

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

ESCUELA DE SISTEMAS

CARRERA DE SISTEMAS

TÍTULO DEL TRABAJO:

SISTEMA DE SEGURIDAD DE SERVIDORES WEB MEDIANTE EL USO DE UNA HERRAMIENTA SEÑUELO APLICADO A LA PLATAFORMA SIANET DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, AÑO 2019.

INFORME FINAL DE INVESTIGACIÓN PRESENTADO COMO REQUISITO PARA OPTAR EL TÍTULO DE INGENIERA EN SISTEMAS COMPUTACIONALES.

AUTOR:

VERÓNICA ESTEFANÍA CHICO REDROBÁN

DIRECTOR:

ING. RODRIGO DEL POZO DURANGO

PARES ACADÉMICOS:

ING. DARWIN CARRIÓN **LIC. EDGAR RIVADENEIRA**

GUARANDA, AGOSTO 2019

DERECHOS DE AUTOR

Yo, Verónica Estefanía Chico Redrobán en calidad de autora del trabajo de investigación: "**SISTEMA DE SEGURIDAD DE SERVIDORES WEB MEDIANTE EL USO DE UNA HERRAMIENTA SEÑUELO APLICADO A LA PLATAFORMA SIANET DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, AÑO 2019**", autorizo a la Universidad Estatal de Bolívar a hacer uso de todos los contenidos que me pertenecen o parte de los que contiene esta obra, con fines estrictamente académicos o de investigación.

Los derechos de como autora por derecho me corresponden, con excepción de la presente autorización, seguirán vigentes a mi favor, de conformidad con lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la ley de la Propiedad Intelectual y su Reglamento.

Asimismo, autorizamos a la Universidad Estatal de Bolívar para que realice la digitalización y publicación de este trabajo de investigación en el repertorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma:

Verónica Estefanía Chico Redrobán

C.I. 1804637567

20190201002P01298 DECLARACION JURAMENTADA

OTORGA VERÓNICA ESTEFANÍA CHICO REDROBAN

CUANTIA INDETERMINADA

DI 2 COPIAS

En la ciudad de Guaranda, provincia Bolívar, República del Ecuador, hoy día jueves doce de septiembre de dos mil diecinueve, ante mi DOCTOR PABLO GONZALO AVILA PURCACHI, NOTARIO SUPLENTE SEGUNDO DE ESTE CANTÓN, comparece la señorita Veronica Estefanía Chico Redrohán, por sus propios derechos. La compareciente es de nacionalidad ecuatoriana, mayor de edad, de estado civil soltera, domiciliada en barrio Huachu San Francisco, parroquia Huachu Grande, cantón Ambato, provincia Tungurahua, y de transito por este lugar, con celular número. cero nueve nueve cuatro nueve cero nueve tres tres nueve, correo electrónico. vchicoredroban@gmail.com, a quien de conocerla doy fe en virtud de haberme exhibido su cédula de ciudadanía en base a la que procedo a obtener su certificado electrónico de datos de identidad ciudadana, del Registro Civil, mismo que agrego a esta escritura como documento habilitante; bien instruida por mi el Notario en el objeto y resultado de esta escritura de Declaración Juramentada que a celebrarla proceden, libre y voluntariamente - En efecto juramentado que fue en legal forma previa las advertencias de la gravedad del juramento, de las penas de perjurio y de la obligación que tienen de decir la verdad con claridad y exactitud, declaran lo siguiente. "Que previo a la obtención del Titulo de Ingeniera en Sistemas Computacionales de la Facultad de Ciencias Administrativas Gestión Empresarial e Informática, otorgado por la Universidad Estatal de Bolívar, manifestó que el criterio e ideas emitidas en el presente Proyecto de Investigación **"SISTEMA DE SEGURIDAD DE SERVIDORES WEB MEDIANTE EL USO DE UNA HERRAMIENTA SEÑUELO APLICADO A LA PLATAFORMA SIANET DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, AÑO 2019"**, es de mi exclusiva responsabilidad en calidad de autora, es todo cuanto tengo que decir en honor a la verdad". Hasta aqui la declaración juramentada que junto con los documentos anexos y habilitantes que se incorpora queda elevada a escritura pública con todo el valor legal, y que a la compareciente aceptan en todas y cada una de sus partes, para la celebración de la presente escritura se observaron los preceptos y requisitos previstos en la Ley Notarial, y, leida que le fue a la compareciente por mi el Notario, se ratifica y firma conmigo en unidad de acto quedando incorporada en el Protocolo de esta Notaria, de todo cuanto DOY FE.

Srta. Verónica Estefanía Chico Redrobán
C. C. 1804637567

DR. PABLO GONZALO AVILA PURCACHI
NOTARIO SUPLENTE SEGUNDO DEL CANTÓN GUARANDA

Se otorgó ante mi, en fe de ello confiero esta **SEGUNDA COPIA CERTIFICADA**, sellada, signada y firmada en el mismo lugar y fecha de su celebración, en dos fojas. DOY FE.

DR. PABLO GONZALO AVILA PURCACHI
NOTARIO SUPLENTE SEGUNDO DEL CANTÓN GUARANDA

NOTARÍA SEGUNDA · DE PABLO AVILA · SUPLENTE · Guaranda - Ecuador

APROBACIÓN DEL TUTOR DE TRABAJO DE TITULACIÓN

Yo, Rodrigo Humberto del Pozo Durango en calidad de tutor de trabajo de titulación: "SISTEMA DE SEGURIDAD DE SERVIDORES WEB MEDIANTE EL USO DE UNA HERRAMIENTA SEÑUELO APLICADO A LA PLATAFORMA SIANET, AÑO 2019", elaborado por la estudiante Verónica Estefanía Chico Redrobán, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas, Gestión Empresarial e Informática de la Universidad Estatal de Bolívar, considero que el mismo reúne los requisitos y méritos necesarios en el campo metodológico y en el campo epistemológico, para ser sometido a la evaluación por parte del jurado examinador que se designe, por lo que lo APRUEBO, a fin de que el trabajo investigativo sea habilitado para continuar con el proceso de titulación determinado por la Universidad Estatal de Bolívar

En la ciudad de Guaranda a los 07 días del mes de agosto del año 2019



Ing. Rodrigo del Pozo Durango

C.I. 0200856557

LIC. EDGAR RIVADENEIRA RAMOS EN CALIDAD DE PAR ACADÉMICO DEL PROYECTO DE INVESTIGACIÓN, A PETICIÓN DE LA PARTE INTERESADA

CERTIFICO·

Que la señorita **VERÓNICA ESTEFANÍA CHICO REDROBÁN** estudiante de la Facultad de Ciencias Administrativas, Gestión Empresarial e Informática, carrera de **SISTEMAS** dentro de la modalidad de titulación (Proyecto de investigación), ha cumplido con el ingreso de sugerencias y recomendaciones emitidas por el suscrito a su proyecto denominado **"SISTEMA DE SEGURIDAD DE SERVIDORES WEB MEDIANTE EL USO DE UNA HERRAMIENTA SEÑUELO APLICADO A LA PLATAFORMA SIANET DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, AÑO 2019",** en tal virtud, faculto a la interesada, seguir el trámite legal pertinente.

Es todo cuanto puedo certificar,

Guaranda a los 07 días del mes de Agosto del 2019

Atentamente

Lic. Edgar Rivadeneira
Cd. N° 0201176062

ING DARWIN CARRIÓN BUENAÑO EN CALIDAD DE PAR ACADÉMICO DEL PROYECTO DE INVESTIGACIÓN, A PETICIÓN DE LA PARTE INTERESADA

CERTIFICO

Que la señorita **VERÓNICA ESTEFANÍA CHICO REDROBÁN** estudiante de la Facultad de Ciencias Administrativas, Gestión Empresarial e Informática, carrera de **SISTEMAS** dentro de la modalidad de titulación (Proyecto de investigación), ha cumplido con el ingreso de sugerencias y recomendaciones emitidas por el suscrito a su proyecto denominado **"SISTEMA DE SEGURIDAD DE SERVIDORES WEB MEDIANTE EL USO DE UNA HERRAMIENTA SEÑUELO APLICADO A LA PLATAFORMA SIANET DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, AÑO 2019",** en tal virtud, faculto a la interesada, seguir el trámite legal pertinente.

Es todo cuanto puedo certificar,

Guaranda a los 07 días del mes de Agosto del 2019

Atentamente



Ing. Darwin Carrión Buenaño
Cd. N° 0604090571

DEDICATORIA

El presente proyecto se lo dedico a Dios porque sin él nada de esto sería posible, me ayudó a iniciar esta travesía y asimismo terminarla.

A mis amados padres Hugo Chico Pérez y Teresita Redrobán Flores quienes han sido siempre mi ejemplo de lucha incansable, por su apoyo constante, su confianza inquebrantable día a día y por ser mi fuerza en cualquier momento de derrota o alegría, económica y moralmente.

A mis hermanas Delia y Viviana quienes han sido parte esencial de mi vida.

Verónica Chico Redrobán

RECONOCIMIENTOS

A Dios por hacer cada día una aventura nueva de dichas y desdichas para de cada una obtener lo más importante, sabiduría y madurez.

A mis padres porque de no haber sido su por amor tan grande, su trabajo diario, su dureza a pesar de la tristeza por la distancia, sus esfuerzos económicos; este logro no hubiese sido posible y lo que un día parecía lejano llegó, lo logré, porque ellos lo hicieron posible.

Verónica Chico Redrobán

ÍNDICE GENERAL

DERECHOS DE AUTOR .....**¡Error! Marcador no definido.**
DEDICATORIA VI
RECONOCIMIENTOS VII
RESÚMEN XIV
INTRODUCCIÓN 1
PLANTEAMIENTO DEL PROBLEMA 3
OBJETIVOS 3
Objetivo General.....3
Objetivos Específicos 3
PREGUNTAS DIRECTRICES 3
MARCO GEO REFERENCIAL 6
MARCO LEGAL.....7
Ley de comercio electrónico, firmas electrónicas y mensajes de datos 7
Utilización de software libre en la administración pública 10
MARCO CONCEPTUAL 12
Servidor Web.....12
Ataques a servidores.....12
Seguridad en Servidores Web.....14
Firewall.....15
Redes 15
Sistemas señuelo o Honeypots 15
Honeypot 15
Finalidad de los Honeypots 16
Clasificación de Honeypots.....16
Según su implementación:.....16
Según su interacción:.....17
Honeynet.....18
DISEÑO METODOLÓGICO.....19
Método De Investigación.....19
Método Cualitativo.....19
TIPOS DE INVESTIGACIÓN.....19
Descriptiva.....19
Bibliográfica.....19

De campo 20
TÉCNICAS E INSTRUMENTOS PARA LA OBTENCIÓN DE DATOS 20
Entrevista 20
Observación Directa 20
Instrumentos 20
Universo y muestra 21
Procesamiento de Datos 21
ANÁLISIS DE RESULTADOS 22
RESULTADOS 27
DISCUSIÓN 28
Análisis de riesgos informáticos 28
Identificación de riesgos 29
Matriz de análisis de riesgos 31
CONCLUSIONES 32
RECOMENDACIONES 33
PROPUESTA DE SOLUCION DEL PROBLEMA 34
Plan de contingencia propuesto a partir de los resultados del análisis de riegos 34
Antecedentes 34
Justificación 34
Objetivos 35
Objetivo General 35
Objetivos Específicos 35
Factibilidad 35
Ubicación 36
Recursos 36
Implementación de una Honeynet 36
Instalación de Centos 38
Configuración bajo consola/terminal de Centos como servidor web 44
Instalación de NIDS Snort en Centos 46
ANEXOS 74
Anexo 1. Entrevista 74
Anexo 2. Ficha de observación 77
Anexo 3. Certificado Urkund 78
Anexo 4. Informe Solinfra 79

LISTA DE FIGURAS

Figura 1 Ejemplo de Honeynet 36
Figura 2 Configuraciones de distribución de memoria 38
Figura 3 Instalación gráfica de Centos 39
Figura 4 Idioma de Sistema 39
Figura 5 Destino de instalación 40
Figura 6 Disco destino de instalación 40
Figura 7 Configuración de red 41
Figura 8 Conexión de red 41
Figura 9 Selección de software de instalación 42
Figura 10 Selección de software de instalación más sus complementos 42
Figura 11 Ajustes de usuario 43
Figura 12 Interfaz de Centos 7 43
Figura 13 Ingreso root e instalación de Apache 44
Figura 14 Aprobación de instalación 44
Figura 15 Instalación de php 45
Figura 16 Instalación de Mysql server 45
Figura 17 Levantamiento de servicio 45
Figura 18 Verificación funcionamiento mysql 45
Figura 19 Enlace php y mysql 45
Figura 20 Apache y Php corriendo 46
Figura 21 Instalando librerías 47
Figura 22 Instalando librerías externas 47
Figura 23 Creando carpeta temporal 47
Figura 24 Descargando DAQ 48

Figura 25 Descomprimiendo DAQ....48
Figura 26 Instalando DAQ....48
Figura 27 ingresamos a la carpeta de descarga temporal....48
Figura 28 Descargando snort....49
Figura 29 Extrayendo e instalando snort....49
Figura 30 Página oficial de Snort....49
Figura 31 Registro de usuario snort....50
Figura 32 Reglas disponibles snort....50
Figura 33 Actualizando bibliotecas....51
Figura 34 Configuración usuarios y carpetas....51
Figura 35 Creación de directorios contenedores....51
Figura 36 Estableciendo permisos....51
Figura 37 Creando archivos para listas....52
Figura 38 Oinkcode personal....52
Figura 39 Comando de descarga....53
Figura 40 Copiar reglas....53
Figura 41 Editar archivo snort.conf....53
Figura 42 Editar archivo snort.conf....53
Figura 43 Registro de salida....54
Figura 44 Validando instalación....54
Figura 45 Editando rules....55
Figura 46 Accediendo a mysql....56
Figura 47 Creando base de datos....56
Figura 48 Snort Report....57
Figura 49 Descarga snort report....57

Figura 50 Configuración snort report 57
Figura 51 Configuración contraseña snort 58
Figura 52 Configuración contraseña snort 58
Figura 53 Instalando barnyard 59
Figura 54 Ossec página principal 59
Figura 55 Instalando paquetes necesarios 60
Figura 56 Agregando repositorios 60
Figura 57 Agregando puertos 60
Figura 58 Instalando ossec server 61

LISTA DE TABLAS

Tabla 1 Especificaciones técnicas pc anfitrión 37

Tabla 2 Especificaciones técnicas de las máquinas virtuales 38

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

CARRERA DE SISTEMAS

“Sistema de Seguridad de Servidores Web mediante el uso de una herramienta señuelo aplicado a la plataforma Sianet de la Universidad Estatal de Bolívar, año 2019.”

AUTOR:

Chico Redrobán Verónica Estefanía

DIRECTOR:

Ing. Rodrigo del Pozo Durango

2019, abril

RESÚMEN

Mediante el presente trabajo de investigación se muestra el potencial funcional de un Sistema de Seguridad de Servidores Web, mediante el uso de una herramienta señuelo aplicado a la plataforma SI@NET de la Universidad Estatal de Bolívar a través de un prototipo. Para esto se utilizan las siguientes herramientas de investigación: entrevista y observación, con los cuales se hizo la recolección de datos para mediante estos lograr conocer la situación actual de la estructura de la red y la seguridad aplicada a los servidores de la Universidad Estatal de Bolívar. Se propone un prototipo estructural adaptable para el correcto funcionamiento de la herramienta señuelo Honeynet, la cual fue selecciona mediante una evaluación de gratuidad para abaratar costos, esto quiere decir que para su construcción y configuración se utiliza la virtualización y el uso de software libre.

Con las preguntas directrices se logra conocer el alcance de la investigación dando solución a la problemática identificada utilizando el prototipo de sistema de seguridad de servidores web.

PALABRAS CLAVE

Seguridad informática, servidores web, herramienta señuelo

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTY OF ADMINISTRATIVE SCIENCES, BUSINESS AND COMPUTER MANAGEMENT

CARRERA DE SISTEMAS

" Security System of Web Servers through the use of a decoy tool applied to the Sianet platform of the State University of Bolívar, 2019"

AUTHOR:

Chico Redrobán Verónica Estefanía

DIRECTOR:

Ing. Rodrigo del Pozo Durango

2019, April

SUMMARY

Through the present research work, the functional potential of a Web Server Security System is shown, through the use of a decoy tool applied to the SI@NET platform of the State University of Bolívar through a prototype. For this, the following research tools are used: interview and observation, with which the data collection was done through these to get to know the current situation of the structure of the network and the security applied to the servers of the State University of Bolívar. An adaptable structural prototype is proposed for the correct functioning of the Honeynet decoy tool, which was selected through a free evaluation to reduce costs, this means that virtualization and the use of free software are used for its construction and configuration.

With the guidelines questions, it is possible to know the scope of the investigation by solving the identified problem using the prototype web server security system.

KEYWORDS

Computer security, web servers, decoy tool

INTRODUCCIÓN

Desde el principio de los tiempos la información, en distintas formas, ha sido parte de la raza humana, tratando de representar mediante ella hábitos, costumbres, sentimientos y conocimientos; se guardaban con el cuidado correspondiente puesto que eran talladas en objetos muy valiosos y por esta razón yacían en lugares con acceso privilegiado.

Actualmente la información es el objeto de mayor importancia tanto personal como para las instituciones de cualquier índole y la informática como las redes de comunicación, a través de su progreso han llegado a tener un papel vital dentro de esto transformando la información en bits y bytes que ocupan un lugar en otra dimensión, no dejando de tener la misma importancia que cuando se la guardaba en objetos reales, en muchos casos más aun debido a su delicadeza. Es por esto que la seguridad informática es importante dado que se trata de la protección de nuestros datos e información personal si tan solo hablamos de un ser humano común más aún si hablamos de gobiernos e instituciones.

A medida que las formas de comunicación, mediante la informática y las redes progresan, las maneras de tener acceso de forma violenta también lo hacen y es por esto que se ha reconocido a James P. Anderson como uno de los pioneros dentro del tema, quien crea uno de los primeros textos investigativos relacionados al tema "Computer Security Threat Monitoring and Surveillance" (Anderson Co., 1980) por pedido de un ente gubernamental, en donde ya estos términos se vuelven comunes pero que por esas épocas sonaban como fantasía, encontrando en este texto las primeras definiciones que hoy por hoy son parte de nuestro día a día.

Amenaza: la posibilidad de un intento deliberado y no autorizado de acceso y manipulación de la información, transformar un sistema en no confiable y obsoleto.

Riesgo: Exponer información de manera impredecible, integridad violentada de operaciones por fallas de hardware, diseño incompleto de software operacional.

Vulnerabilidad: conocimiento en cuanto a fallas de software o hardware accidental

confirmadas o bajo estudio que permite la penetración a los mismos.

Ataque: Ejecución maliciosa de una amenaza.

Penetración: Acceso malicioso con éxito hacia el objeto de ataque, muchas veces o dependiendo de la complejidad de los conocimientos utilizados, puede ser indetectable.

Dentro de las instituciones educativas tanto públicas como privadas son de suma importancia proteger la información que ingresa y se genera dentro de las mismas, para así mantener la transparencia de los procesos, todo esto mediante el debido cuidado de sus servidores, redes internas, plataformas web a través de políticas de seguridad, ACL (Listas de Control de Acceso) o métodos como IDS, herramientas señuelo para la alerta de los intrusos y el manejo correcto de la misma información.

La Universidad Estatal de Bolívar posee múltiples equipos informáticos como Servidores, Modem, Switches, Routers, Firewall, Sistema de Video Vigilancia, entre otros, conjuntamente con diversas plataformas web como el Sistema Académico Integrado en Red (Si@Net), E-mail docente y estudiantil, Entorno Virtual de Aprendizaje, Biblioteca Digital que prestan varios servicios a la comunidad universitaria, a través de una red local con conexión a Internet por lo que la información está expuesta a amenazas logrando ser modificada por personas internas y/o externas de la institución por no tener un sistema de seguridad para evitar intrusiones, por ende el Sistema Integrado Académico en Red (SI@NET) que contiene módulos de matriculación estudiantil, prácticas pre-profesionales, portafolio docente, control de asistencia estudiantil y el distributivo académico es vulnerado por los intrusos en diferentes ocasiones.

PLANTEAMIENTO DEL PROBLEMA

La red de comunicación de datos de la Universidad Estatal de Bolívar cuenta con una infraestructura vulnerable a delitos informáticos, el software es expuesto a varios riesgos y amenazas, por la inexistencia de políticas de seguridad de la información e informática para la prevención de daños, no existen listas de control de acceso (ACL), no cuenta con un sistema de detección de intrusos (IDS), y una configuración limitada del firewall, el mismo que permite la conexión directa desde la red de datos interna hacia la red externa logrando que un intruso pueda tener acceso fácil a la plataforma desde cualquier sitio y lugar pudiendo alterar los datos de los estudiantes, docentes y personal administrativo presentando diferentes falencias sin poder evitar un ataque cibernético.

OBJETIVOS

Objetivo General

Crear un prototipo de sistema de seguridad de servidores web mediante una herramienta señuelo que mitigue las amenazas y riesgos que colocan en peligro la integridad de la información del Sistema Académico Integrado en Red (SI@NET).

Objetivos Específicos

- Analizar la situación actual de la seguridad de la información del servidor web de la plataforma SI@NET.
- Diseñar la arquitectura adaptable del sistema de seguridad para servidores web
- Mostrar un prototipo de sistema de seguridad para servidores web

PREGUNTAS DIRECTRICES

¿Cómo analizar la situación actual de la seguridad de la información del servidor web de la plataforma SI@NET?

¿Cómo diseñar la arquitectura adaptable del sistema de seguridad?

¿Cuándo mostrar un prototipo del sistema de seguridad para servidores web?

JUSTIFICACIÓN

En la actualidad la información es uno de los activos más importantes de las instituciones, empresas u organizaciones tanto públicas como privadas siendo necesario el uso de la seguridad informática para la protección de datos.

En el Departamento de Informática de la Universidad Estatal de Bolívar, surge la necesidad de implementar un sistema de seguridad para servidores web mediante el uso de una herramienta señuelo, misma que trata de configurar un servidor virtual o real para exponerlo de manera controlada, con el objetivo de obtener evidencias de ataques reales y así poder realizar bitácoras. A la vez sirve de aprendizaje para contribuir y reducir las inseguridades informáticas existentes en la plataforma SIANET, en el mismo que se ha identificado varias falencias a nivel de programación y configuraciones de servicios para la protección de datos, teniendo un control crítico.

Durante los últimos años han surgido diversos proyectos de señuelos (miel para hackers), sistemas hardware o herramientas software que simulan ser equipos vulnerables para poder exponerlos sin ningún riesgo y permitir el análisis de todos los ataques efectuados sobre ellos (Gfos seguridad, 2015) permitiendo luego de un análisis:

- Deshabilitar usuarios no requeridos.
- Establecer contraseña robusta a la única cuenta activa (Administrador).
- Deshabilitado de puertos y servicios no requeridos.
- Instalación de las últimas actualizaciones disponibles para el sistema operativo.
- Habilitado de bitácoras del sistema
- Protección perimetral por medio de un firewall

Con la implementación de una de estas herramientas se busca la detección de intrusos, lo cual permite realizar una recolección y creación de un historial de información de las actividades

que ejecutan los atacantes para conocer los principales métodos de ataques cibernéticos y a través de ellos implementar nuevas formas de salvaguardar la información, contrarrestando así las amenazas de alteración o destrucción de datos de los estudiantes, docentes y personal administrativo dentro de la plataforma SIANET, construyendo de esta manera una especie de barrera para los atacantes.

Por los diversos riesgos, amenazas y vulnerabilidades que tiene la plataforma es preciso que la institución implemente las políticas de seguridad informática con los procedimientos establecidos por las normas y estándares existentes para asegurar y salvaguardar los datos del sistema informático. (Software ISO Riesgos y Seguridad, 2018)

MARCO REFERENCIAL

El presente proyecto de grado se realiza en la Universidad Estatal de Bolívar que está ubicada en el cantón Guaranda, provincia Bolívar, en la Av. Ernesto Che Guevara S/N y Gabriel Secaira. Su nombre es dado en honor al Libertador Simón Bolívar y a la provincia en donde nace y se ubica. Se encuentra dividida en facultades, como también en departamentos, específicamente el Departamento de Informática.

MARCO GEO REFERENCIAL

País: Ecuador

Provincia: Bolívar

Cantón: Guaranda

Parroquia: Guanujo

Dirección: Av. Ernesto Ché Guevara S/N y Gabriel Secaira

Ubicación Geográfica:

Longitud: -79º 0’ 28.5’’

Latitud: -1º 33’ 21.20’’ Sistema de referencia: WGS84 Zona 17 Sur



Fuente: https://www.openstreetmap.org/search?query=Universidad%20Estatal%20de%20bolivar%20#map=18/-1.57111/-79.00650

MARCO LEGAL

Ley de comercio electrónico, firmas electrónicas y mensajes de datos

TITULO V

De las infracciones informáticas

CAPITULO I

DE LAS INFRACCIONES INFORMÁTICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

Art.- El que empleando cualquier medio electrónico, informático o a fin, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a una o multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art.- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

Art.- 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad detales, o que les hubieren sido en comendados si razón de su cargo.

Art. 60.- A continuación del artículo353, agréguese el siguiente artículo enumerado:

Art.- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.-Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

Art. 61.- A continuación delartículo415 del Código Penal, inclúyanse los siguientes artículos innumerados:

Art.-Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimido con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

Art. 62.- A continuación del artículo553 del Código Penal, añádanselos

Siguientes artículos innumerados:

Art.- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art.- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento o descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

Art.64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.". (: Ley de Comercio Electrónico)

Utilización de software libre en la administración pública

Decreto ejecutivo 1014

En ejercicio de la atribución que le confiere el numeral 9 del artículo 171 de la Constitución Política de la República

Decreta:

Art. 4.- Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de software libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno. Para efectos de este decreto se comprende como seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa de patrimonio nacional.

Para efectos de este decreto se entiende por un punto de no retorno, cuando el sistema o proyecto informático se encuentre en cualquiera de estas condiciones:

a) Sistema en producción funcionando satisfactoriamente y que un análisis de costo beneficio muestre que no es razonable ni conveniente una migración a software libre; y,

b) Proyecto en estado de desarrollo y que un análisis de costo - beneficio muestre que no es conveniente modificar el proyecto y utilizar software libre. Periódicamente se evaluarán los sistemas informáticos que utilizan software propietario con la finalidad de migrarlos a software libre.

Art. 5.- Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:

a) Nacionales que permitan autonomía y soberanía tecnológica;

b) Regionales con componente nacional;

c) Regionales con proveedores nacionales;

d) Internacionales con componente nacional;

e) Internacionales con proveedores nacionales;

Art. 6.- La Subsecretaría de Tecnologías de la Información como órgano regulador y ejecutor de las políticas y proyectos informáticos en las entidades del Gobierno Central deberá realizar el control y seguimiento de este decreto. Para todas las evaluaciones constantes en este decreto la Subsecretaría de Tecnologías de la Información establecerá los parámetros y metodologías obligatorias. (Gobierno de la República del Ecuador, 2011)

MARCO CONCEPTUAL

Servidor Web

Según (TECHTARGET, 2019) un servidor web es un aplicativo que utiliza HTTP, el protocolo de transferencia de hipertexto para soportar los archivos que forman páginas Web y muestran a los usuarios, en respuesta a sus solicitudes, reenviados por los clientes HTTP de sus computadoras. Comúnmente tiene junto a el una amplia gama de programas con relación a internet e intranet para servir correo electrónico, descargar solicitudes de archivos (FTP), crear y publicar páginas Web. Para elegir un servidor web se deben tomar cuenta varios ítems, como: que tan bien se acopla al sistema operativo. Comunicación con otros servidores, tiempo de respuesta, dificultad de manejo, características de seguridad, herramientas y motores de búsqueda además del impacto del montaje del servicio del mismo.

Un servidor web debe mantener las actualizaciones necesarias y a más de eso, al poseer un tiempo de vida útil, tener una secuencia de renovación para obtener un servicio seguro y de calidad. La Universidad Estatal de Bolívar posee servidores, cada uno tiene una edad diferente de uso, es decir que cada uno fue adquirido según la necesidad de alojamiento de un servicio web, correo electrónico o manejo de datos.

Ataques a servidores

Según (TUTORIALES EN LINEA, 2019) un ataque a servidor es el acceso lógico violento para irrumpir en la integridad de los datos que alberga, protege o simplemente muestra en mínima cantidad. Día con día, y gracias a la WWW (World Wide Web) se amplían los modos de ataques, más también muchas de las veces no depende de los servidores, si del código ineficiente en cuanto a seguridad montado sobre este servidor, es entonces que se ha llegado a tomar los ataques a servidores como un problema real y se están tomando cada vez más seguridades sobre los métodos más viejos de la criptografía, la cual obviamente es peligrosa.

La única diferencia hoy es el número de capas complejas que se han añadido para hacer el proceso parecer confuso.

Según (MUÑOZ ESTRADA, 2019) en su trabajo de grado titulado "Vulnerabilidades de seguridad en el Sistema Académico Integrado en Red (Si@net) de la Universidad Estatal de Bolívar, año 2018", el servidor que aloja el Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, ha recibido un sinnúmero de ataques en todo el tiempo que lleva trabajando en favor de la comunidad universitaria, teniendo como consecuencias la alteración de algunos de los datos y el robo de información importante.

A continuación veremos algunos de ellos:

1. **Pishing:** El atacante enviará un correo electrónico fingiendo ser alguien de confianza, en ese mensaje estará un enlace de acceso a un sitio falso en donde el usuario atacado ingresa sus datos siendo capturadas de inmediato. (Rapid7 & Common Types of Cybersecurity Attacks, 2019)
2. **Inyección SQL:** Permite vulnerar las bases de datos accediendo a ellas a través del servidor web, mediante sus líneas de código con la acción de autocompletación, haciendo que el servidor haga lo que se le ha ordenado. (Rapid7 & Common Types of Cybersecurity Attacks, 2019)
3. **Cross Site Scripting (XSS):** Trabaja en modo silencioso haciendo que el usuario entregue sus datos importantes pero sin mostrar ningún tipo de anomalía. (Rapid7 & Common Types of Cybersecurity Attacks, 2019)
4. **Denegación de servicios:** Sobrecargar las peticiones a las que el servidor que aloja la aplicación o página web es capaz de atender de manera que este colapse de tal manera que su servicio finalice. (Rapid7 & Common Types of Cybersecurity Attacks, 2019)

Seguridad en Servidores Web

Según (Red Hat, 2019) una vez que un sistema es utilizado como servidor en la red pública, se convierte automáticamente en un objetivo de ataques maliciosos. Por esta razón, es importante para el administrador blindar el sistema de tal manera que se bloqueen ciertos servicios ajenos al servidor.

Se comercializan, desde ya algunos años en el mercado, herramientas que tienen como objetivo la protección de servidores web. Estos dispositivos de seguridad son capaces de ofrecer multitud de funcionalidades dispuestas a proteger el entorno web, una de estas es la puesta en marcha de un firewall de aplicación web (WAF), balanceo entre IPS y servidores además de la mejora en el rendimiento de las mismas aplicaciones web. Con esto podemos decir que ya tenemos muchas posibilidades de protección para aquello que muestre la empresa o sociedad mediante las plataformas web. (SEGURIDAD, 2019)

Entre los beneficios que nos ofrecen este tipo de dispositivos, se pueden destacar:

1. Protección de firewall e IPS sobre aplicaciones web.
2. Firewall de aplicaciones XML, implementando las capacidades IPS, sobre el código XML.
3. Balanceo de carga entre los servidores web, con el fin de conseguir una descongestión de los mismos.
4. Bloqueo de amenazas sobre las aplicaciones que corren en el servidor web como cross site, inyección SQL o ataques de buffer overflow.
5. Soporte para comunicaciones SSL y procesamiento de cifrado XML.
6. Cumplimiento de normativas de seguridad.
7. Reducción de la complejidad en la administración.

En cuanto a la seguridad de servidores de la Universidad Estatal de Bolívar, se mantiene en poder y administración de cada uno de sus usuarios administradores, por tanto no se mantiene un nivel de seguridad estándar.

Firewall

Según (Panda Security, s.f.) un firewall o cortafuegos es un sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada. Se puede implementar en forma de hardware, de software o en una combinación de ambos. Los cortafuegos impiden que los usuarios no autorizados accedan a redes privadas conectadas a Internet, especialmente a intranets. Todos los mensajes que entran o salen desde tu red local pasan por él, para que examine cada mensaje y bloquee los que no cumplan los criterios de seguridad especificados.

Redes

Según (Olifer, N. & Olifer, V, 2009) También conocidas como redes de comunicación de datos o de transmisión de datos, representan el resultado lógico de la evolución de dos de las ramas científicas y tecnológicas más importantes de la civilización moderna: las tecnologías de las computadoras y de las telecomunicaciones**.**

Sistemas señuelo o Honeypots

Honeypot

Según (The Honeynet Project, 2019) un honeypot (en inglés "tarro de miel") es un sistema muy flexible dentro de la seguridad informática, que se encarga de atraer y analizar el comportamiento de los atacantes en internet, y que provee al informático forense de una información extremadamente valiosa, se busca con esta implementación es capturar todo el tráfico de red entrante y conocer todos los detalles acerca de las tendencias y metodologías de ataque de los atacantes así como los fallos de seguridad en nuestra red con el fin de subsanarlos.

Los honeypots pueden ejecutarse bajo cualquier sistema operativo y bajo cualquier servicio. Los servicios configurados determinan los vectores de ataque disponibles para que el intruso comprometa y ponga a prueba el sistema.

Finalidad de los Honeypots

Estas son algunas de las posibilidades que nos ofrecen los honeypots:

- Desviar y distraer la atención del atacante.
- Detectar y aprender nuevas vulnerabilidades.
- Obtener información sobre el atacante (geolocalización, ip,puertos,etc).
- Obtener tendencias de ataque y paises más atacados.
- Detectar nuevas muestras de malware que aún no se conozcan.
- Recopilar y estudiar tendencias de ataque

Clasificación de Honeypots

Los honeypots se clasifican según su implementación (virtual o física) y su nivel de interacción (baja, media, alta).

Según su implementación:

- **Para producción:** Al implementar un honeypot en una red de producción, el objetivo principal es la obtención de información sobre técnicas empleadas para tratar de vulnerar los sistemas que componen dicha infraestructura.

- **Para investigación:** Por otro lado, en este caso los honeypots constituyen recursos educativos de naturaleza demostrativa cuyo fin es recopilar la mayor cantidad de información que permita al investigador poder analizar las nuevas tendencias y métodos de ataque así como los distintos objetivos atacados y orígenes de los ataques.

Según su interacción:

- **Alta interacción:** Este tipo de honeypots se trata de un sistema convencional, construidos con máquinas reales como el que podría utilizar cualquier usuario. Se sitúan generalmente en la red interna en producción y no tiene más utilidad que la de ser atacados, lo cual significaría que el sistema está mal configurado. Cada interacción con este honeypot se considera sospechosa por definición, y todo el tráfico debe ser monitorizado y almacenado en una zona segura de la red a la que un potencial atacante no tenga acceso.

- **Baja interacción:** Este tipo suele ser creado y gestionado por organizaciones dedicadas a la investigación de acciones fraudulentas en la red, con la cual se investiga acerca de nuevas amenazas en la red. Son más fáciles de utilizar y mantener, con un riesgo prácticamente nulo. Esta implementación se basa por lo general en una instalación de software de emulación de sistema operativo, utilizando herramientas conocidas como VMware o Virtual Box.

Tipos

Estos son algunos de los honeypots más conocidos:

- **Kippo**: Baja interacción, emula servicios de Secure Shell (SSH).
- **Glastopf:** Baja interacción para aplicaciones web.
- **Dionaea**; Baja interacción, sucesor de *"Nepenthes"* para la recogida de malware.
- **Honeyd:** Baja interacción , demonio que crea host virtuales en la red para servicios arbitrarios.
- **Sebek**: Alta interacción, funciona como HIDS (*Host-Based Intrusion Detection System*).
- Otros: KFSensor, Specter, HoneyBOT, HiHat (Jurado, 2016)

Honeynet

Según (Honeynet Project, 2003) la cual es una organización investigativa sin fines de lucro enfocada al aprendizaje de tácticas, herramientas y ataques de blackhat para luego compartirlas con la comunidad, no solo para que se alimenten de ellas sino también para que continúen con la mejora de la misma, es decir, impulsan el trabajo colaborativo bajo licencia open source. La principal herramienta para este fin es la Honeynet, que no es más que la unión complementaria de honeypots de alta iteración, creando de esta manera una red trampa, misma que se encarga de recolectar información del enemigo.

De esta manera se puede monitorear aquellos ataques que sucedan en tiempo real pudiendo aprender de ellos y logrando corregir poco a poco logrando mantener un perímetro seguro alrededor de la aplicación web.

DISEÑO METODOLÓGICO

Método De Investigación

Método Cualitativo

Según (Bonilla & Rodriguez, 2019) el método cualitativo trata de profundizar un objetivo específico cualificando y describiendo el fenómeno en base a rasgos que lo determinen a partir de un todo, mediante esta premisa se analiza y evalúa la situación actual de la aplicación de la seguridad en el servidor de la plataforma SI@NET.

TIPOS DE INVESTIGACIÓN

En este proyecto se utilizaron siguientes tipos de investigación:

Descriptiva

Según (Bonilla & Rodriguez, 2019) la investigación descriptiva busca describir la realidad del objetivo de estudio, su comportamiento y situaciones, a razón de esto se pudo permitió conocer la situación actual, tanto procesos como organización dentro de la Unidad de Redes de la Universidad Estatal de Bolívar mediante una descripción detallada de las características del área a investigar.

Bibliográfica

Según (Bonilla & Rodriguez, 2019) la investigación bibliográfica se refiere a toda aquella información encontrada en medios físicos y virtuales, como libros, páginas web, papers, blogs, etc. En esta investigación, al ser la raíz la seguridad informática y los métodos para su cuidado; sabiendo que a medida que avanzan los modos de ataques informáticos de la misma manera avanzan las vacunas, soluciones o herramientas que colaboran con el aseguramiento de los servidores web y las redes mismas, la información es extraída netamente desde el internet, tanto de publicaciones en blogs como también proyectos ya realizados en base al proyecto base (Honeypot Project, 2008) sustentando así el presente trabajo de grado.

De campo

Según (Bonilla & Rodriguez, 2019) la investigación de campo busca de extraer la información requerida directamente desde la realidad utilizando herramientas necesarias. A través de esta investigación se logró recopilar datos reales de la situación actual de la seguridad del servidor que alberga el sistema SI@NET, esto gracias a la ejecución: entrevistas (ver anexo1) y observación directa. (ver anexo 2)

TÉCNICAS E INSTRUMENTOS PARA LA OBTENCIÓN DE DATOS

Para la recopilación de datos se utilizaron las siguientes técnicas: entrevista (ver anexo 1) y observación directa (ver anexo 2), mismas que fueron empleadas en un momento adecuado y de estar manera se llevó a cabo el estudio y obtención de datos que nos sirvieron para la investigación.

Entrevista

Permitió obtener la información necesaria a través de un conversatorio formal con el Administrador de la Unidad de Redes de la Universidad Estatal de Bolívar y de esta manera se ha conseguido información que aporta al cumplimiento exitoso del proyecto de investigación.

Observación Directa

Se observó el comportamiento actual de los componentes utilizados para el funcionamiento del Sistema SI@NET: estructura de la red, configuración del servidor, firewall, ACLs en tiempo real.

Instrumentos

Para la presente investigación se realizó la obtención de la información mediante los siguientes instrumentos:

- Cuestionario de entrevista (ver anexo 1)
- Ficha de observación directa (ver anexo 2)

Universo y muestra

La Universidad Estatal de Bolívar posee una Unidad de redes y telecomunicaciones en donde el Ing. Patricio Pachala es el administrador de la red y los servidores existentes dentro de la institución por lo cual la entrevista se la hizo únicamente a él para recabar la información necesaria para el desarrollo del presente proyecto.

Procesamiento de Datos

Se logró la obtención de los datos mediante la utilización de la observación directa (ver anexo 1) y la técnica de entrevista (ver anexo 2), estos instrumentos tienen los requisitos de confiabilidad y validez, además de que está estructurada con su respectivo cuestionario lo que permitió mostrar la situación actual de los servidores y la red de datos de la Universidad Estatal de Bolívar y de la misma manera poder plantear una solución a la misma.

Puesto que esta investigación es cualitativa no se utilizó un análisis estadístico que muestre la reacción o comportamiento de la población.

ANÁLISIS DE RESULTADOS

Resultados obtenidos mediante la entrevista aplicada al administrador de la red previo a la construcción del prototipo de Sistema de Seguridad de Servidores Web mediante el uso de una herramienta señuelo. (Ver anexo 1)

1. **¿Qué Sistema operativo utiliza actualmente para los servidores?**

En la actualidad se utiliza el Sistema Operativo CentOS

2. **¿Con cuántos servidores tanto físicos como virtualizados cuentan?**

Enumere los aplicativos funcionando en cada uno de ellos

Físicamente cuentan con 10 servidores físicos funcionales y ninguno virtualizado.

a) Asociación de profesores
b) Dspace (Repositorio de Trabajos de grado)
c) Koha (Biblioteca)
d) Ciencias de la Educación
e) Entorno Virtual de Aprendizaje (.EVA)
f) Bolsa de Empleo
g) Departamento Financiero
h) Sistema Académico Integrado en Red (SI@NET)
i) Página Web de la Universidad Estatal de Bolívar
j) Mail institucional (Actualmente no está brindando servicio)

3. **¿A qué generación pertenecen cada uno de los servidores?**

No se puede definir a ciencia cierta a que generación pertenecen cada uno de ellos ya que fueron adquiridos de apoco y en ese entonces se mantenía una administración diferente por lo que se presume que al menos podrían tener unos 8 años cada uno.

4. **¿Qué tipo de accesos remotos utilizan para los servidores fuera de la intranet de la institución?**

Existe una configuración básica en general, pero en algunos de los casos como es el del SI@NET es el administrador quien se encarga de esa información.

5. **¿Se encuentra dividida la capa de datos de la capa de servicios?**

No se ha definido una división de las zonas de trabajo lógico dentro de los servicios de la red de servidores web.

6. **¿Cuentan actualmente con un firewall?**

Enuncie sus características

Si, se adquirió un firewall marca Fortinet FortiGate modelo: 2000E. en el año 2018 el cual posee las siguientes características, entre las mas importantes:

- Salida de firewall: 90000 Mbit/s,
- Rendimiento VPN: 65000 Mbit/s,
- IPS / IDS rendimiento: 25000 Mbit/s.
- Disipación del calor: 1467 BTU/h,
- Usuarios concurrentes: 10000 usuario(s),
- Nivel de ruido: 58 dB.
- Número de usuarios: 10000 usuario(s).
- Algoritmos de seguridad soportados: SHA-256,
- Seguridad con cortafuegos: UDP,
- Soporte VPN: IPsec, SSL.
- Plataforma de gestión: FortiOS (Icecat, 2019)

7. ¿Cuáles son las configuraciones de seguridad se están aplicando a dicho firewall?

Mantiene la configuración básica, es decir no se están utilizando todos los beneficios que brinda el mismo y con la actualización de firmware (6.0) al 12 de junio del año 2018 por parte de la Empresa externa SOLINFRA CIA LTDA, el cual mostro que está trabajando en el rango de temperatura normal y el uso del procesador de hasta el 7% de capacidad, funcionando de manera óptima.

8. ¿Qué tipo de seguridad se utiliza actualmente para salvaguardar la información contenida en dichos equipos?

Se guarda una gran confiabilidad en salvaguardar la información y por medio de esta la seguridad de la misma el hecho de poseer un firewall, el cual fue configurado no hace menos de un año además de la creación de backups.

9. ¿Qué reglas de autenticación aplican para el acceso a servidores?

A pesar de estar a cargo de un administrador, en algunos de los casos son los mismos encargados de los sistemas que funcionan dentro de los servidores quienes manejan la autenticación.

10. ¿Existe un informe detallado sobre las vulnerabilidades o ataques informáticos que han recibido los servidores?

Si, No. Explique.

No existe, nunca se ha hecho un análisis forense de ciertas anomalías en los servidores únicamente se ha tratado de corregir en cuanto a código.

11. ¿Poseen actualmente un sistema señuelo?

De ser afirmativa su respuesta explique cuál es.

No existe pero se tiene un ligero conocimiento del mismo

12. ¿Cuáles son las reglas ACL (Listas de Control de Acceso) configuradas en el servidor de la plataforma SIANET?

No existen listas de control de acceso configurado en routers ni en el firewall.

13. ¿Qué método de recuperación de datos poseen en el caso de sufrir algún tipo de caída de servidores?

Únicamente está la creación de Backups

14. ¿Poseen Listas de Contr

15. ol de Acceso?

No, ninguno de los routers, switches o firewall tienen una configuración similar.

16. ¿Poseen políticas de seguridad?

Actualmente no

17. ¿Poseen un IDS?

No, el actual firewall en funcionamiento posee dentro de si el servicio pero no se encuentra configurado

Análisis e interpretación

- Los servidores web de la institución son custodiados por el administrador de la Unidad de redes y telecomunicaciones de la Universidad Estatal de Bolívar, se encuentran en dicho departamento, pero los mismos no son lógicamente administrados por la persona en cuestión, sino en ciertos casos por cada uno de los directores o administradores de los sistemas que se alojan en cada uno de ellos.
- El firewall adquirido a través de la contratación externa de una empresa de infraestructuras de red posee características que están siendo pasadas por alto.
- Poseen dos métodos para salvaguardar o asegurar la información que es a través de la utilización del firewall y la creación de backups, además de que no cuentan con una DMZ, IDS, ACLs o políticas de seguridad actualmente implementadas.

Resultados de la ficha de observación dirigida a la Unidad de Redes y Telecomunicaciones

Observador: Verónica Chico Redrobán

Tema: Sistema de Seguridad de Servidores Web mediante el uso de una herramienta señuelo aplicado a la plataforma SIANET de la Universidad Estatal de Bolívar, año 2019.

Aspectos a observar:

a) Estructura de red para ubicación estratégica de la herramienta

Una estructuración de la red a nivel universitario es de gran importancia en este proyecto debido a que en base a ella se decide la ubicación estratégica de la herramienta Honeynet para su óptimo funcionamiento pero lastimosamente no se encontró documentación del crecimiento de la red tan solo planos antiguos.

b) Políticas de Seguridad

Actualmente no se han implementado dichas políticas son el protocolo, normas y reglas que dicen cuál es el modo de manejar la información para de esta manera cuidar la integridad de la Universidad Estatal de Bolívar.

c) IDS, DMZ, ACLs y VLANs

IDS: Un Sistema de detección de intrusiones monitorea accesos no autorizados, el firewall en función actual posee un IDS pero no está configurado.

DMZ: La zona desmilitarizada permite separar los servicios que prestan los servidores, actualmente no existe.

ACLs: Estas listas de control de acceso permiten controlar las áreas de la red a donde los clientes pueden acceder, actualmente se encuentran en configuración.

VLANs: Redes de área local y virtual, permiten hacer divisiones lógicas de una red física. No se cuenta con documentación.

Análisis e interpretación:

De acuerdo con lo recopilado dentro de la observación directa y a través de la misma se decide plantear el diseño de un prototipo funcional adaptable de la herramienta señuelo Honeynet.

RESULTADOS

Resultado del primer objetivo

A través del análisis de la situación actual de la seguridad de la información del servidor web de la plataforma SI@NET se llega a la conclusión de que existen dos problemas bastante visibles; en cuanto a hardware existe un descuido de actualización tecnológica, esto debido a que un servidor web tiene una vida útil de 5 años más sus debidos mantenimientos tanto preventivos como correctivos, más en la actualidad, y por su uso ya sus productores los han reforzado, de esta manera los atacantes ya no lo ven quizá como una vía de ataque y se enfocan en las falencias en cuanto a su código (software), por lo cual un desarrollador juega un papel estratégico para cuidar la seguridad de las páginas web.

Resultado del segundo Objetivo

Se propone un diseño de la arquitectura adaptable de prototipo de sistema de seguridad de servidores mediante la herramienta señuelo Honeynet, bajo una configuración modificable.

Resultado del tercer objetivo

Se muestra el trabajo del prototipo funcional monitoreando la red, registrando ataques simulados mediante el uso de los recursos y herramientas definidos para esta causa.

DISCUSIÓN

La seguridad de la información es una pieza de vital importancia en toda entidad que maneje gran cantidad de información, en este caso la Universidad Estatal de Bolívar al ser una institución de educación superior necesita cuidar los datos que a ella llegan y también envía a través de su red de comunicación. A través de los métodos de investigación utilizados en este proceso se ha logrado localizar los datos necesarios para poder construir la propuesta de análisis, diseño e implementación de una herramienta señuelo.

Esta herramienta tiene una tendencia OpenSource, por lo que no se necesita pagar licencias para la instalación de cada uno de sus componentes también llamados nodos que son la clave del funcionamiento óptimo de la herramienta para que el atacante no pueda sospechar de que es un Honeypot, este término quiere decir "tarro de miel" de donde viene toda la idea de este proyecto ya que un tarro de miel es un señuelo para osos, pues bien, los atacantes son nuestros osos hambrientos.

Análisis de riesgos informáticos

Para realizar la aplicación de nuevos proyectos para la optimización de la seguridad dentro de una institución es necesario realizar un analisis de riesgos informáticos, mismo que muestra la situación actual de cada una de las dependencias que requieren cuidado en cuanto a seguridad.

Quizá una de las razones mas notables por las que las inseguridades informaticas aun no han tenido solución directa es por la aparición de renovadas amenazas, es por esto que al mismo tiempo que estas evolucionan tambien lo debe hacer la seguridad informática para de esta manera porder mitigar contantemente los peligros que amenazan la información que mas debe ser cuidada. El analisis de riesgos requiere pasos a seguir, dependiendo del caso, para lograr un resultado confiable de los riegos existentes, en mi caso se analizan los riesgos en cuanto al servidor SIANET.

Para este análisis se utilizó las metodologías: Magerit y Octave. (MAÑAS, J. AMUTIO;, 2012)

Identificación de riesgos

- **Sistemas**

Servidor web

Firewall

Equipos de red

- **Personal**

Soporte técnico interno

Soporte técnico externo

Administración de servidores

- **Datos**

Base de datos

Plataforma web

Respaldos

Documentación

Niveles de medición

A continuación se detallan los rangos de valores que califican a cada uno de los idenficativos y con los cuales, mediante una multiplicacion se logra conocer el nivel de riego de cada uno.

Magnitud del daño: Muestra que tan severo puede llegar a ser el daño en determinado activo.

	Baja	**Mediana**	**Alta**

Magnitud del daño	1	2	3

Tabla 1 Analisis de riesgos - Magnitud de daño

Autor: Verónica Chico

Probabilidad de amenaza: Se refiere al número de veces que la amenaza puede presentarse independientemente de si esta sea o no contrarrestada.

	Baja	**Mediana**	**Alta**
Probabilidad de amenaza	1	2	3

Tabla 2 Analisis de riesgos - probabilidad de amenaza

Autor: Verónica Chico

Nivel de impacto: Mide las consecuencias del efecto de las múltiples amenazas mismas que pueden ser pérdidas monetarias en un corto o largo plazo.

	Bajo			**Medio**			**Alto**		
Nivel de impacto	1	2	3	4	5	6	7	8	9

Tabla 3 Análisis de riesgos - nivel de impacto

Autor: Verónica Chico

Riesgo según color:

Verde: Nivel de impacto bajo, representa un nivel de riesgo aceptable en donde se lo puede asumir, compartir o asignar y tolerar.

Amarillo: Nivel de impacto medio, considerada una zona de riesgo moderada en donde aún se puede prevenir el riesgo, proteger y mitigar.

Rojo: Nivel de impacto alto, considerada una zona de riesgo inaceptable al cual hay que ponerle mucha atención y darle solución inmediata.

Matriz de análisis de riesgos

AMENAZAS - PROBABILIDAD DE AMENAZA (BAJA=1) (MEDIANA=2)(ALTA=3)																			
ATRIZ DE RIEGOS SERVIDOR WEB CONTENEDOR DEL SIANET		OR. FÍSICO				USUARIO		HARDWARE		DATOS	SOFTWARE		INFRAESTRUCTURA		POLITICAS			RED	
		Sismo	Polvo	Daño disco duro	Falta de ventilación	Falta de capacitación, inducción y sensibilazión sobre riesgos	Pérdida de datos por error de usuario	Falta de mantenimiento físico	Renovación de equipos	Transmisión no cifrada de datos	Actualización procesos y recursos	Mejoras nivel seguridad	Red cableada expuesta acceso no autorizado	Dependencia servicio externo	Falta de mecanismos de autenticación	Ausencia de documentación	Falta de definición de políticas de privacidad	Ausencia de documentación estructural y de configuración	Implementación ACLs nula
		1	2	3	2	3	2	3	3	2	2	2	1	2	2	3	3	3	3
Servidor web	3	3	6	9	6	9	6	9	9	6	6	6	3	6	6	9	9	9	9
Firewall	2	2	4	6	4	6	4	6	6	4	4	4	2	4	4	6	6	6	6
Equipos de red	2	2	4	6	4	6	4	6	6	4	4	4	2	4	4	6	6	6	6
Soporte técnico interno	1	1	2	3	2	3	2	3	3	2	2	2	1	2	2	3	3	3	3
Soporte técnico externo	2	2	4	6	4	6	4	6	6	4	4	4	2	4	4	6	6	6	6
Administración servidores	3	3	6	9	6	9	6	9	9	6	6	6	3	6	6	9	9	9	9
Base de datos	3	3	6	9	6	9	6	9	9	6	6	6	3	6	6	9	9	9	9
Plataforma web	3	3	6	9	6	9	6	9	9	6	6	6	3	6	6	9	9	9	9
Respaldos	2	2	4	6	4	6	4	6	6	4	4	4	2	4	4	6	6	6	6
Documentación	1	1	2	3	2	3	2	3	3	2	2	2	1	2	2	3	3	3	3

Tabla 4 Análisis de riesgos - Matriz de análisis de riesgos

Autor: Verónica Chico

CONCLUSIONES

Mediante esta investigación se llega a conocer la siguiente problemática:

Conclusión matriz de análisis

De acuerdo con la información encontrada a través del análisis de riesgos se demuestra que en realidad, en cuanto al servidor web que contiene al SIANET posee un riesgo alto de seguridad no solo de servidor sino también de sus componentes que lo rodean, que dicho sea de paso son un conjunto de piezas vitales para el buen tratamiento de la seguridad de la información.

Conclusión primer objetivo

La situación actual de la seguridad de la información del servidor web de la plataforma SI@NET, se encuentra en un nivel medio de protección; esto a razón de que algunas de las vulnerabilidades encontradas en los últimos meses ya han sido corregidas, más un gran porcentaje de ellas aún son parte de los objetivos para los atacantes.

Conclusión segundo objetivo

Bajo la realización de un diseño de arquitectura adaptable de un sistema de seguridad de servidores, mediante el uso de una herramienta señuelo o honeynet, denominada también red trampa, se espera que luego de una documentación adecuada de la estructura de la red, configuración de VLANs, las configuraciones del firewall, ACLs, DMZ, políticas de seguridad que actualmente se encuentren funcionando en la Universidad Estatal de Bolívar, se pueda poner en funcionamiento.

Conclusión tercer objetivo

Mostrando la ejecución del prototipo adaptable de sistema de seguridad mediante el uso de una herramienta señuelo Honeynet o red y un ataque simulado se muestra la recolección de datos importantes sobre algunos modos de ataque.

RECOMENDACIONES

De acuerdo con los resultados obtenidos en esta investigación, es importante establecer las siguientes recomendaciones:

Recomendación sobre la matriz de análisis

Es necesario proponer un plan de contingencia basado en la propuesta de este proyecto.

Recomendación para el primer objetivo

Priorizar la seguridad de la información alojada en los servidores web no solo mediante la remodelación de los medios físicos; es decir, respetar la vida útil de los equipos, sino también con la actualización del software y mejoras disponibles, mantenimiento del mismo además de la colaboración de en base al refuerzo de seguridades en la codificación e implementación de otros métodos disponibles para los aplicativos montados y funcionando el mismo, formando de esta manera una especie de escudo colaborativo ante los ataques informáticos.

Recomendación para segundo objetivo

Documentar el crecimiento de la red, la configuración de cada uno de sus componentes y su estado para con esto poder hacer uso positivo en beneficio de la protección de la posible información expuesta, llevando así una bitácora de mejoras u observaciones útiles.

Recomendación para el tercer objetivo

Capacitar a las personas a cargo del Sistema Académico Integrado en Red (SI@NET) en cuanto al uso de herramientas que colaboren en favor de la mitigación de los ataques a servidores web para poder aprovechar y hacer uso de los datos que se puedan obtener y asimismo poder dar un mantenimiento adecuado a la misma.

PROPUESTA DE SOLUCION DEL PROBLEMA

Plan de contingencia propuesto a partir de los resultados del análisis de riegos

Un plan de contingencia es aquel que menciona las acciones a seguir en caso de que ocurriera algún desastre, es decir es un plan de recuperación.

Se presenta la propuesta de implementación de una Honeynet como una de las soluciones a los problemas de seguridad informática encontrados a través de la matriz de riesgos. (ver Tabla 4)

Antecedentes

A través de la investigación previamente realizada, además gracias a los datos recogidos en el trabajo de grado "Vulnerabilidades de seguridad en el Sistema Académico Integrado en Red (SI@NET) de la Universidad Estatal de Bolívar, año 2018" (MUÑOZ ESTRADA, 2019), en donde muestra las vulnerabilidades localizadas en los protocolos de seguridad utilizados en el servidor y la misma aplicación SI@NET. Con todos estos datos se propone la construcción y configuración de una Honeynet (red trampa) con base de sistemas operativos libres y virtualizados, como uno de los métodos de mitigación de ataques al sistema SI@NET, conociendo así al enemigo y su modus operandi, es decir, a través de la recolección de los modos de ataque se puede seguir reforzando la seguridad sin poner en riesgo la integridad de la información.

Justificación

La presente propuesta se la realiza buscando un cuidado de la seguridad del servidor web que aloja el Sistema Académico Integrado en Red (SI@NET) en la Universidad Estatal de Bolívar debido a que al poseer información de vital importancia, tanto de estudiantes como, docentes y personal administrativo hay que priorizar el refuerzo de las herramientas que colaboren con la custodia la misma para de esta manera mantener el buen nombre de la institución y a la vez

aprender a partir de los datos recogidos con la herramienta y de esta manera lograr corregir errores a medida que los ataques se vayan produciendo.

Objetivos

Objetivo General

Crear un prototipo funcional de un sistema de seguridad de servidores web mediante el uso de una Honeynet o red señuelo.

Objetivos Específicos

- Analizar los requerimientos necesarios para la construcción de una Honeynet
- Diseñar el prototipo adaptable de Honeynet
- Simular el funcionamiento básico

Factibilidad

Para definir la factibilidad de la propuesta presente, se tomaron en cuenta los más importantes aspectos para que este tenga viabilidad.

Legal

Este proyecto cumple con todas las normas legales debido a que al ser de libre distribución y utilización por parte de los usuarios, no infringe ninguna política o pago de licencia.

Económica

Es factible realizar el proyecto pues no necesita un mayor monto de dinero, en cuanto a licencias y en el caso de equipo hardware se reduce al mínimo pues se está utilizando la virtualizción.

Tecnológica

Al ser una tecnología relativamente nueva se toma como iniciativa a la mejora de las tecnologías dentro de la Universidad Estatal de Bolívar para el mejor manejo de la seguridad informática y de esta manera también crecer tecnológicamente.

Estructura de una Honeynet

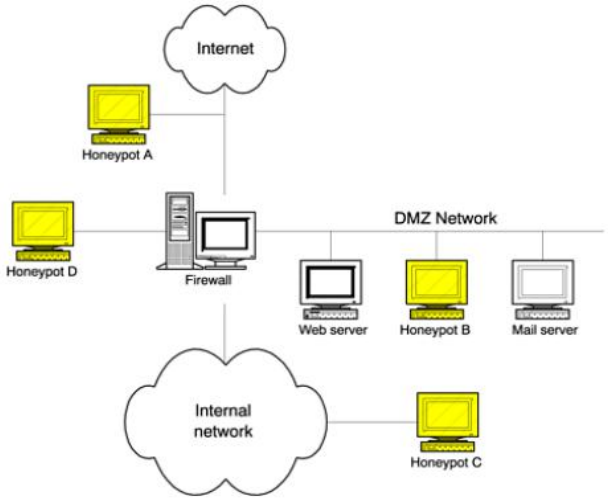


Figura 1 Ejemplo de Honeynet

Fuente: Proyecto Honeynet

Ubicación

La posición de esta red trampa será elegible debido a que está virtualizada, por lo tanto mejora la portabilidad y puede ser modificada para bien del lugar en donde se presente la necesidad de conocer cuan segura esta nuestra información, esta posición permitirá que el Honeynet logre captar los ataques que se hagan desde afuera tanto como dentro de la red.

Recursos

Para el diseño y construcción de la red señuelo se utilizó software de tipo libre, es decir, sin necesidad de adquirir licencia. Además se emularon las maquinas necesarias a través de la virtualización en una sola maquina abaratando costos y mejorando la portabilidad.

Implementación de una Honeynet

A continuación se detallan paso a paso los procedimientos e instrumentos necesarios para la configuración, instalación y virtualización de las herramientas que se utilizaron en la construcción de la herramienta señuelo **Honeynet**.

Especificaciones técnicas del diseño

Se utilizó:

- Software de virtualización: “Oracle VM Virtual Box V6.0.6”
- Sistemas Operativos: Windows 10 (Anfitrión). Clientes: CentOS, Xubuntu y Debian
- IDS: Snort (red), Ossec (host)

Computador Anfitrión en donde se virtualizaran los sistemas clientes

Modelo	Asus X555L
Procesador	Intel Core i7 5ta
Tipo de Sistema	64 bits
Sistema operativo	Windows 10
Disco Duro	1 Tb
RAM	6gb
IP	*****

Tabla 5 Especificaciones técnicas pc anfitrión

Autor: Verónica Chico

Clientes virtualizados

Sistema Operativo	CentOS 7	Xubuntu	Debian
Disco Duro	8 GB	6 GB	6 GB
RAM	1024 MB	1024 MB	1024 MB
IP	****	****	****
Detalles	Se encarga de recoger la información de los otros clientes. Tiene instalado: IDS de red: Snort IDS host: Ossec en modo servidor	Cliente, funciona como señuelo de la Honeynet HoneyDrive: preinstalado IDS host: Ossec en modo cliente	Cliente, funciona como señuelo de la Honeynet. IDS de red: Ninguno IDS host: Ossec en modo cliente

Tabla 6 Especificaciones técnicas de las máquinas virtuales

Autor: Verónica Chico

Instalación de Centos

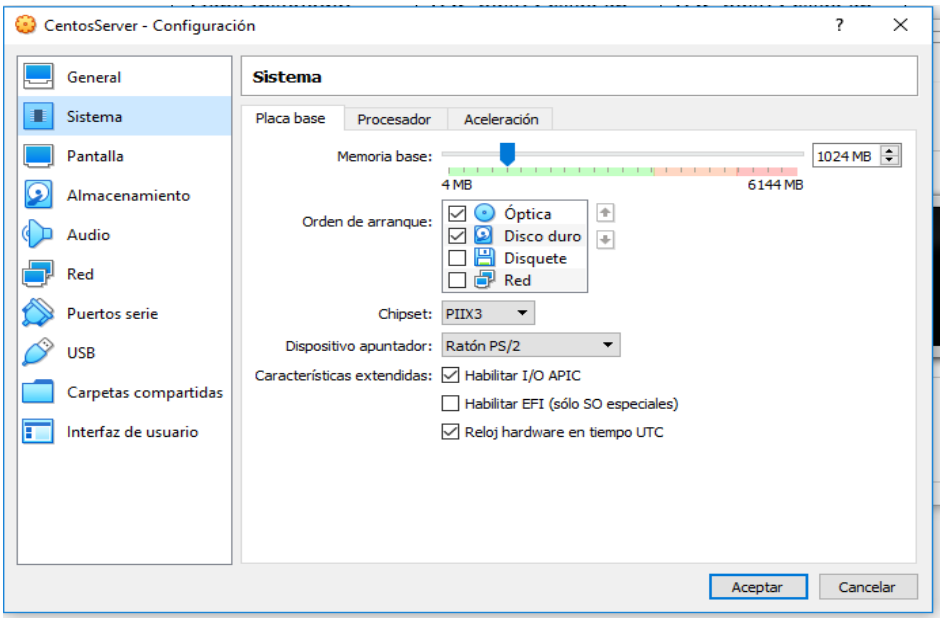


Figura 2 Configuraciones de distribución de memoria

Fuente: Virtual Box

Se procede a la instalación:

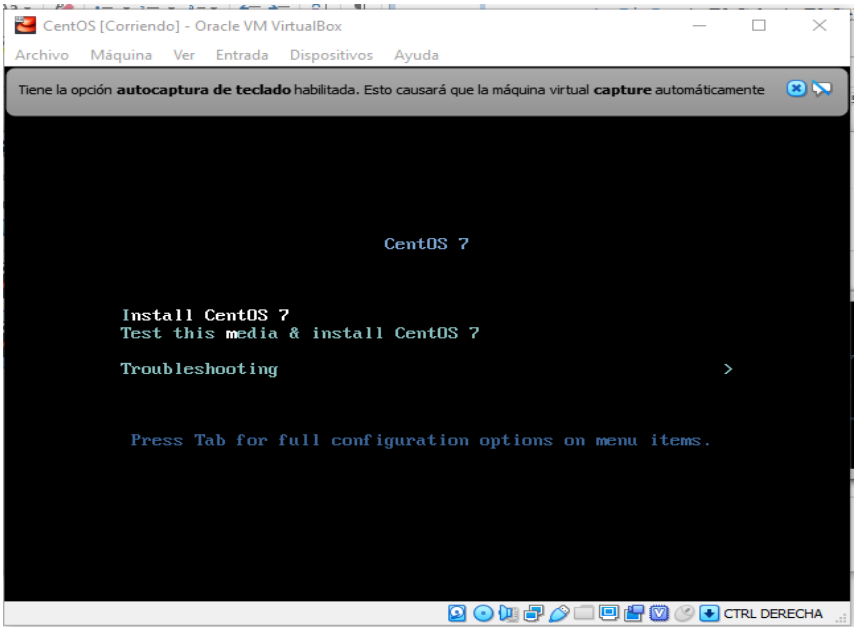


Figura 3 Instalación gráfica de Centos

Fuente: CentOS 7

Se elige idioma español de nuestra región, Ecuador.

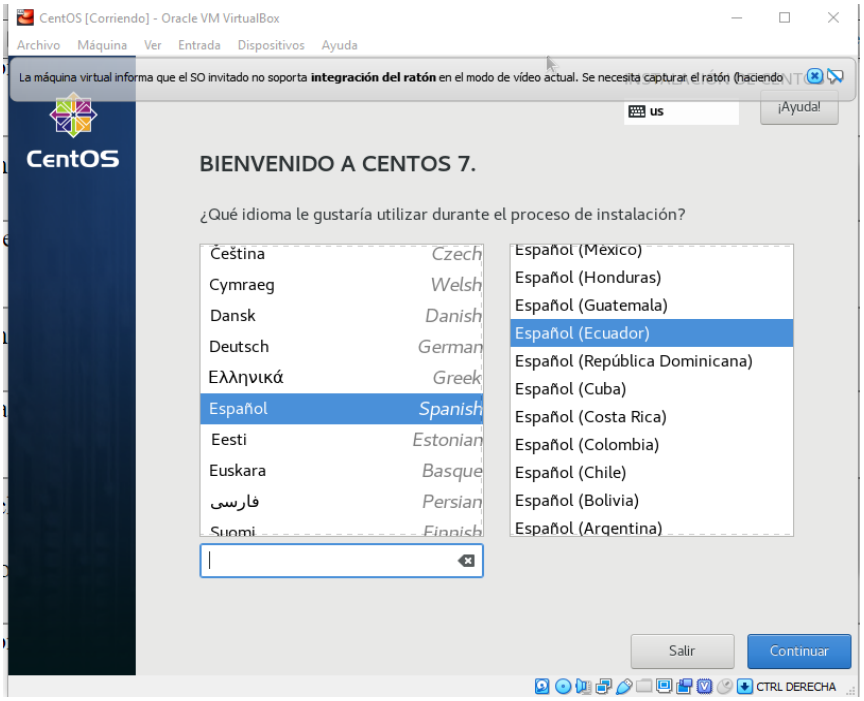


Figura 4 Idioma de Sistema

Fuente: CentOS 7

En la sección Sistema, selecciona el disco de destino de la instalación de Centos

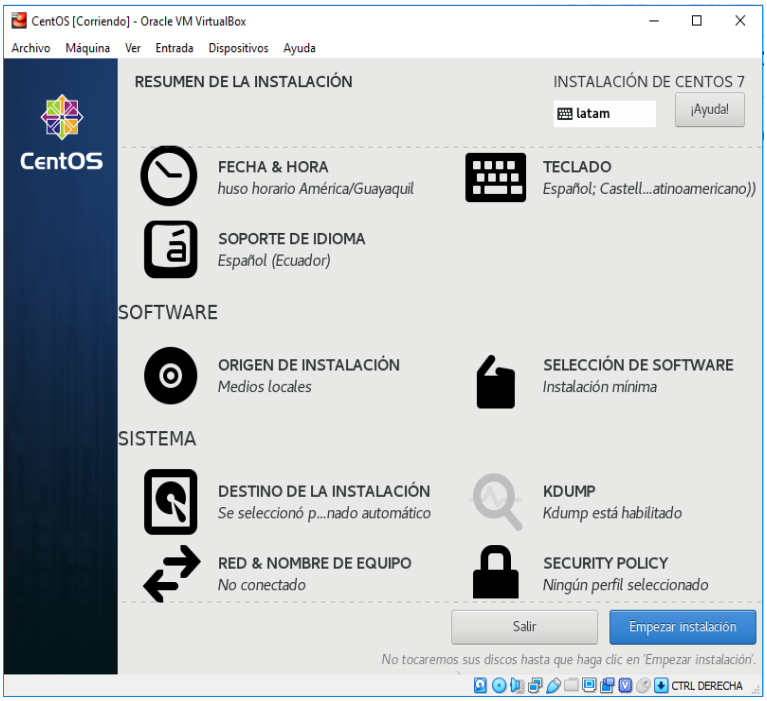


Figura 5 Destino de instalación

Fuente: CentOS 7

Selecciona todo el disco ya que al ser una máquina virtual no necesitaremos partición manual sino por defecto, damos clic en Listo.

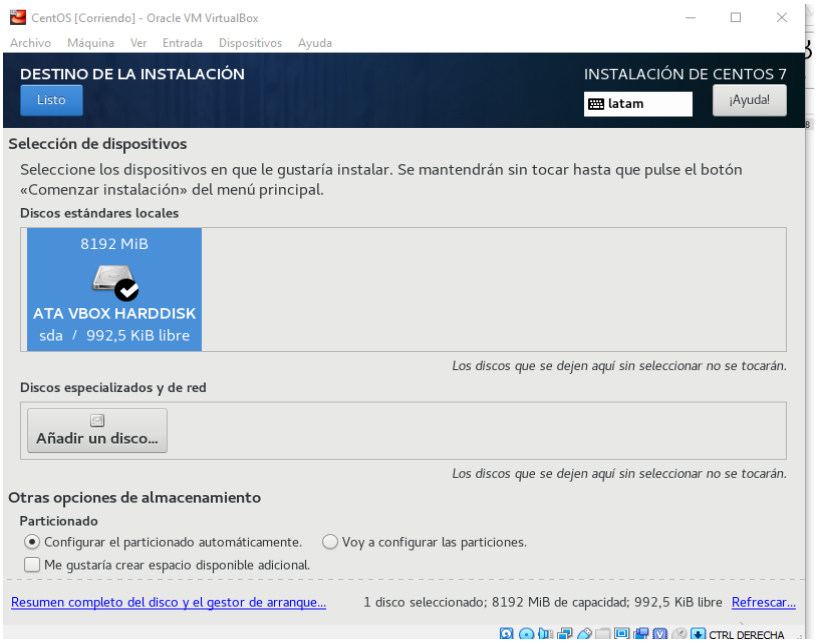


Figura 6 Disco destino de instalación
Fuente: CentOS 7

Se configura la red



Figura 7 Configuración de

Fuente: CentOS 7

Se activa su conexión

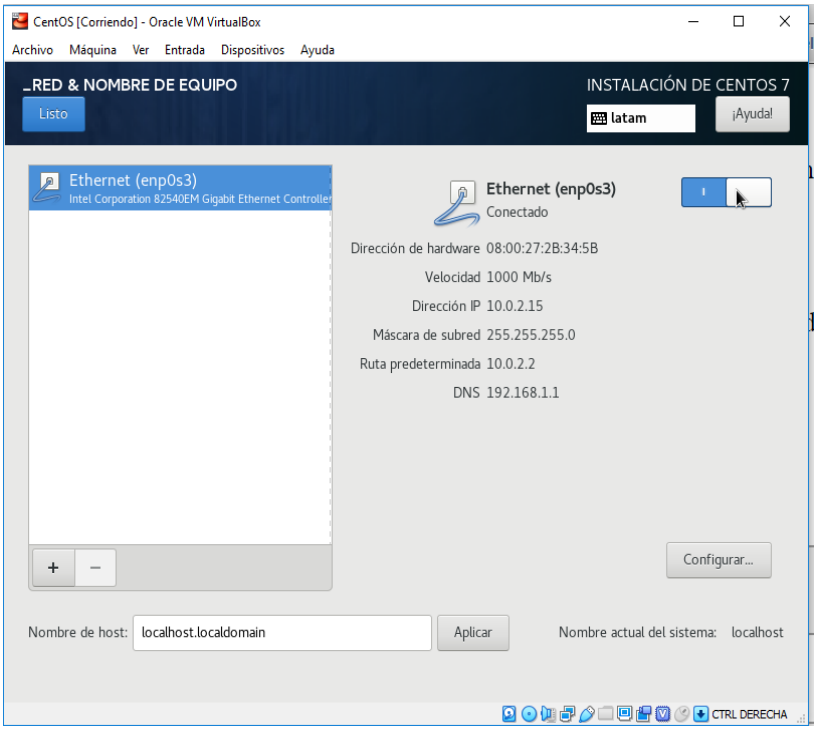


Figura 8 Conexión de

Fuente: CentOS 7

En la sección se Software vamos a elegir el tipo de instalación que necesitamos de nuestro sistema operativo Centos.



Figura 9 Selección de software de instalación

Fuente: CentOS 7

Seleccionamos **Servidor con GUI**, es decir con Interfaz gráfica más los complementos que creamos necesarios.

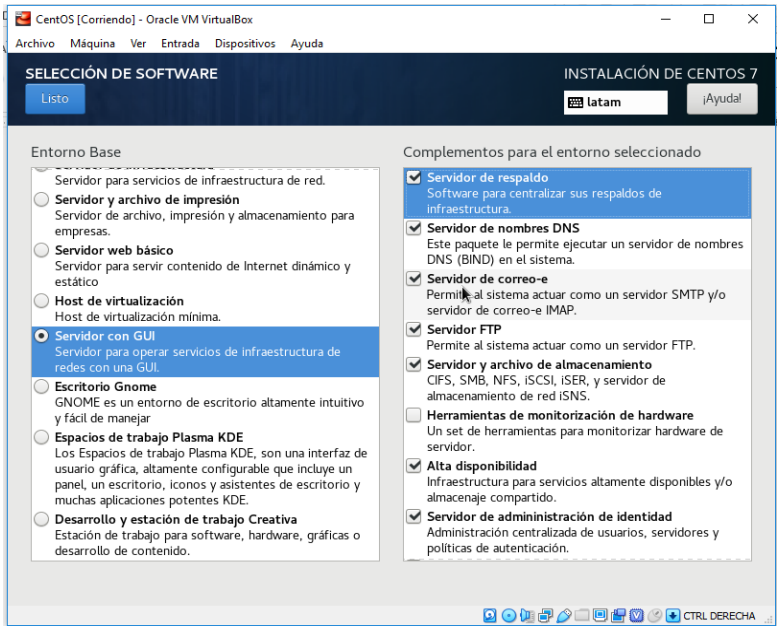


Figura 10 Selección de software de instalación más sus complementos

Fuente: CentOS 7

La instalación ha empezado, y mientras esto sucede hay que configurar tanto **Contraseña de root** como también la **Creación de usuarios** ya que en los Sistemas operativos de Linux existen dos tipos de usuarios; uno para realizar instalaciones en el sistema y otro para trabajar dentro de el sin hacer ningún cambio administrativo



Figura 11 Ajustes de usuario

Fuente: CentOS 7

Una vez concluido este proceso, el proceso es similar a cualquier instalación de un Sistema operativo, por lo tanto se procede a reiniciar la máquina virtual.

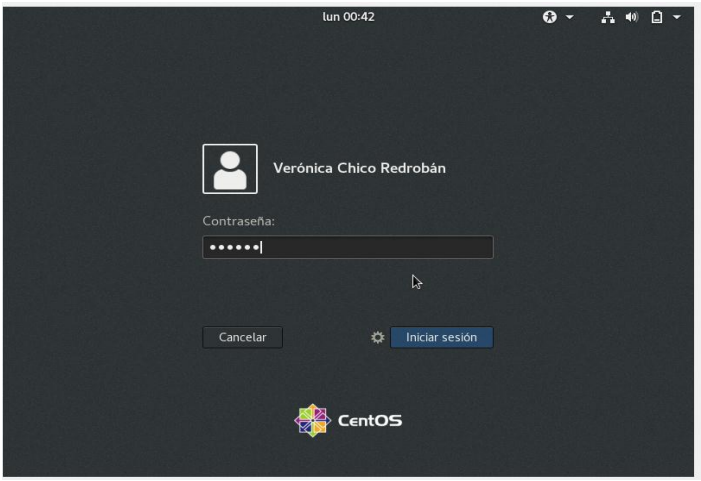


Figura 12 Interfaz de Centos

Fuente: CentOS 7

Configuración bajo consola/terminal de Centos como servidor web

Servidor web: Apache

Lenguaje de programación: PHP7

Base de datos: MySql

Comando de instalación de Apache

Accedemos a la Consola de Centos en donde debemos rootearnos como super usuario a traves del comando: **$su** para posteriormente ingresar el comando de instalación **$yum install httpd.**

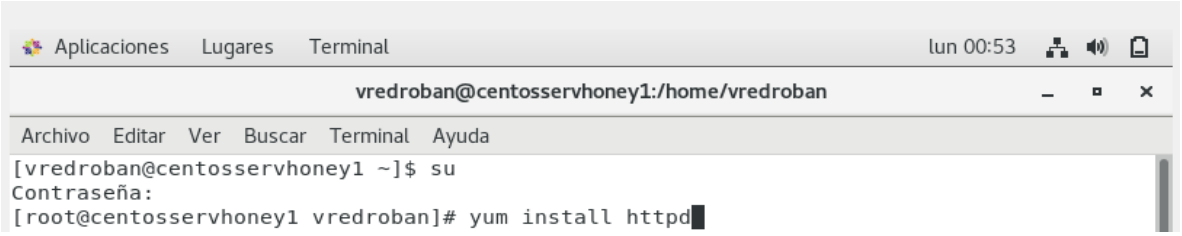


Figura 13 Ingreso root e instalación de Apache

Autor: Verónica Chico

Por consiguiente el sistema analizara los componenetes necesarios para la instalación por lo que solicitará su aprobación.

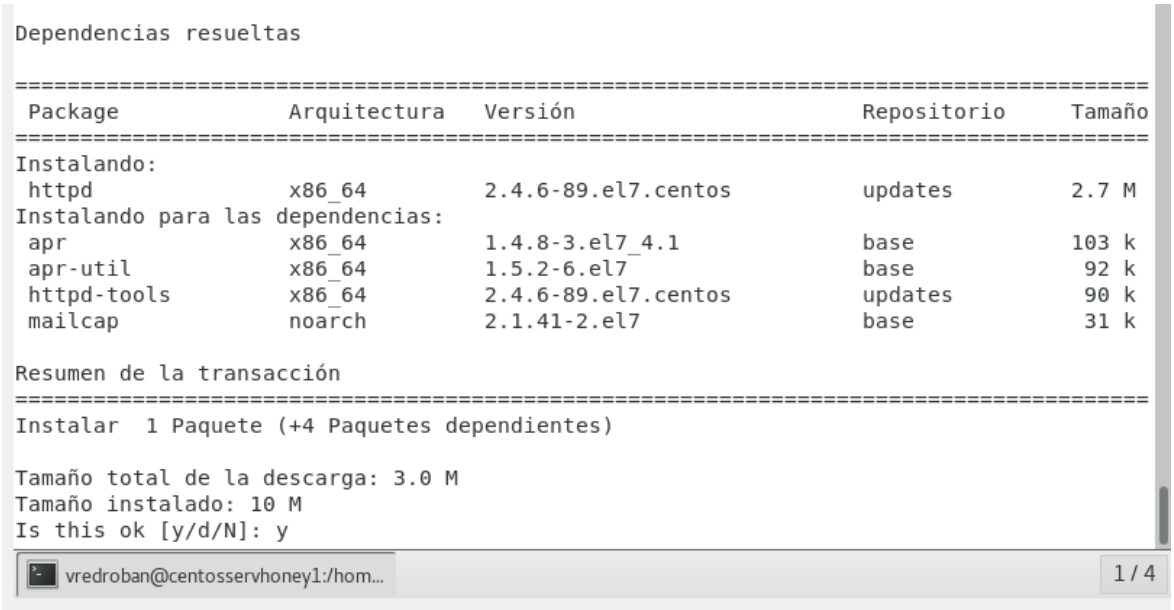


Figura 14 Aprobación de instalación

Autor: Verónica Chico

Continuamos con la instalación de php

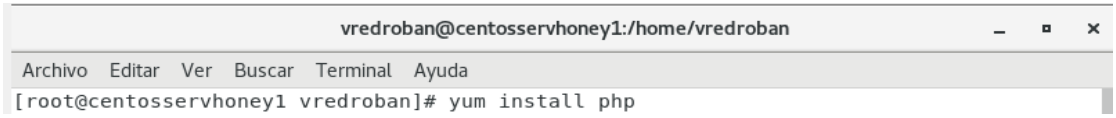


Figura 15 Instalación de php

Autor: Verónica Chico

Ahora instalamos Mysql server

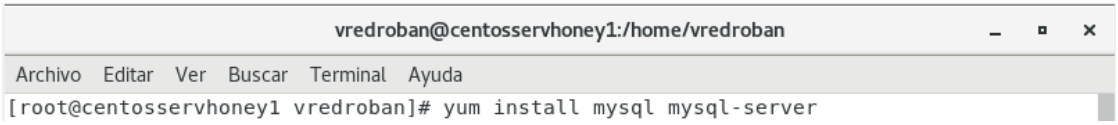


Figura 16 Instalación de Mysql server

Autor: Verónica Chico

Levantamos el servicio

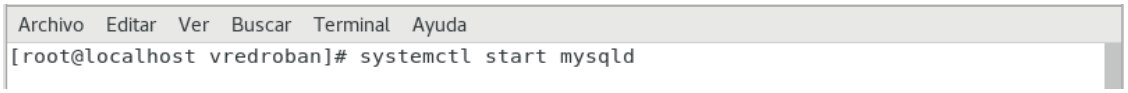


Figura 17 Levantamiento de servicio

Autor: Verónica Chico

Verificamos que esté funcionando correctamente

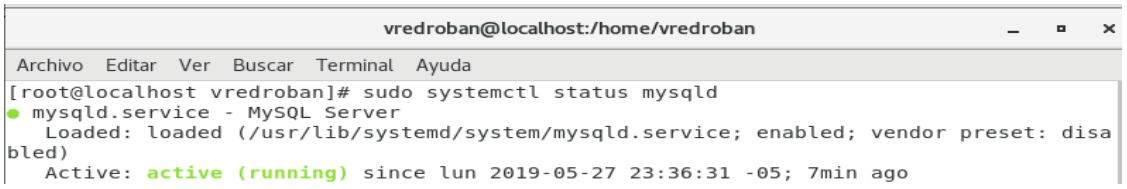


Figura 18 Verificación funcionamiento mysql

Autor: Verónica Chico

Y agregamos el enlace con de php y mysql

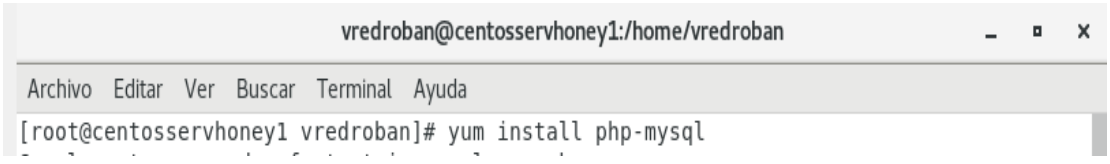


Figura 19 Enlace php y mysql

Autor: Verónica Chico

Verificar la instalación del servidor y php

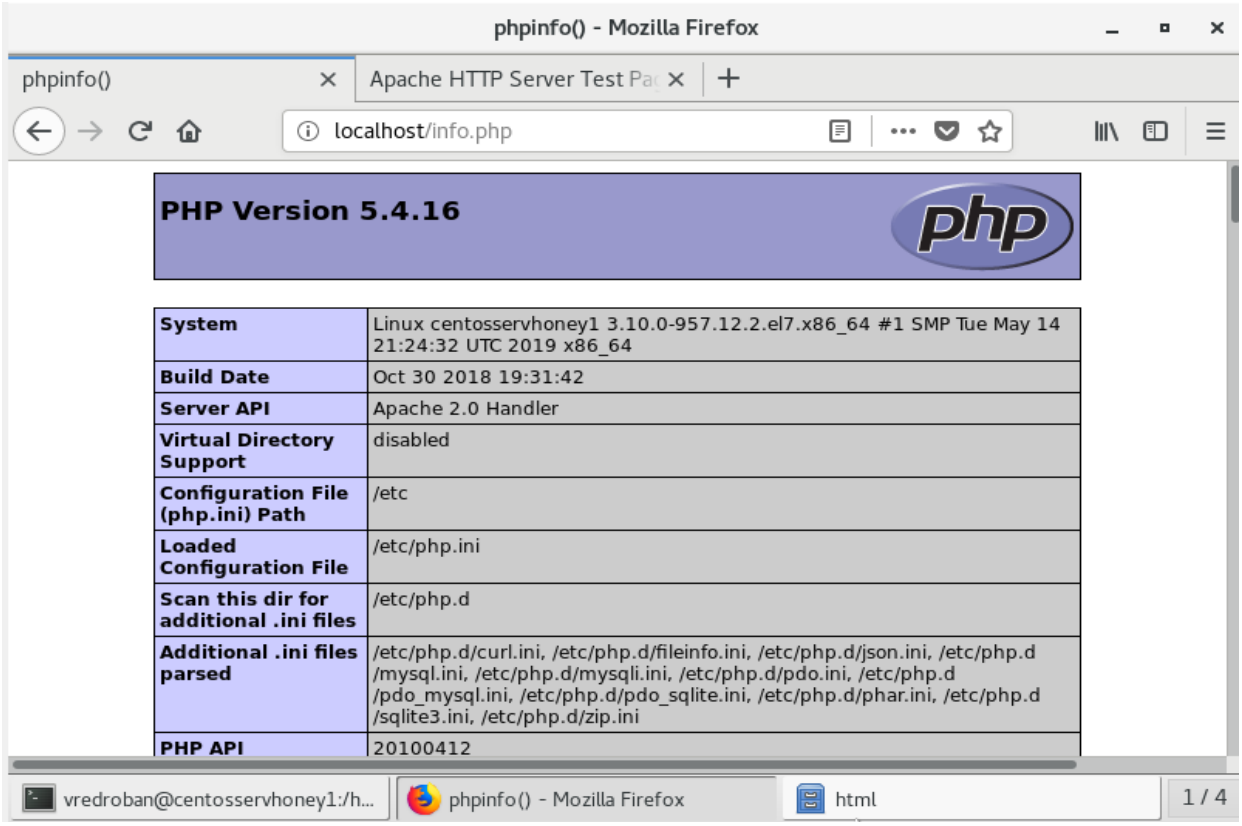


Figura 20 Apache y Php corriendo

Autor: Verónica Chico

Instalación de NIDS Snort en Centos

Snort es un sistema de prevención de intrusiones de código abierto capaz de análisis de tráfico en tiempo real y registro de paquetes. (Roesch, 2019)

Modos de trabajo de Snort

- **Sniffer**: Muestra dirección ip y cabeceras tcp/udp/icmp.
- **Packet logger:** Especifica el directorio de almacenamiento de los archivos log de snort.
- **Network Intrussion Detection System (NIDS):** Captura y manipula de paquetes entrantes y salientes en el segment de red.
- **Inline:** son mensajes de alerta que llevan información con datos importantes de los paquetes que viajan por la red.

A continuación se detallan los pasos y comandos a utilizar para su instalación dentro del servidor de Centos como IDS de red pues a través de él se monitorea la red y se recolecta la información de la misma.

Preparando requisitos previos de instalación

```
[root@localhost vredroban]# yum install -y libnghttp2
```

Se necesitan algunas librerías importantes

```
vredroban@localhost:/home/vredroban
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost vredroban]# sudo yum install -y gcc flex bison zlib libpcap pcre libdnet tcpdump
```

Figura 21 Instalando librerías

Autor: Verónica Chico

Se necesitan además librerías que se encuentran fuera de la página oficial

```
vredroban@localhost:/home/vredroban
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost vredroban]# sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@localhost vredroban]# sudo yum install -y zlib-devel libpcap-devel pcre-devel libdnet-devel openssl-devel
ibnghttp2-devel luajit-devel
```

Figura 22 Instalando librerías externas

Autor: Verónica Chico

Crear una carpeta temporal de descarga

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost vredroban]# mkdir ~/snort_src && cd ~/snort_src
```

Figura 23 Creando carpeta temporal

Autor: Verónica Chico

Descargar de la fuente e instalar DAQ, bibliotecas de adquisición de datos que sirven para hacer llamadas abstractas a bibliotecas de captura de paquetes.

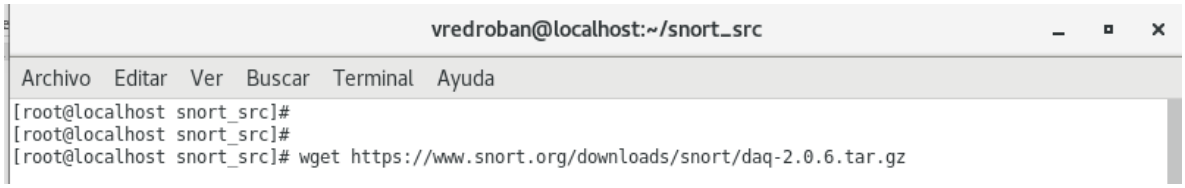


Figura 24 Descargando DAQ

Autor: Verónica Chico

Extraer los datos a instalar e ingresar en su carpeta con **$cd daq-2.0.6**

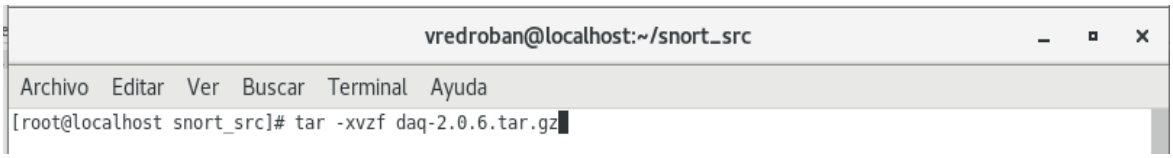


Figura 25 Descomprimiendo DAQ

Autor: Verónica Chico

A continuación ejecutar el script para la instalación



Figura 26 Instalando DAQ

Autor: Verónica Chico

Una vez instalado, re ingresar a la carpeta temporal que fue creada anteriormente

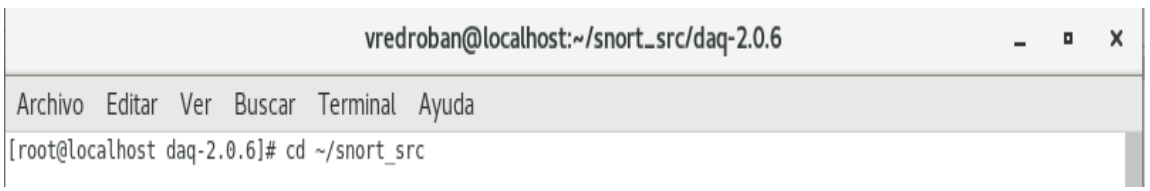


Figura 27 ingresamos a la carpeta de descarga temporal

Autor: Verónica Chico

Descargar Snort verificando en su página oficial www.snort.org la última versión

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost snort_src]# wget https://www.snort.org/downloads/snort/snort-2.9.12.tar.gz
```

Figura 28 Descargando snort

Autor: Verónica Chico

Una vez hecho esto, extraer el paquete e ingresar a su carpeta para proceder a la instalación a través de comandos como se ha venido haciendo, luego de extraer los archivos.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost snort-2.9.13]# ./configure --enable-sourcefire && make && sudo make install
```

Figura 29 Extrayendo e instalando snort

Autor: Verónica Chico

Configuración de Snort

Para obtener la configuración y sus reglas actualizadas, debe registrarse en la página oficial de Snort https://www.snort.org/

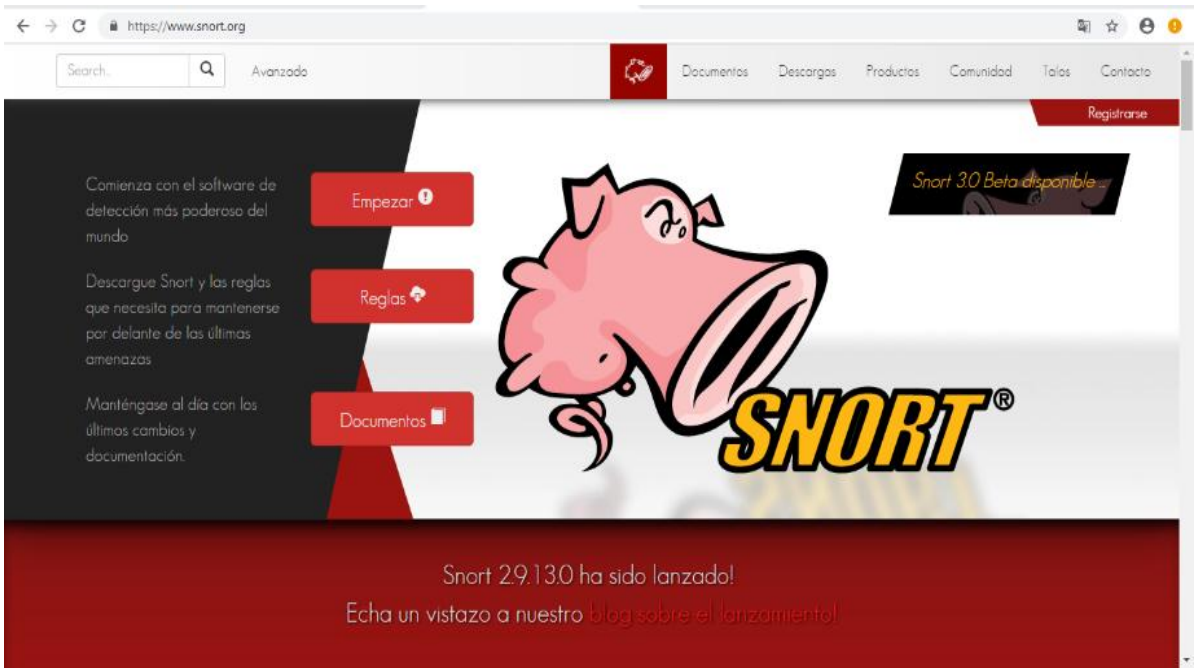


Figura 30 Página oficial de

Fuente: Snort.org

Registro como usuario



Figura 31 Registro de usuario snort

Fuente: Snort.org

Acceso a reglas actualizadas por medio de registro

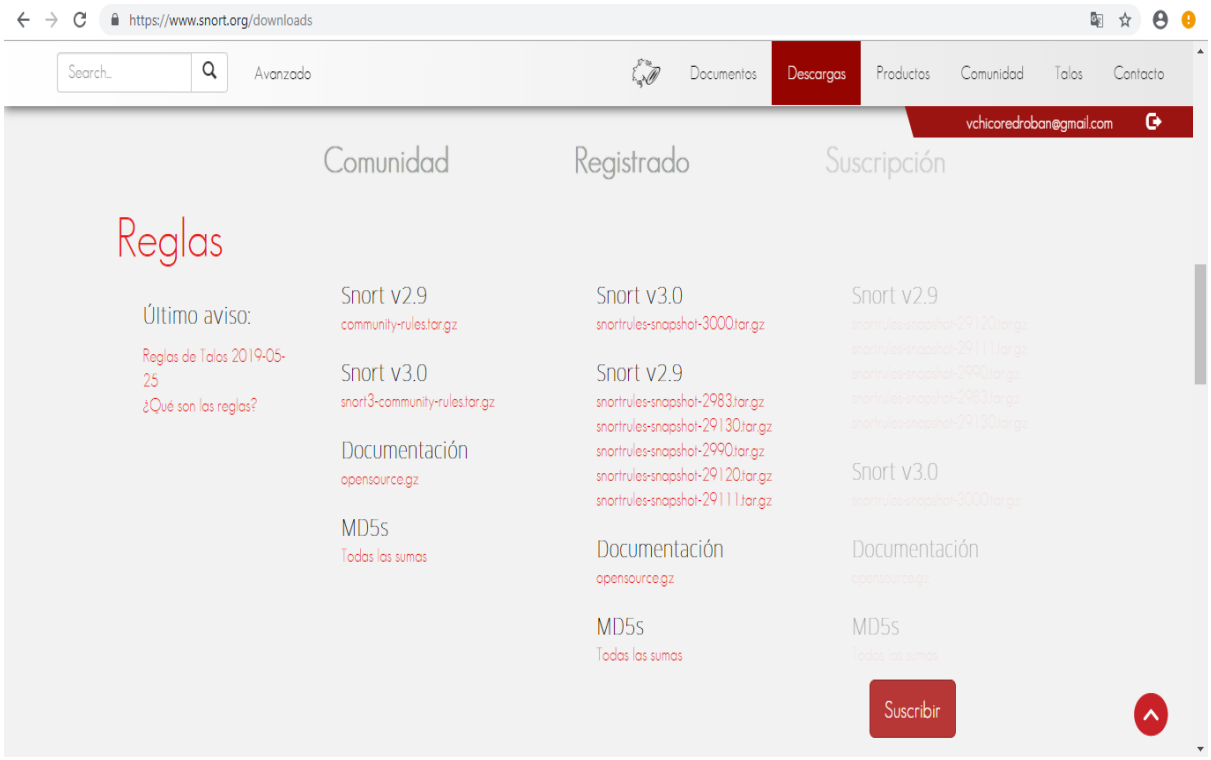


Figura 32 Reglas disponibles snort

Fuente: Snort.org

Empezar a configurar Snort como IDS además de sus reglas, actualizar bibliotecas

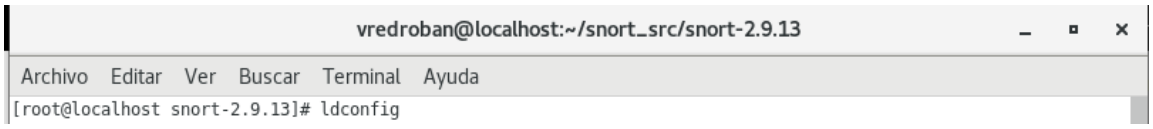


Figura 33 Actualizando bibliotecas

Autor: Verónica Chico

Configurando usuarios y carpetas

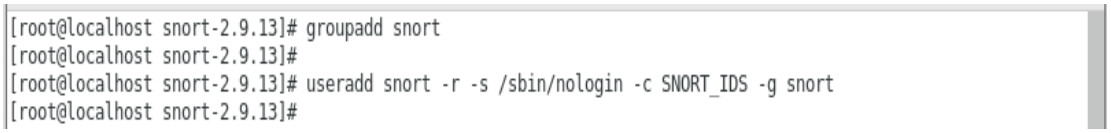


Figura 34 Configuración usuarios y carpetas

Autor: Verónica Chico

A continuación se crean carpetas que van a contener la información y configuración de Snort.

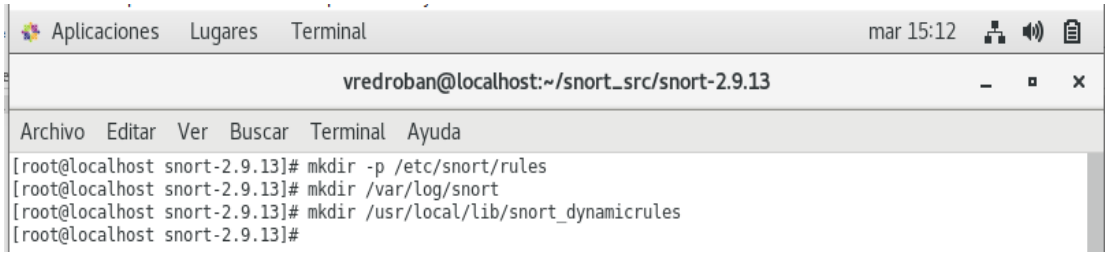


Figura 35 Creación de directorios contenedores

Autor: Verónica Chico

Establecer permisos a las carpetas creadas

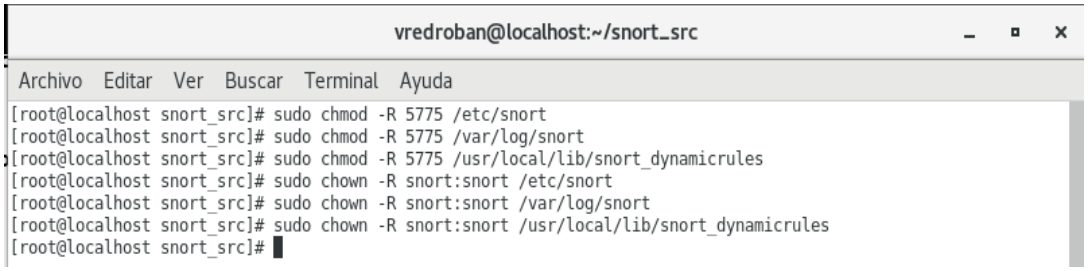


Figura 36 Estableciendo permisos

Autor: Verónica Chico

Crear archivos nuevos para las listas negras como también para las listas blancas

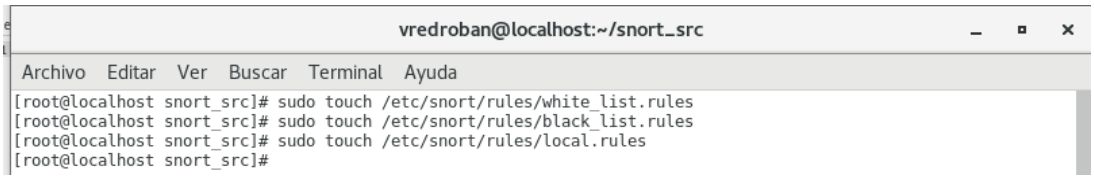


Figura 37 Creando archivos para listas

Autor: Verónica Chico

Una vez hecho esto, como anteriormente ya habiendo registrado en la página oficial de Snort se tendrá acceso a las reglas de la comunidad gratuitas (su código oink), es decir se pueden descargar las reglas que los usuarios registrados, mismas que se actualizan cada cierto tiempo, al ser Open Source, es lo que se hace, colaboraciones y el subir las suyas es parte de la colaboración con la comunidad.

Descargar reglas de Snort

Utilizando el siguiente comando reemplazar **oinckode** con tú código de usuario snort.

$wget https://www.snort.org/rules/snortrules-snapshot-29120.tar.gz?oinkcode= **oinkcode** -O ~ / registered.tar.gz

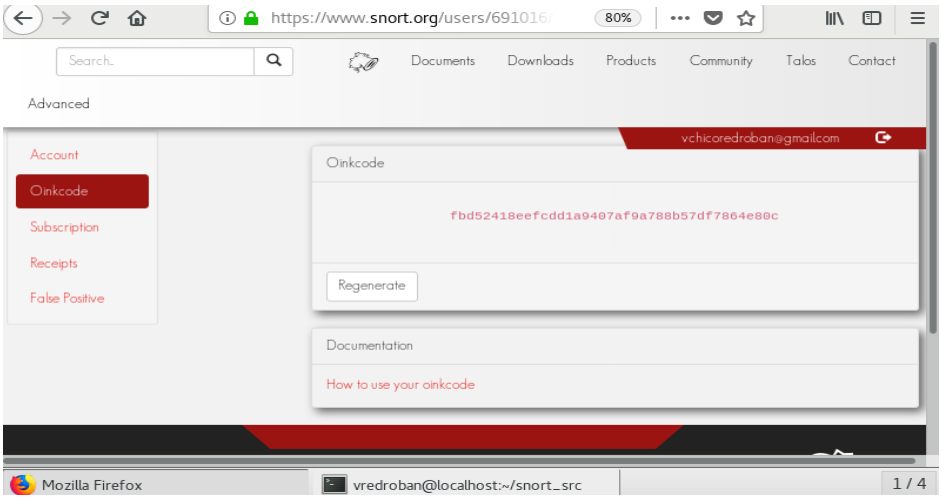


Figura 38 Oinkcode personal

Fuente: Snort.org

Ejecutar el comando anterior

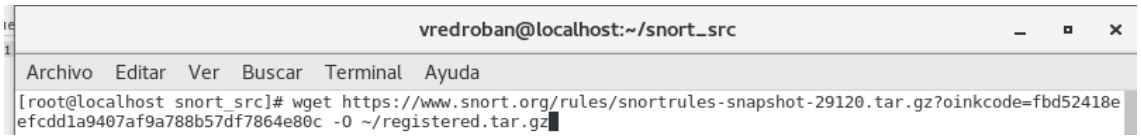


Figura 39 Comando de descarga

Autor: Verónica Chico

Las reglas se extraerán en la carpeta creada para la configuración de Snort.

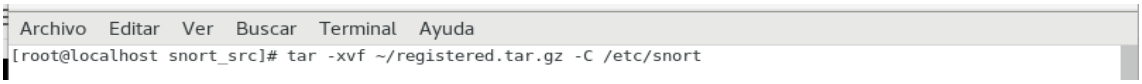


Figura 40 Copiar reglas

Autor: Verónica Chico

Configurar reglas y red

Editar el archivo snort.conf para modificar parámetros acordes a nuestras necesidades.

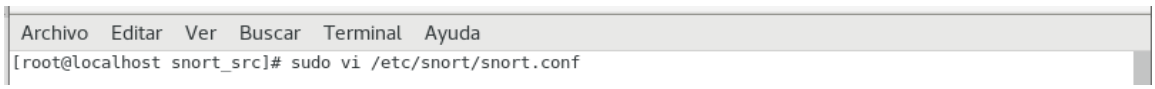


Figura 41 Editar archivo snort.conf

Autor: Verónica Chico

Cambie los siguientes parámetros para que queden de esta manera:

```
# Setup the network addresses you are protecting
ipvar HOME_NET server_public_ip/32

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any !$HOME_NET

# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

Figura 42 Editar archivo snort.conf

Autor: Verónica Chico

En el mismo archivo, en el paso 6, modificar lo siguiente.

```
##################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
##################################################

# unified2
# Recommended for most installs
output unified2: filename snort.log, limit 128
```

Figura 43 Registro de salida

Autor: Verónica Chico

Habilitar las reglas locales, es decir las descomentar y guardar los cambios.

Validando instalación

Habilitar el modo de prueba con el parámetro **-T** esto hace que se validen las reglas y variables configuradas.

```
[root@localhost snort_src]# sudo snort -T -c /etc/snort/snort.conf
```

```
vredroban@localhost:~/snort_src
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
       --== Initialization Complete ==--

  ,,_     -*> Snort! <*-
 o"  )~   Version 2.9.13 GRE (Build 15013)
  ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using libpcap version 1.5.3
          Using PCRE version: 8.32 2012-11-30
          Using ZLIB version: 1.2.7

          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
          Preprocessor Object: appid  Version 1.1  <Build 5>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>

Snort successfully validated the configuration!
Snort exiting
[root@localhost snort_src]#
How to install Snort on CentOS - U...   vredroban@localhost:~/snort_src   1 / 4
```

Figura 44 Validando instalación

Autor: Verónica Chico

Comprobar instalación de Snort

Agregamos una línea al archivo local.rules para que muestre una alerta

```
alerta icmp cualquiera cualquiera -> $ HOME_NET cualquiera (msg: "prueba ICMP"; sid:
10000001; rev: 001;)
```

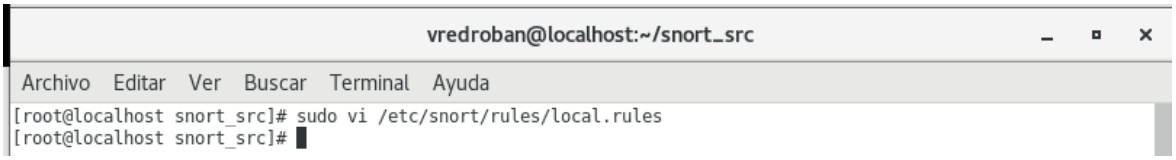


Figura 45 Editando rules

Autor: Verónica Chico

Esta regla consiste en:

- Acción para el tráfico que coincide con la regla, alerta en este caso. protocolo de tráfico como TCP, UDP o ICMP como aquí
- La dirección de origen y el puerto, simplemente marcados como cualquiera para incluir todas
- Las direcciones y puertos la dirección y el puerto de destino, $ HOME_NET como se declara en la configuración y cualquier puerto
- Algunos bits adicionales
    - mensaje de registro
    - identificador de regla único (sid) que para las reglas locales debe ser 1000001 o superior
    - Número de versión de la regla

(UpCloud & Pihlajamaa, 2018)

Crear base de datos con Mysql

Para iniciar debemos configurar la contraseña segura de Mysql con el siguiente comando

$ mysql_secure_installation

Mostrará un aviso de ingreso de contraseña para root, pero de no tenerla darle enter para configurarla, ingresar la nueva contraseña y por consiguiente aceptar (y) las siguientes peticiones que aparezcan en consola.

Mysql ayudará a guardar la información que genere Snort, y la presentación se hará al usuario final a través de la herramienta Snort report.

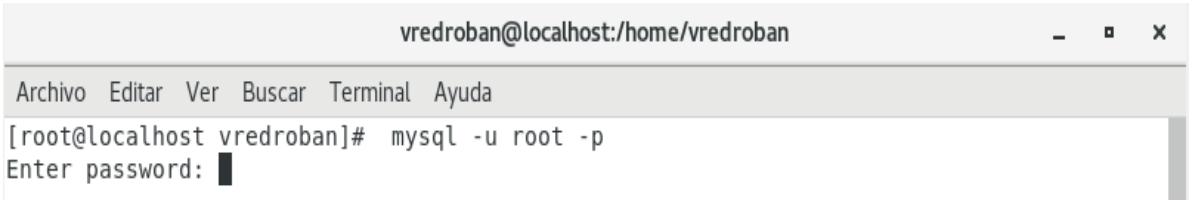


Figura 46 Accediendo a mysql

Autor: Verónica Chico

Se crea la base de datos con el nombre **Snort** mas sus privilegios ademas de sus contraseñas

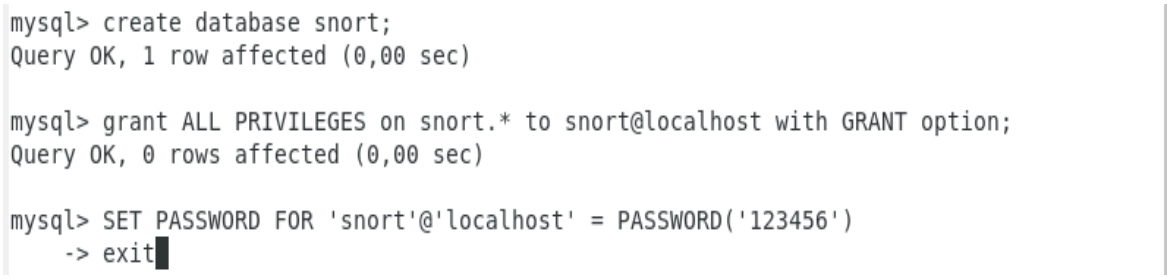


Figura 47 Creando base de datos

Autor: Verónica Chico

Instalamos Snort Report

Snort Report es una herramienta aleada a Snort para mostrar la información recogida gráficamente, página de descarga: https://symmetrixtech.com/downloads/



Figura 48 Snort Report

Fuente: www.symetrix.com

Descargar el paquete necesario, descomprimir y mover por consola

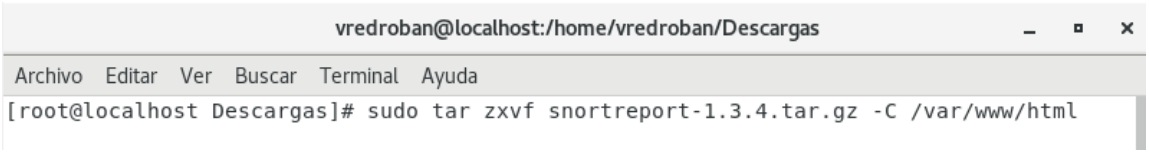


Figura 49 Descarga snort report

Autor: Verónica Chico

Editar dependencias

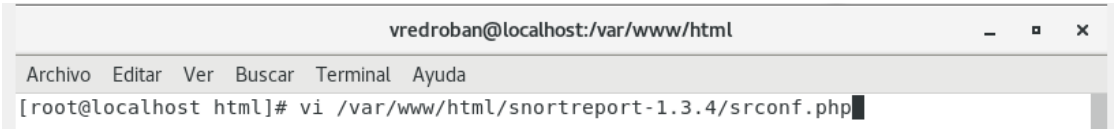


Figura 50 Configuración snort report

Autor: Verónica Chico

Configurar contraseña actual

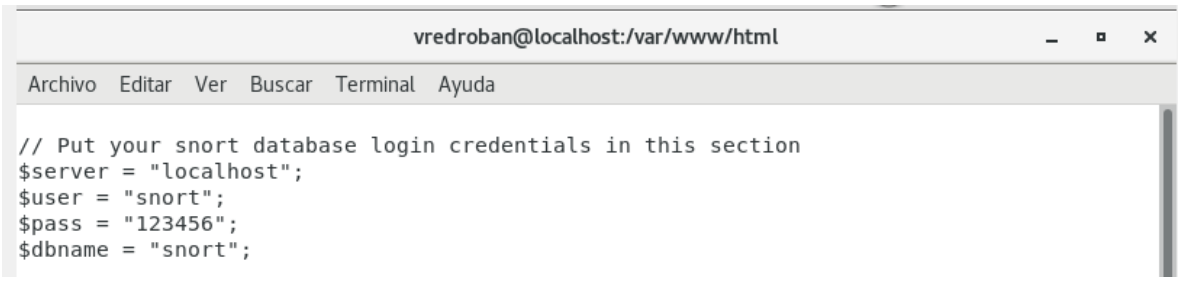


Figura 51 Configuración contraseña snort

Autor: Verónica Chico

Una vez configurado Snort Report, instalar una herramienta que nos ayuda a procesar los datos para de esta manera reducir el consumo de recursos en el proceso de paquetes.

Anteriormente, en colaboración con la reducción de consumo, se creó un archivo local en donde almacenara los datos recogidos **snort.log**, es decir le estamos diciendo que escriba las alertas con un limite de tamaño de 128 MB, de esta manera Snort creará alertas con las rapidez.

Pues bien, estos datos guardados en el archivo .log deben ser interpretados para ser escritos en la base de datos, para esto utilizaremos **Barnyard** un intérprete open source.

Instalando Barnyard

Esta herramienta la encuentra en la página oficial de Snort, la que enviara a un enlace en GitHub en donde se aloja el código, lo descargaremos y configuraremos.

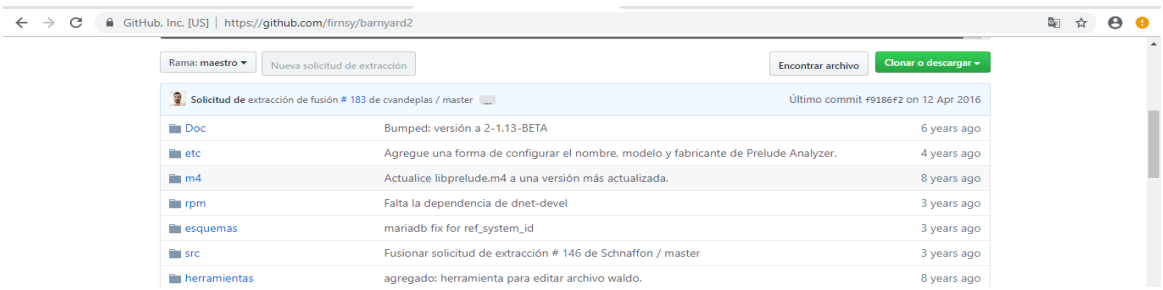


Figura 52 Configuración contraseña snort

Autor: Verónica Chico

Acceder a la carpeta de descarga e iniciar la instalación con comandos

```
cd /usr/local/src
git clone https://github.com/firnsy/barnyard2.git
cd barnyard2
./autogen.sh
make
make install
cp etc/barnyard2.conf /etc/snort
cp rpm/barnyard2 /etc/init.d
chmod 700 /etc/init.d/barnyard2
cp rpm/barnyard2.config /etc/sysconfig/barnyard2
cp /etc/init.d/barnyard2 /etc/init.d/barnyard2_default

sed -i -e '/BARNYARD_OPTS=/s/$SNORTDIR\/${INT}/$SNORTDIR/' -e '/BARNYARD_OPTS=/s/-L \$SNORT
-e '/"b.*2"/s/barnyard2/\/usr\/local\/bin\/barnyard2/'
 -e '/touch \/var/s/\$prog/barnyard2/' /etc/init.d/barnyard2

sed -i 's#$SNORTDIR/${INT}#$SNORTDIR#g' /etc/init.d/barnyard2

cp /etc/sysconfig/barnyard2 /etc/sysconfig/barnyard2_default
sed -i '/CONF=/s/barnyard.conf/barnyard2.conf/' /etc/sysconfig/barnyard2
sed -i '/LOG_FILE=/s/"snort_unified.log"/"snort.log"/' /etc/sysconfig/barnyard2
```

Figura 53 Instalando barnyard

Autor: Verónica Chico

Instalando Ossec (Modo server)

Un sistema de detección de intrusiones basado en host (HIDS), monitoriza y controla los sistemas además servicio de log centralizado, avisos y también un sistema de alertas.



Figura 54 Ossec página principal

Fuente: Ossec

Se debe descargar el paquete disponible para nuestro CentOS, cabe recalcar que Ossec posee plataformas disponibles para los Sistemas operativos Windows y Mac.

Primero se debe instalar las dependencias necesarias

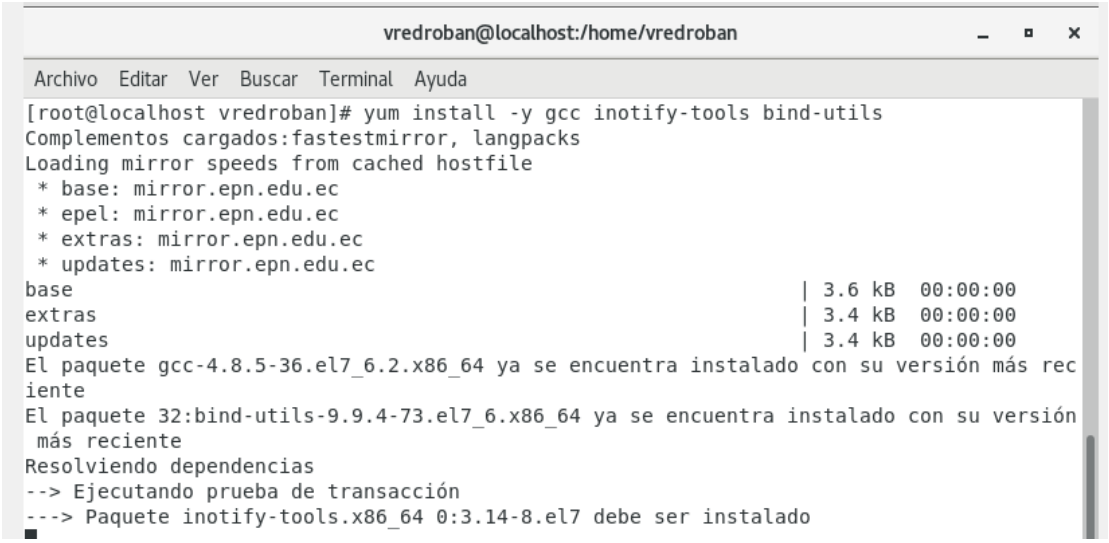


Figura 55 Instalando paquetes necesarios en ossec

Autor: Verónica Chico

Agregar los repositorios de instalación



Figura 56 Agregando repositorios en ossec

Autor: Verónica Chico

Añadir puerto al firewall que viene por defecto en CentOS

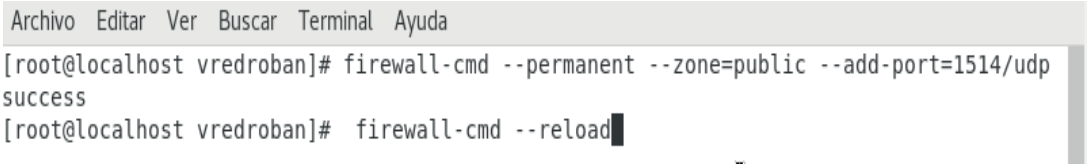


Figura 57 Agregando puertos en ossec

Autor: Verónica Chico

Iniciando la instalación en modo server

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
[root@localhost vredroban]# sudo yum install ossec-hids-server
Complementos cargados:fastestmirror, langpacks
Loading mirror speeds from cached hostfile
epel/x86_64/metalink                                     | 3.4 kB  00:00:00
 * atomic: www6.atomicorp.com
 * base: mirror.epn.edu.ec
 * epel: mirror.epn.edu.ec
 * extras: mirror.epn.edu.ec
 * updates: mirror.epn.edu.ec
atomic                                                   | 3.4 kB  00:00:00
```

Figura 58 Instalando ossec server

Autor: Verónica Chico

Configurar algunos detalles:

- Configuración en español: es
- En este caso el tipo de instalación que utilizaremos será: servidor
- Para los demás pasos que vengan por consiguiente será: **s** como aceptación

```
[root@localhost ossec-hids-3.3.0]# ./install.sh

  ** Para instalação em português, escolha [br].
  ** 要使用中文进行安装，请选择 [cn].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
  ** For installation in English, choose [en].
  ** Para instalar en Español , eliga [es].
  ** Pour une installation en français, choisissez [fr]
  ** A Magyar nyelvű telepítéshez válassza [hu].
  ** Per l'installazione in Italiano, scegli [it].
  ** 日本語でインストールします．選択して下さい．[jp].
  ** Voor installatie in het Nederlands, kies [nl].
  ** Aby instalować w języku Polskim, wybierz [pl].
  ** Для инструкций по установке на русском ,введите [ru].
  ** Za instalaciju na srpskom, izaberi [sr].
  ** Türkçe kurulum için seçin [tr].
  (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: es


 OSSEC HIDS v3.3.0 Guión de instalación - http://www.ossec.net
```

Figura 59 Configuración ossec

Autor: Verónica Chico

Habilitar las listas blancas añadiendo IPs de confianza y tambien confirmando las preguntas siguientes.

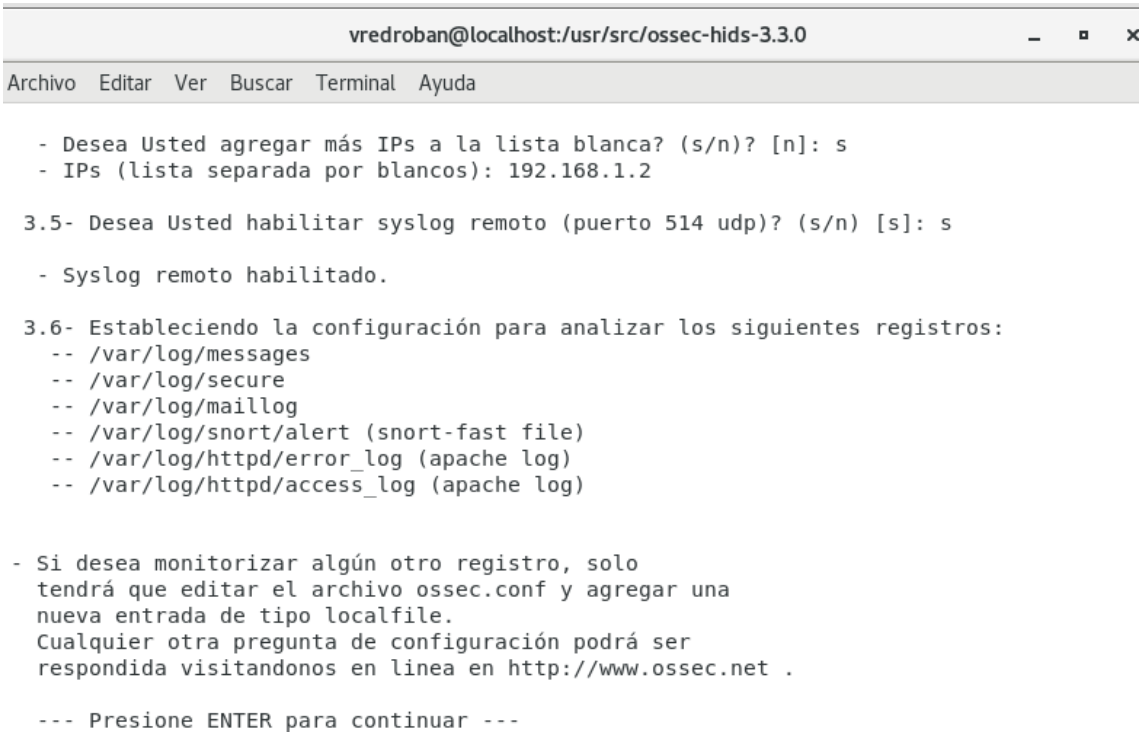


Figura 60 Configuración ossec

Autor: Verónica Chico

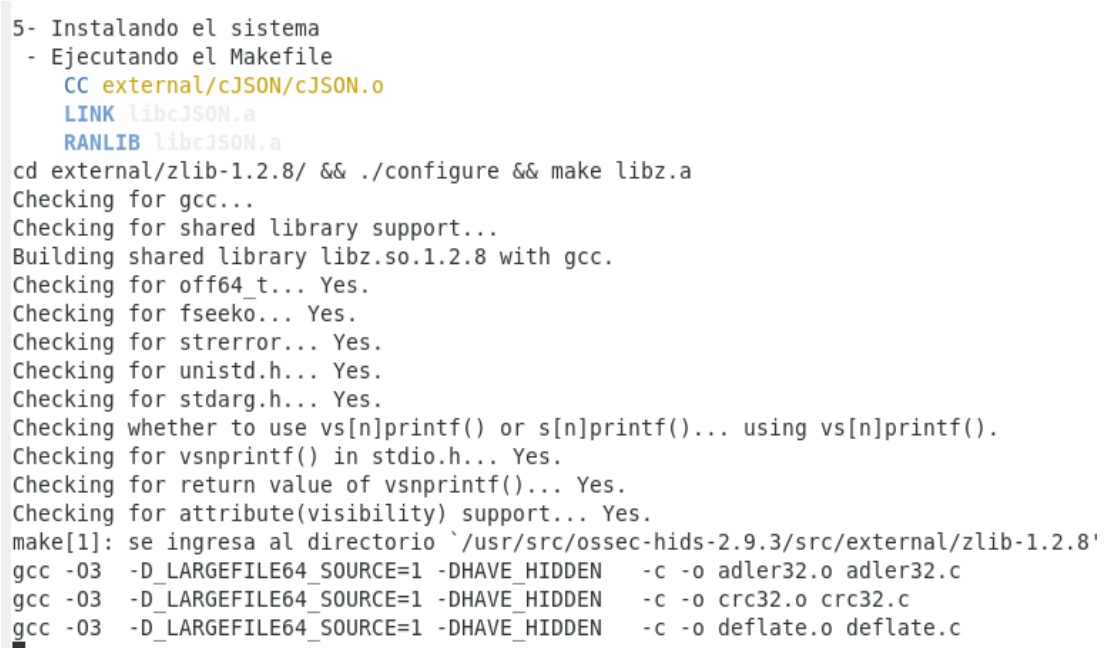


Figura 61 Configuración ossec

Autor: Verónica Chico

Al finalizar la configuración nos muestra lo que en adelante debemos configurar:

```
- El sistema es Redhat Linux.
- Init script modificado para empezar OSSEC HIDS durante el arranque.

- Configuración finalizada correctamente.

- Para comenzar OSSEC HIDS:
     /var/ossec/bin/ossec-control start

- Para detener OSSEC HIDS:
     /var/ossec/bin/ossec-control stop

- La configuración puede ser leída ó mofificada en /var/ossec/etc/ossec.conf
```

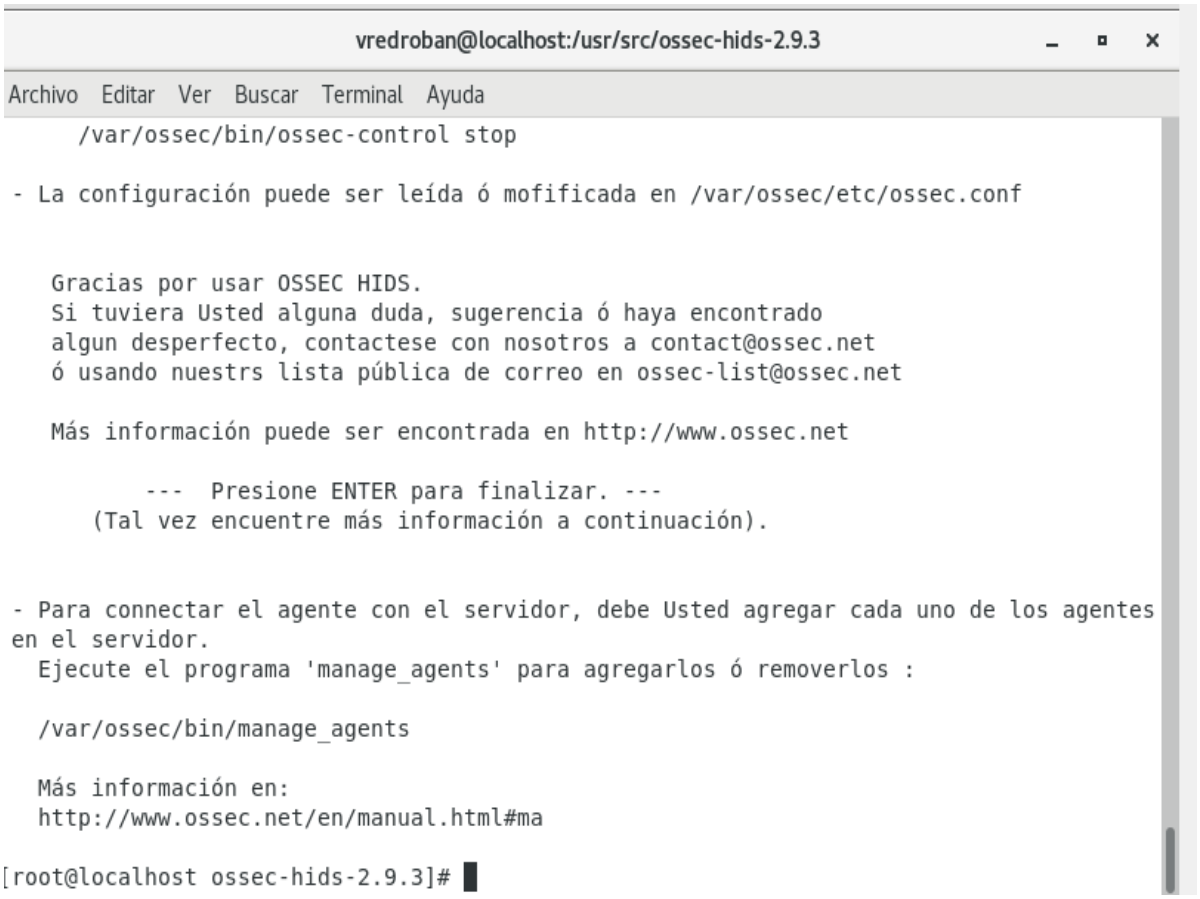


Figura 62 Configuración ossec

Autor: Verónica Chico

Tenemos que editar el archivo /var/ossec/etc/ossec.conf para añadir las reglas y las reacciones de los comandos que vamos a ejecutar, de la misma manera habilitamos las conexiones hechas dese la subred 192.168.1.0/24 por el puerto 1514 UDP finalizando en nuestra IP (*.*.*.*).

Aquí mismo denegar el acceso a ciertos archivos tanto de agente como de cliente para evitar el daño por parte de los intrusos que accedan al tarro de miel.

```
<command>
    <name>win_nullroute</name>
         <executable>route-null.cmd</executable>
         <expect>srcip</expect>
         <timeout_allowed>yes</timeout_allowed>
    <name>host-deny</name>
         <executable>host-deny.sh</executable>
         <expect>srcip</expect>
         <timeout_allowed>yes</timeout_allowed>
 </command>
```

Figura 63 Configurando ossec.conf

Autor: Verónica Chico

```
vredroban@localhost:/home/vredroban
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
 GNU nano 2.3.1          Fichero: /var/ossec/etc/ossec.conf

<!-- Active Response Config -->
<active-response>
  <!-- This response is going to execute the host-deny
     - command for every event that fires a rule with
     - level (severity) >= 6.
     - The IP is going to be blocked for  600 seconds.
    -->


<command>win_nullroute</command>
  <location>local</location>
  <level>6</level>
  <timeout>600</timeout>

<command>host-deny</command>
  <location>local</location>
  <level>6</level>
  <timeout>600</timeout>
</active-response>
```

Figura 64 Configurando ossec.conf

Autor: Verónica Chico

```
<remote>
  <connection>secure</connection>
  <port>1514</port>
  <allowed-ips>192.168.1.0/24</expect>
  <local-ip>192.168.1.10</local-ip>
</remote>
```

Figura 65 Definiendo conexión remota en ossec.conf

Autor: Verónica Chico

Ahora les daremos acceso desde iptables

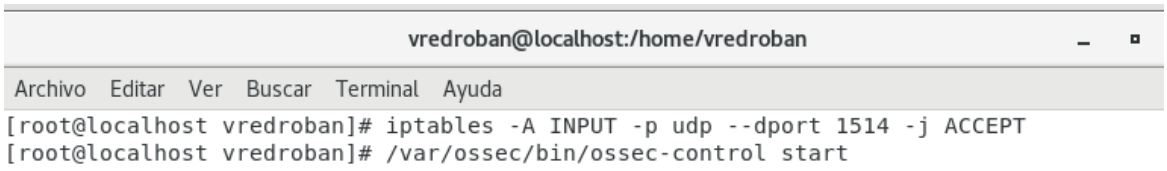


Figura 66 Habilitando iptables y reiniciando servicios en ossec

Autor: Verónica Chico

Honeypot creada en CentOS trabajando

Para la demostración generamos un ping de la maquina física, la cual se encuentra en la misma red para demostrar parte del funcionamiento, en donde snort se encuentra mostrando el trafico ICMP (Protocolo de mensajes de control de internet).

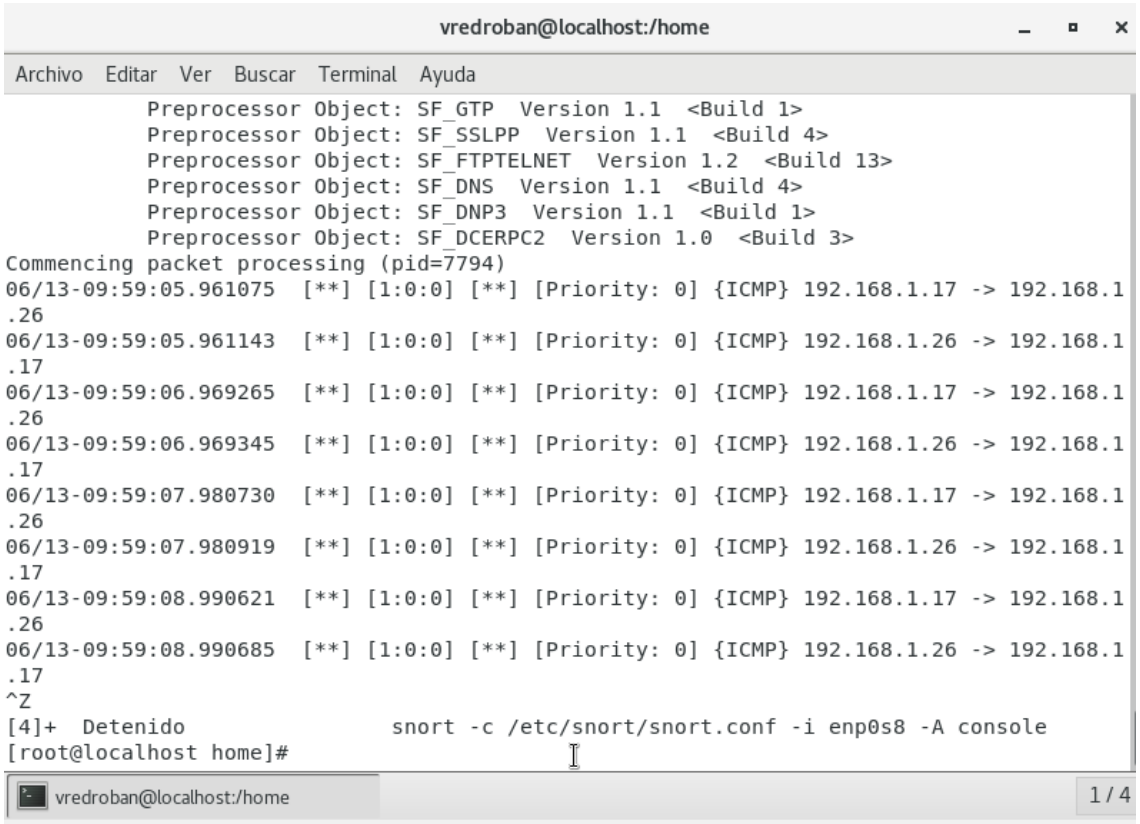


Figura 67Demostracion Honeynet trabajando

Autor: Verónica Chico

Instalando y configurando HoneyDrive

HoneyDrive es un CdRom (.ova) de distribución Linux con un sistema operativo Xubuntu de 32 bits que viene ya preinstalado con varias herramientas de monitoreo de redes y tráfico de la misma, es decir, un HoneyPot listo para ser configurado en base a nuestras necesidades y que lo podemos conseguir en su página principal (Koniaris, 2019) que detallaré a continuación algunas de ellas:

```
MySQL root password:    honeydrive

[Kippo]
Location:               /honeydrive/kippo/
Start script:           /honeydrive/kippo/start.sh
Stop script:            /honeydrive/kippo/stop.sh
Downloads:              /honeydrive/kippo/dl/
TTY logs:               /honeydrive/kippo/log/tty/
Credentials:            /honeydrive/kippo/data/userdb.txt
MySQL database:         kippo
MySQL user/password:    root/honeydrive

[Kippo-Graph]
Location:               /var/www/kippo-graph/
Configuration:          /var/www/kippo-graph/config.php
URL:                    http://local-or-remote-address/kippo-graph/
MySQL database:         kippo
MySQL user/password:    root/honeydrive

[Kippo-Malware]
Location:               /honeydrive/kippo-malware/

[Kippo2MySQL]
Location:               /honeydrive/kippo2mysql/
MySQL database:         kippo2mysql
MySQL user/password:    root/honeydrive
```

```
[Specs]
OS:                     Xubuntu Desktop 12.04.4 LTS i386
HDD:                    80GB VMDK (dynamically allocated)
Localization:           English (United States)
Keyboard layout:        English (United States)
Timezone:               UTC (Coordinated Universal Time)

[System]
Connectivity:           DHCP
Hostname:               honeydrive
User:                   HoneyDrive
Username/password:      honeydrive/honeydrive
Sudo password:          honeydrive
Log in automatically:   enabled

[Virtualization]
VBox Guest additions:   installed
Shared Clipboard:       bidirectional
Drag'n'Drop:            disabled

[LAMP]
Apache 2 support:       PHP, Perl, Python, Ruby/Rails
Document root:          /var/www/
Apache 2 changes:       AllowOverride All (/var/www/), ServerTokens Minimal, ServerSignature Off
Apache php.ini changes: max_execution_time = 300
                        max_input_time = 180
                        memory_limit = 256M
                        post_max_size = 256M
                        upload_max_filesize = 256M
                        max_file_uploads = 40
```

```
[Kippo2MySQL]
Location:               /honeydrive/kippo2mysql/
MySQL database:         kippo2mysql
MySQL user/password:    root/honeydrive

[Kippo2ElasticSearch]
Location:               /honeydrive/kippo2elasticsearch/
MySQL database:         kippo
MySQL user/password:    root/honeydrive
ElasticSearch index:    kippo
ElasticSearch type:     auth
Kibana dashboard:       http://localhost/kibana/#/dashboard/elasticsearch/Kippo2ElasticSearch

[Kippo-Scripts]
Location:               /honeydrive/kippo-scripts/
Scripts:                + kippo-sessions
                        + kippo-stats
                        + kippo2wordlist
```

Figura 68 Configuración de HoneyDrive

Autor: Verónica Chico

Como anteriormente se ha visto, en el archivo readme.txt que viene por defecto en el sistema preinstalado, se tienen cada una de las rutas, los scripts necesarios y las configuraciones para poner a andar el honeypot, para lo que en primera instancia se debe restaurar en virtualbox, en una máquina virtual nueva.

Las principales herramientas que utilizaremos serán:

Kippo

Un honeypot de baja interacción pero de un potente motor de rastreo por lo que es uno de los más utilizados, su modo de trabajo es simular un servicio SSH, detectar los ataques de fuerza bruta como también las intrusiones.

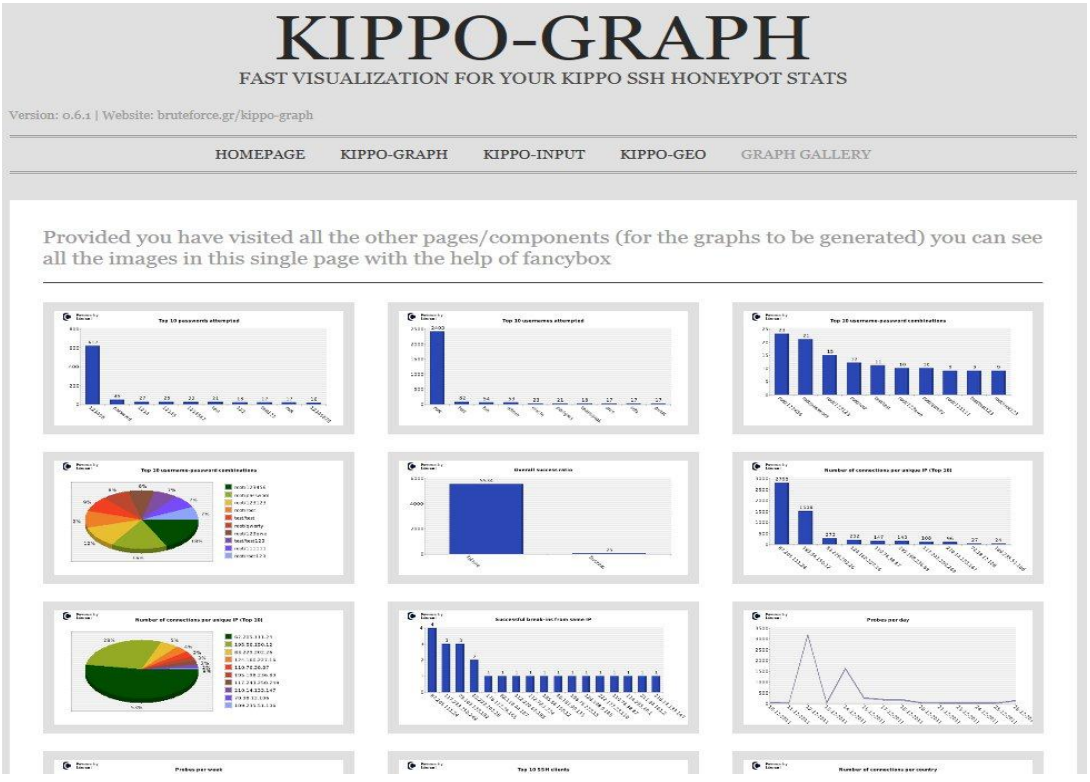


Figura 69 Kippo trabajando

Fuente: Kippo

Lo que muestra actualmente es el tráfico de internet, es decir al acceder a paginas cuando nos retornan spam o algún otro tipo de amenazas.

Dionaea

También considerado un honeypot de baja interacción pero que posee varios servicios, como la detección y análisis de malware, entre otros servicios. Cuenta con una interfaz amigable en donde reporta cada uno del movimiento en modo gráfico y estadístico.

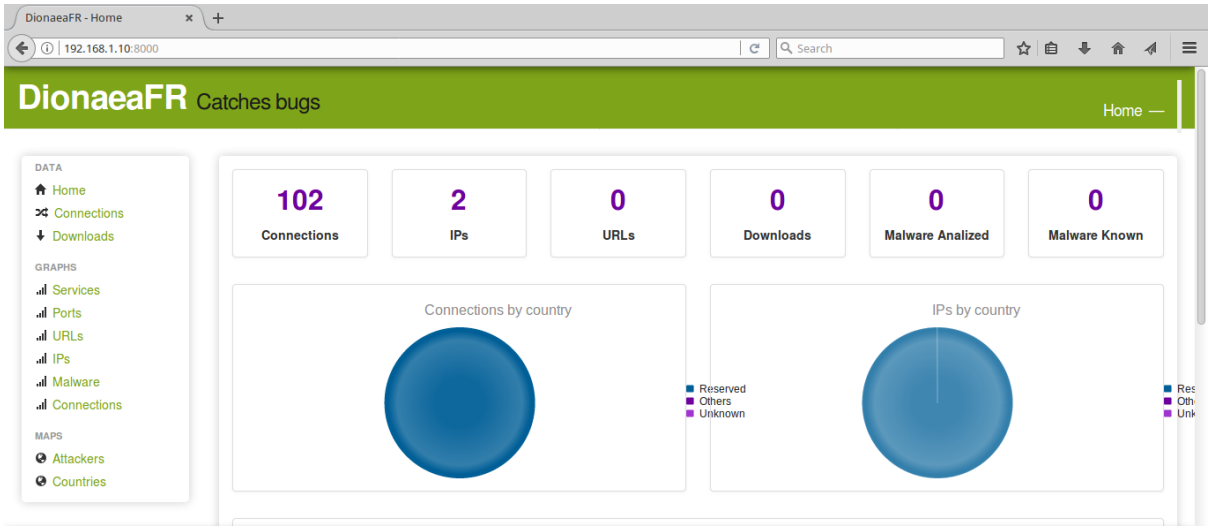


Figura 70 Entorno virtual de Dionaea

Autor: Dionaea

Mostrando componentes trabajando

Ahora se pueden ver varios intentos de inicio de sesión fallidos captados por Ossec, ubicando su nivel, en este caso nos mostrara la máquina que fue atacada, la fecha y la hora como también su dirección ip.

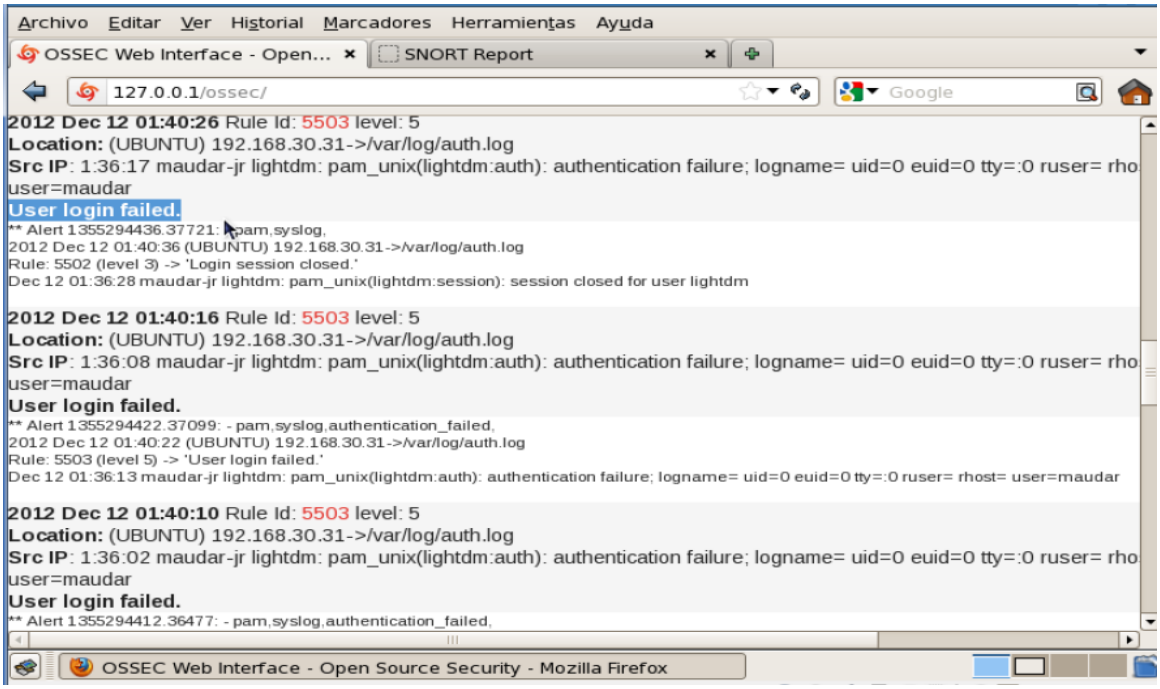


Figura 71 Ossec trabajando

Autor: Verónica Chico

Niveles de Alerta en Ossec

Nivel 0: Ignorado, no se tomaron medidas. Se utiliza principalmente para evitar falsos positivos. Estas reglas se analizan antes de todos los demás y son eventos sin importancia para la seguridad.

Nivel 2: Sistema de notificación de baja prioridad. Sistema de notificación de mensajes de estado o que no tienen ninguna importancia para la seguridad.

Nivel 3: El éxito / eventos autorizados. Intentos exitosos de acceso, permitido en el firewall, etc

Nivel 4: Sistema de errores de baja prioridad. Los errores relacionados con malas configuraciones o dispositivos no utilizados / aplicaciones. No tienen importancia para la seguridad y generalmente son causados??por las Instalaciones por defecto o pruebas de software.

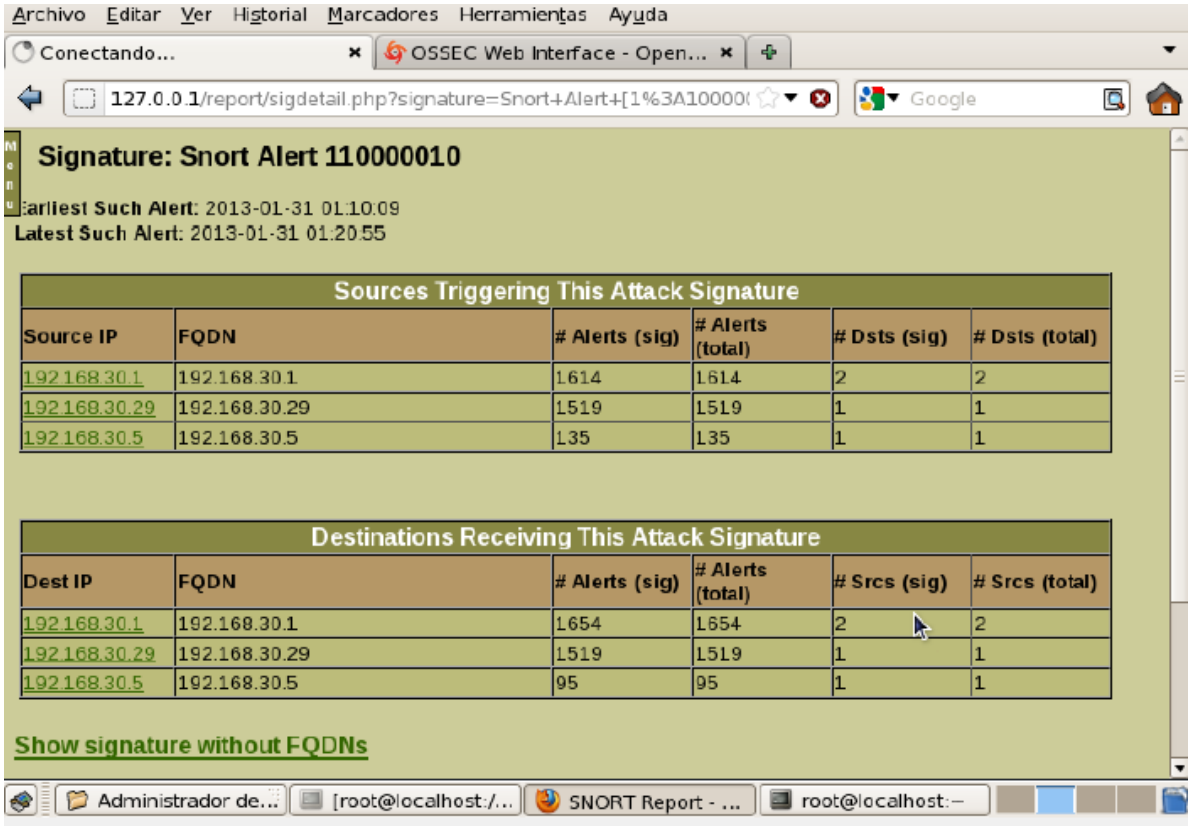
Nivel 5: El usuario los errores generados por contraseñas perdidas, las acciones denegado, etc. Estos mensajes no tienen de seguridad pertinentes.

Nivel 6: Ataques de baja relevancia. Indican un gusano o un virus que no ofrecen ninguna amenaza para el sistema, tales como un gusano de Windows atacar a un servidor Linux. También se incluyen con frecuencia provocado IDS eventos y sucesos comunes de error.

Nivel 9: Error de la fuente no válida. Incluyen los intentos de inicio de sesión como un usuario desconocido o de una fuente no valida. El mensaje podría tener importancia para la seguridad, especialmente si se repite. También se incluyen los errores en relación con el administrador o root.

Snort Trabajando

Lo que se muestra actualmente es un ataque DDOS, donde se observa 1614 alertas de un equipo que se encuentra dentro de la misma honeynet.


Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Conectando...
OSSEC Web Interface - Open...
127.0.0.1/report/sigdetail.php?signature=Snort+Alert+[1%3A10000(
Google
Menu
Signature: Snort Alert 110000010
Earliest Such Alert: 2013-01-31 01:10:09
Latest Such Alert: 2013-01-31 01:20:55
Sources Triggering This Attack Signature
Source IP | FQDN | # Alerts (sig) | # Alerts (total) | # Dsts (sig) | # Dsts (total)
192.168.30.1 | 192.168.30.1 | 1614 | 1614 | 2 | 2
192.168.30.29 | 192.168.30.29 | 1519 | 1519 | 1 | 1
192.168.30.5 | 192.168.30.5 | 135 | 135 | 1 | 1
Destinations Receiving This Attack Signature
Dest IP | FQDN | # Alerts (sig) | # Alerts (total) | # Srcs (sig) | # Srcs (total)
192.168.30.1 | 192.168.30.1 | 1654 | 1654 | 2 | 2
192.168.30.29 | 192.168.30.29 | 1519 | 1519 | 1 | 1
192.168.30.5 | 192.168.30.5 | 95 | 95 | 1 | 1
Show signature without FQDNs
Administrador de...
[root@localhost:/...
SNORT Report - ...
root@localhost:~

BIBLIOGRAFÍA

Ley de Comercio Electrónico, F. E.-6. (s.f.). : Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos del Ecuador (Ley No. 2002-67). Ecuador.

Anderson Co., J. (1980). Computer Security Threat Monitoring and Surveillance.

Bonilla, & Rodriguez. (2019). Obtenido de Metodológía de la investigación: https://books.google.com.ec/books?id=h4X_eFai59oC&lpg=PA57&dq=metodo%20cualitativo&pg=PA57#v=onepage&q=metodo%20cualitativo&f=false

Gfos seguridad. (2015). Information security. Obtenido de Breve historia de un servidor señuelo: interpretación y análisis de bitácoras.: https://gf0s.files.wordpress.com/2015/09/historia-de-un-servidor-sec3b1uelo-en-internet1.pdf

Gobierno de la República del Ecuador. (2011). Agencia de Regulación y Control Hidrocarburífero. Obtenido de Agencia de Regulación y Control Hidrocarburífero: https://www.controlhidrocarburos.gob.ec/wp-content/uploads/MARCO-LEGAL-2016/Registro-Oficial-322-Decreto-Ejecutivo-1014.pdf

Honeynet Project. (25 de julio de 2003). Honeynet Project. Obtenido de Honeynet Project: http://his.sourceforge.net/honeynet/papers/honeynet/

Icecat. (mayo de 2019). ICECAT. Obtenido de ICECAT: https://icecat.biz/es/p/fortinet/fg-2000e-bdl-usg-900-60/hardware+firewalls-fortigate+2000e-35747177.html

Jurado, D. (2016). FWHIBBIT. Obtenido de https://www.fwhibbit.es/introduccion-a-los-sistemas-senuelo-honeypots

Koniaris, I. (2019). BruteForce Lab. Obtenido de BruteForce Lab: https://bruteforcelab.com/honeydrive

MAÑAS, J. AMUTIO;. (2012). Centro Criptológico Nacional. Obtenido de Centro Criptológico Nacional: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

MUÑOZ ESTRADA, B. F. (2019). Vulnerabilidades de seguridad en el Sistema Académico Integrado en Red (Si@net) de la Universidad Estatal de Bolívar, año 2018. Guaranda.

Olifer, N. , & Olifer, V. (2009). Redes de Computadoras. México: Litográfica Ingramex.

Panda Security. (s.f.). Panda Security Mediacenter. Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/que-es-un-firewall/

Rapid7, & Common Types of Cybersecurity Attacks. (2019). Rapid7. Obtenido de Common Types of Cybersecurity Attacks: https://www.rapid7.com/fundamentals/types-of-attacks/

Red Hat, I. (2019). MIT, Red Hat Enterprise Linux 3: Manual de seguridad. Obtenido de http://web.mit.edu/rhel-doc/3/rhel-sg-es-3/ch-server.html

Roesch, M. (02 de mayo de 2019). Snort. Obtenido de Snort: https://www.snort.org/

SEGURIDAD, R. (2019). SEGURITECNIA, Revista Decana Independiente de Seguridad. Obtenido de http://www.redseguridad.com/especialidades-tic/virtualizacion/seguridad-en-servidores-web-la-importancia-de-tener-un-sistema-seguro

Software ISO Riesgos y Seguridad. (2018). Software ISO Riesgos y Seguridad. Obtenido de Software ISO Riesgos y Seguridad: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Solís Solís, L. A., & Jijón Ramos, M. D. (2013). Implantación de una Honeynet para la optimización de la seguridad de la información en los servidores de la Universidad Técnica de Ambato. Ambato.

TECHTARGET. (2019). TechTarget. Obtenido de https://searchdatacenter.techtarget.com/es/definicion/Servidor-Web

The Honeynet Project. (2019). The Honeynet Project. Obtenido de The Honeynet Project: https://www.honeynet.org/project

TUTORIALES EN LINEA. (MAYO de 2019). TUTORIALES EN LINEA. Obtenido de TUTORIALES EN LINEA: https://tutorialesenlinea.es/455-los-ataques-mas-comunes-que-afectan-a-los-sitios-web-y-servidores.html#sel=29:1,30:87

UpCloud, & Pihlajamaa, J. (2018). UpCloud. Obtenido de UpCloud: https://upcloud.com/community/tutorials/installing-snort-on-centos/

ANEXOS

Anexo 1. Entrevista

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

ESCUELA DE SISTEMAS

UNIDAD DE TITULACIÓN

FICHA DE ENTREVISTA

Administrador de Redes

Entrevistador: Verónica Chico Redrobán

Lugar y Fecha: 16/04/2019

1. **¿Qué Sistema operativo utiliza actualmente para los servidores?**

   CentOS en la actualidad

2. **¿Con cuántos servidores tanto físicos como virtualizados cuentan y enumere los aplicativos funcionando en cada uno de ellos?**

   Fisicamente cuentan con 10 servidores físicos y ninguno virtualizado:

   a) Asociación de profesores d) Ciencias de la educación

   b) Dspace (Repositorio de trabajos de grado) e) EVA Mail institucional (no func).

   c) Koha (Biblioteca) f) Bolsa de empleo g) Depto. financiero h) SIANET i) pag. web

3. **¿A qué generación pertenecen cada uno de los servidores?**

   No se puede definir a ciencia cierta a que generación pertenecen cada uno de ellos ya que fueron adquiridos de a poco y se mantenia una administración diferente por lo que se presume que al menos podrian tener 8 años cada uno.

4. **¿Qué tipo de accesos remotos utilizan para los servidores fuera de la intranet de la institución?**

   Existe una configuración básica en general, pero en algunos de los casos como es el del SIANET, es el administrador quien se encarga de esa información

5. **¿Se encuentra dividida la capa de datos de la capa de servicios?**

   No se ha definido una división de las zonas de trabajo lógico dentro de los servicios de la red de servidores web

6. **¿Cuentan actualmente con un firewall?**

   Enuncie sus características

   Si, se adquirió un firewal marca Fortinet FortiGate modelo 2000E. en el año 2008 el cual posee las siguientes características:
   Salidade firewall: 40 000 Mbit/s, Rendimiento VPN: 65000 Mbit/s, IPS/IDS: 25000 Mbits. Disipación de calor: 1467 BTU/h, Nivel de Ruido: 58 dB, Número de usuarios: 10000 usr.

7. **¿Cuáles son las configuraciones de seguridad se están aplicando a dicho firewall?**

   Mantiene la configuración básica, es decir, no se están utilizando todos los beneficios que brinda el mismo con la actualización del firmware (6.0) al 12 de junio del 2018 por parte de la empresa externa SOLINFRA CIA LTDA, el cual mostró que está trabajando en el rango de temperatura normal y el uso del procesador de hasta el 7% de capacidad, funcionando de manera óptima.

8. **¿Qué tipo de seguridad se utiliza actualmente para salvaguardar la información contenida en dichos equipos?**

   Se guarda una gran confiabilidad en salvaguardar la información y por medio de esta la seguridad de la misma el hecho de poseer un firewall, el cual fue configurado no hace mas de un año ademas de la creación de backups.

9. **¿Qué reglas de autenticación aplican para el acceso a servidores?**

   A pesar de estar a cargo de un administrador, en algunos de los casos son los mismos encargados de los sistemas que funcionan dentro de los servidores quienes manejan la autenticación.

10. **¿Existe un informe detallado sobre las vulnerabilidades o ataques informáticos que han recibido los servidores?**

    Si, No. Explique.

    No existe, ponca se ha hecho un análisis forense de ciertas anomalías en los servidores unicamente se ha tratado de corregir en cuanto a código.

11. **¿Poseen actualmente un sistema señuelo? De ser afirmativa su respuesta explique cuál es.**

    No existe pero se tiene un ligero conocimiento sobre el mismo

12. **¿Cuáles son las reglas ACL (Listas de Control de Acceso) configuradas en el servidor de la plataforma SIANET?**

No existen listas de control de acceso ni en routers ni en firewall.

13. **¿Qué método de recuperación de datos poseen en el caso de sufrir algún tipo de caída de servidores?**

Backups, creación de los mismos.

14. **¿Poseen Listas de Control de Acceso?**

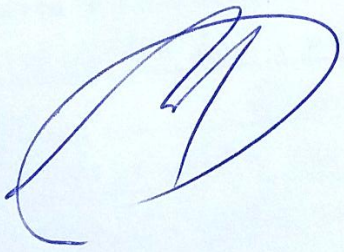
No

15. **¿Poseen políticas de seguridad?**

No

16. **¿Poseen un IDS?**

No



Anexo 2. Ficha de observación

UNIVERSIDAD ESTATAL DE BOLÍVAR

FACULTAD DE CIENCIAS ADMINISTRATIVAS, GESTIÓN EMPRESARIAL E INFORMÁTICA

ESCUELA DE SISTEMAS

UNIDAD DE TITULACIÓN

FICHA DE OBSERVACIÓN

Observador: Verónica Chico Redrobán

Fecha: 16 de abril del 2019

Lugar: Unidad de Redes

Criterio	Observación
Estructura de red para ubicación estratégica de la herramienta	Una estructuración de la red a nivel universitario es de gran importancia en este proyecto debido a que en base a ella se decide la ubicación estratégica de la herramienta Honeybot para su funcionamiento, lo que lastimosamente no se encontró documentación del crecimiento de la red, solo planos antiguos.
Políticas de Seguridad	Actualmente no se han implementado dichas políticas; son el protocolo normas y reglas que dicen cuál es el modo de manejar la información para de esta manera evitar la integridad de la información.
IDS, DMZ, ACLs y VLANs	IDS: Sistema IDS no funcionando en firewall. DMZ: No existe zona desmilitarizada ACLs: Listas de control de Acceso : No VLANs: Redes de área local y virtual, permiten dividir servicios. No hay documentación

Anexo 3. Certificado Urkundg

CERTIFICADO ANTIPLAGIO

Yo, Del Pozo Durango Rodrigo Humberto, Director del Proyecto de Investigación, certifica que la señorita **VERÓNICA ESTEFANÍA CHICO REDROBÁN** con cédula 1804637567, estudiante de la Carrera de Sistemas, Facultad de Ciencias Administrativas, Gestión Empresarial e Informática de la Universidad Estatal de Bolívar dentro de la modalidad de titulación. Proyecto de investigación, ha cumplido con la revisión a través de la herramienta URKUND, el día 11 de julio del 2019 del informe final del proyecto denominado "**SISTEMA DE SEGURIDAD DE SERVIDORES WEB MEDIANTE EL USO DE UNA HERRAMIENTA SEÑUELO APLICADO A LA PLATAFORMA SIANET DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR, AÑO 2019**", dando como resultado el 4% de coincidencia, porcentaje que se encuentra dentro del parámetro legal establecido.

Es todo cuanto puedo certificar,

Ing. Rodrigo del Pozo

C.I. 0200856557

Anexo 4. Informe Solinfra Firewall

SOLINFRA

INFORME

MANTENIMIENTO PREVENTIVO

U.E.B
Universidad Estatal de Bolivar

Versión 1.0

www.solinfra.com

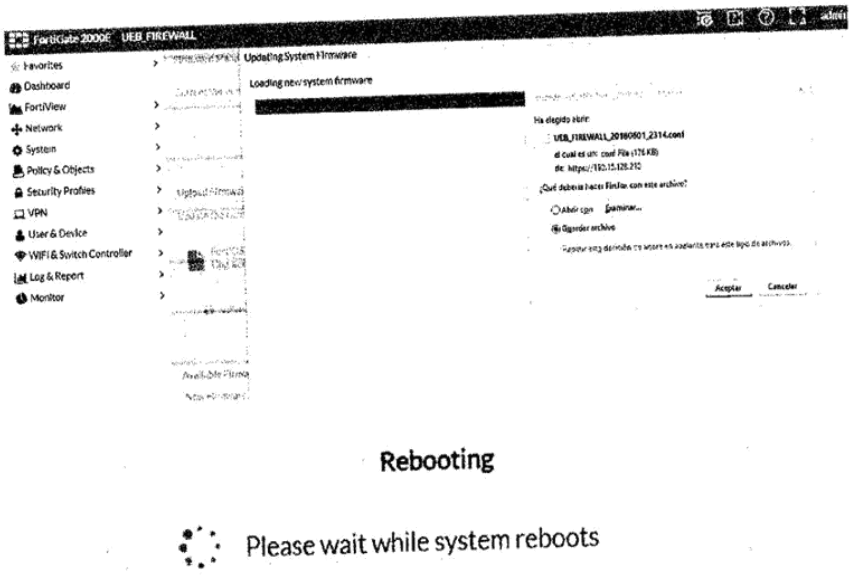


Figura 3. *Backup, actualización y reinicio de equipo.*

Una vez realizada la actualización el firewall de la Universidad Estatal de Bolívar cuenta con la última versión de firmware recomendada por el fabricante (*Figura 4*).

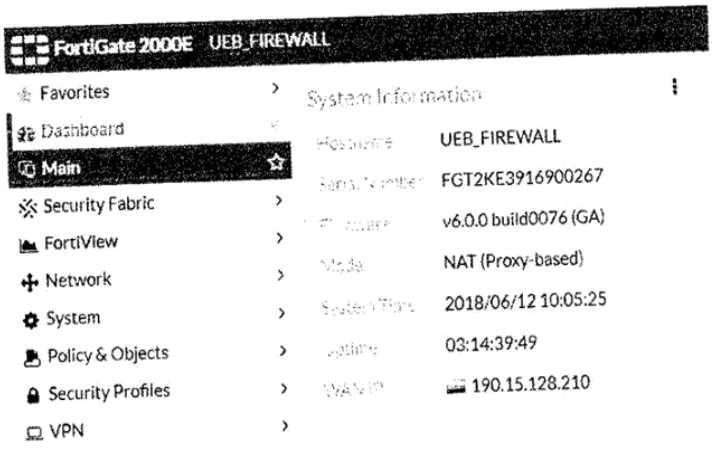


Figura 4. *Firmware actual (6.0)*

4.- MONITOREO

Los resultados obtenidos muestran que el switch de core está trabajando en el rango de temperatura normal y el uso del procesador de hasta el 7% de su capacidad.

```
[UEB_SW_CORE]display environment
 System temperature information (degree centigrade):
 ------------------------------------------------------------------------
 Slot  Sensor     Temperature  Lower  Warning  Alarm  Shutdown
 1     hotspot 1  45           0      61       66     NA
 1     hotspot 2  42           0      58       63     NA
 2     hotspot 1  44           0      65       70     NA
 2     hotspot 2  37           0      65       70     NA
 2     hotspot 3  34           0      67       72     NA
[UEB_SW_CORE]
```

```
[UEB_SW_CORE]display cpu-usage
Slot 1 CPU 0 CPU usage:
       6% in last 5 seconds
       7% in last 1 minute
       6% in last 5 minutes

Slot 2 CPU 0 CPU usage:
       5% in last 5 seconds
       4% in last 1 minute
       4% in last 5 minutes

[UEB_SW_CORE]
```

Figura 5. *Temperatura y uso del procesador.*

En el caso del firewall los datos del uso del procesador, memoria y sesiones concurrentes obtenidos en las últimas 24 horas da como resultado que el equipo de seguridad perimetral funciona de manera óptima.