeypots virtualizadas.

Son aquellas que consisten en emulaciones de hardware a través de soluciones como VMware, son menos costosas ya que con un solo equipo de cómputo se pueden simular varios, y de esta forma se reduce la inversión en hardware y el mantenimiento que pueda implicar su instalación. Por supuesto esto también dependerá de la solución que se use 16 para llevar a cabo el aprovisionamiento de los sistemas, ya que el licenciamiento puede ser más caro en uno u otro.

Honeypots de producción.

Es aquel destinado a dar un soporte en la seguridad de una red de producción, es decir al ser el Honeypot un sistema que está abierto al ataque puede ser puesto en funcionamiento para mostrar de forma temprana un ataque dentro de una red, hay que tener en cuenta que no es una solución de seguridad, y su despliegue al ser un señuelo no debe implicar mayor trabajo.

Honeypots de investigación.

Son complejos y requieren un mayor nivel de responsabilidad en cuanto a su mantenimiento y observación. Generalmente requieren sistemas operativos reales, con aplicativos y bases de datos reales, (se puede decir que hablamos de Honeypots de alta interacción), a fin de conseguir la mayor cantidad de información que sea posible de un ataque.

14. Marco Metodológico

Metodología de la investigación

.

El enfoque es cualitativo-cuantitativo porque es un proceso que recolecta, analiza y vincula datos cuantitativos y cualitativos en un mismo estudio una serie de investigaciones para responder a un planteamiento. En esta investigación el enfoque cuantitativo se aplica al determinar resultados numéricos utilizando la técnica de la encuesta y la tradición de estudio de caso al explicar, describir y explorar información de la honeynet, que es único y particular en su género.

Modalidad

Para poder desarrollar la presente investigación se toma en cuenta la investigación de campo, documental y bibliográfica.

a) **De campo.**

   La investigación de campo nos va ayudar a recolectar información primordial para determinar información de primera mano e información que nos servirá para la aplicación de nuestro sistema de honeynet.

b) **Documental.**

En la investigación documental se indaga sobre toda la información existente sobre el funcionamiento, implementación en todos los ámbitos que involucre en todos los factores la investigación propuesta de honeynet

c) B**ibliográfica**

La investigación bibliografía, trata sobre investigar científicamente con resultados obtenidos por parte de otros investigadores que nos aportaran de gran magnitud al desarrollo de la investigación planteada en este documento**.**

.

Tipos de Investigación

a) **Descriptiva.** Permite verificar el fenómeno en el lugar y tiempo determinados. Su objetivo consiste en llegar a conocer las situaciones y actitudes predominantes en el proceso de inter-aprendizaje a través de la descripción exacta de las actividades, objetos, procesos y personas.

Población y muestra

Dentro del análisis donde se va a desarrollar la investigación, implementación de una red honeynet se la realizará en el cantón Tulcán y será desarrollada íntegramente en la Universidad Politécnica Estatal del Carchi, conjuntamente con el departamento de Redes

Recolección de la información

Fuentes primarias

La fuente principal de información será el departamento de redes de la universidad Politécnica Estatal del Carchi, dicho departamento tiene la información de primera mano para poder tener un punto de inicio de la investigación.

Fuentes secundarias

Las fuentes secundarias se relacionan a documentos, libros, publicaciones y referencias bibliográficas que nos dará un apoyo a la creación del documento para robustecer la información que nos nutrirá de conocimientos y de metodologías de aplicación para desarrollar paso a paso el tema planteado.

Métodos, técnicas e instrumentos de investigación

Métodos

En esta investigación se utilizaron los métodos generales: deductivo, inductivo, análisis, y síntesis; específicos.

La Arquitectura de una red honeypot, se la debe realizar median un diseño conceptual y otro diseño operacional, de los requerimientos que sean necesarios para la implementación del diseño que se propondrá para la red honeypot.

Los Honeypot es toda una red relacionando entre sí; que controla todos los parámetros de seguridad, para poder diseñar una red Honeynet se define requisitos necesarios para su correcto funcionamiento:

- Control de Datos
- Captura de Datos
- Recolección y Análisis de Datos

El proceso a realizar para la implementación sera

Técnicas

a) Encuestas

b) Entrevistas

Instrumentos

a) Cuestionarios

15. Impactos esperados

Impacto social

- Mediante la Implementación del laboratorio se capacitará a los integrantes del departamento de infraestructura de la Universidad Politécnica Estatal del Carchi para robustecer la seguridad de la red y evitar ataques cibernéticos.

Impacto Tecnológico

- Generar una base de datos para facilitar la identificación de técnicas de ataque cibernético y proteger los datos de los departamentos de tecnología.

- Implementación de un laboratorio con equipamiento para detección de intrusos, para toma de decisiones y proteger los datos de la Universidad Politécnica Estatal del Carchi

Impacto Económico

- Se generará contenido para capacitaciones a personas que trabajen dentro de los departamentos de TIC'S.

Impacto Científico

- Mediante la implementación del laboratorio de honeypot se publicarán los datos relevantes mediante Publicaciones.

16. Productos de investigación

- Laboratorio Honeynet para detección de intrusos.
- Publicar dos artículos científicos.
- Capacitación a los integrantes del departamento de infraestructura de la Universidad Politécnica Estatal del Carchi
- Repositorio de técnicas utilizadas por atacantes cibernéticos

17. Cronograma:

Actividades	Inicio	Fin	2021			2022											
			Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Recolección de Información	01/10 /2021	31/12 /2021															
Diagnosticar las herramientas de detección de intrusos actuales sobre la arquitectura de red utilizada en la Universidad Politécnica Estatal del Carchi	01/01 /2022	31/01 /2022			[1]												
Determinar políticas de seguridad que se podrían implementar en la red Universidad Politécnica Estatal del Carchi	01/02 /2022	28/02 /2022															
Diseñar un modelo honeynet que permita la recolección de información sobre los ataques informáticos, implementado en la nueva biblioteca institucional	01/03 /2022	30/04 /2022															
recolección de información sobre los ataques informáticos	01/05 /2022	30/09 /2022															

[1]

Detectar los atacantes cibernéticos de la red de la Universidad Politécnica Estatal del Carchi para el análisis de datos obtenidos en la honeynet	01/05 /2022	30/09 /2022															
Elaboración de un instructivo para mejorar las políticas de seguridad	01/10 /2022	23/12 /2022															
Elaboración de Artículos Científicos	01/06 /2022	30/06 /2022															
Revisión de Bibliografía	01/12 /2022	23/12 /2022															

19. Recursos y presupuesto

Tabla 2

Presupuesto para el desarrollo de la investigación

ACTIVIDADES *(Describir las actividades)*	RECURSOS *(Detalle de los recursos por actividad)*	N° de Partida	UNIDAD	CANTIDAD	PRECIO UNITARIO ($)	PRESUPUESTO ($)		MES DE EJECUCIÓN
						Presupuesto UPEC	Financiamiento externo	
Implementación Red Honeynet	UPS para Rack de 1UR de 1KVa	840107	Unidad	1	1200	1200		05/01/2022
	Cable Serial DTE para Router	530813	Unidad	5	40	200		05/01/2022
	Cable Serial DCE para Router	530813	Unidad	5	40	200		05/01/2022
	Patch Core de Fibra óptica 7m para SPF	530813	Unidad	12	100	1200		05/01/2022
	Modulos SPF para Fibra Óptica	840104	Unidad	20	300	6000		05/01/2022
	Rack Vertical de 42UR	840107	Unidad	1	1500	1500		05/01/2022
	Enlace de Fibra Óptica	530105	Unidad	1	2000	2000		05/01/2022
	Pelador de Fibra Optica	530811	Unidad	5	25	125		05/01/2022
	Espagueti para Fibra Optica	530813	Unidad	100	1	100		05/01/2022
	Fibra Optica	530813	Unidad	200	5	1000		05/01/2022
	Otdr Fibra óptica	840107	Unidad	2	450	900		05/01/2022

	Kit de Herramientas para Fibra óptica	840106	Unidad	2	700	1400		05/01/2022
	medidor de potencia Fibra optica	840104	Unidad	2	250	500		05/01/2022
	Equipamiento biblioteca	840107	Unidad	6	24255,81	145534,83		05/01/2022
	Impresora	840107	Unidad	1	450	450		05/01/2022
	Rack Abatible con ruedas de 9 UR	840107	Unidad	6	450	2700		05/01/2022
	UPS para Rack de 1UR de 1KVa	840107	Unidad	6	700	4200		05/01/2022
	Patch Core de Fibra 7 pies cat 6	530813	Unidad	20	8	160		05/01/2022
	Computador tipo Gamer core I7	840107	Unidad	7	1500	10500		05/01/2022
	Publicacion	530204	Unidad	2	1000	2000		05/01/2022
						181869,83		

18. Bibliografía

Álvarez, L. & Verdejo, S. (2003). Seguridad en redes IP. 2a. ed. Bellaterra: Catalunya – España.

Gupta, N. (2003). Improving the Effectiveness of Deceptive Honeynets through an Empirical Learning Approach. Australia: Science Publishers.

Joshi, R., Sardana, A. & Enfield, N. (2011). Honeypots: A New Paradigm to Information Security. India: Science Publishers.

Roesch, M., Esler, J. (2006). SNORT - The de facto standard on Intrusion Detection and Prevention. Recuperado el 15 de diciembre de 2016 de https://www.snort.org/#documents

Norma ISO 27001. (2005). Anexo A - Objetivos de control y controles. ISO/IEC 27001.

Provos, N., & Holz, T. (2008). Virtual honeypots: From botnet tracking to Intrusion detection. Boston: Pearson Education.

Siles Peláez, R. (2002). Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados. España: GNU Free Documentation License.

Spitzner, L. (2003). Honeypots: Tracking Hackers. Boston: Addison-Wesley Educational Publishers Inc.

Spitzner, L. (2015). The Honeynet Project. 2015, de Honeynet Project Sitio web: Recuperado el 10 de marzo del 2106 http://www.honeynet.org/project

Carpentier, J. (2016). La Seguridad Informática en la PYME. Barcelona: Editions ENI.

Comer, D. (2016). Redes de Computadores e Internet. Porto Alegre: Bookman.

Dordoigne, J. (2015). Redes Informaticas Nociones Fundamentales. Barcelona: Ediciones ENI.

Griera, J. I. (2017). Estructura de Redes de Computadores. Barcelona: UOC.

Mendes, D. R. (2016). Redes de Computadores. Sau Paolo-Brazil: Noatec.

Pérez, A. (2020). La seguridad de las Redes. Reino Unido : ISTE Internacional

21. Certificaciones

a) Oficio de Aprobación del Decano de la Facultad.
b) Oficio de Compromiso del Director y los miembros.
c) Informe del porcentaje de similitud en el sistema anti plagió del proyecto de investigación.
d) En el caso de que el proyecto cuente con investigadores externos deberá anexarse la copia de sus currículos, así como los convenios marco, convenio específico o carta de intención.

Atentamente;

Firmado electrónicamente por:
MILTON GABRIEL DEL HIERRO MOSQUERA

Milton G. Del Hierro M.
DIRECTOR PROYECTO