UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

Estudio De Las Medidas De Seguridad Empleadas En Los Servidores Y Servicios Informáticos Del GADP Los Ríos.

EGRESADO:

José Antonio Lema Vargas

TUTOR:

Ing. José Teodoro Mejía Viteri, MSC

AÑO 2017

Introducción

Este estudio de caso involucra principalmente a las redes y comunicaciones de datos, y sus beneficios al tratar temas relacionados con tecnologías de servidores; también a la forma eficiente de utilizarlos asegurando su operatividad en el mayor tiempo posible.

En la actualidad en el sector público se priorizan la seguridad de la información que es catalogada como uno de los bienes más preciados para la continuidad del negocio, y el punto de diferencia con la competencia. La seguridad de la información dentro de una empresa tiene varios aspectos: seguridad de acceso, seguridad de dispositivos, manejo de contraseñas y control de vulnerabilidades, entro otros, además hay que tener en cuenta que es imposible encontrar sistemas completamente seguros, porque cada día se descubren nuevos riesgos en distintos niveles. (Monsalve-Pulid, 2014)

Hoy en día, cualquier organización, independientemente del tamaño de la misma, dispone de su página web para divulgar por Internet su negocio y su identidad. Con todo esto, los servidores web donde se alojan cada una de estas páginas, han pasado a ser un blanco fácil para cualquier tipo de atacante.

El Gobierno Autónomo Descentralizado Provincial de Los Ríos cuenta con un Datacenter donde funcionan 25 servidores, 7 de estos están expuestos directamente en internet, los mismos que han sido atacados varias veces con el único fin de llamar la atención, utilizarlo de spam o dejar sin servicio a la empresa.

En el Gobierno Autónomo Descentralizado Provincial de Los Ríos, los servidores web tienen una mayor protección frente a cualquier tipo de amenazas, sobre todo tienen una seguridad especializada y bien elaborada, sin embargo, no están exentos de ataques

recurrentes. La mayor parte de estos ataques, en la actualidad, son una consecuencia de deficientes configuraciones de servidores o un mal diseño de los mismos.

Desarrollo

El Gobierno Autónomo Descentralizado Provincial de Los Ríos es una organización gubernamental y de las más importantes de la provincia, en esta institución por varias ocasiones se ha logrado vulnerarla seguridad a nivel de servidores por varios factores.

Se inició la investigación con la elaboración de la infraestructura tecnológica que se encuentra en el centro de datos de la institución con el objetivo de conocer las distintas vulnerabilidades que afecten la información que se encuentra almacenada.

En el Gobierno Autónomo Descentralizado Provincial de Los Ríos, un gran porcentaje de sistemas web trabajan conjuntamente con el uso de bases de datos las cuales nos permiten interactuar con la aplicación y guardar información, estas trabajan con un lenguaje llamado sql el cual permite interactuar con las bases de datos, debido a esto han aparecido múltiples vulnerabilidades entre las cuales sobresalen el ataque por inyección sql el cual pone en riesgo la integridad de los datos que se encuentran registrados.

Entrevistando al Ing. José Velastegui Muñoz, comenta que esto es posible gracias a que el ingreso de la información hacia el servidor se realiza mediante el uso de los métodos POST y GET, es por ello que es necesario realizar un filtrado de esos datos a través de técnicas existentes para evitar este tipo de inconvenientes.

Entre las vulnerabilidades más frecuentes que encontramos en los servidores web son los ataques de inyección sql. Existen muchas medidas de prevención para este tipo de ataques, pero hay que mencionar que la mejor forma de prevenir estos ataques emplear buenas practicas al momento de desarrollar una aplicación. También es de vital importancia

mostrar estos intentos de inyección sql en forma y tiempo con el objetivo de protegerse y establecer medidas que se crean pertinentes antes de que ocurran sucesos desagradables.

Dentro de este tipo de ataques, se puede encontrar el ataque a ciegas por inyección de SQL, o también denominado “Blind SQL Injection”, este tipo de ataques permite realizar consultas sql mal formuladas sin que la pagina devuelva ningún mensaje de error por lo cual los intrusos tiene facilidad a la hora de ejecutar las consultas que crean necesarias y pasar totalmente desapercibidos. (Deckel, 2012)

Al momento de realizar el desarrollo de una aplicación resulta complejo desarrollar sistemas cien por ciento seguros, esto se debe a factores como la escasez de tiempo o la cantidad de personas que trabajen en el proyecto, aun así existen métodos que permiten alejarnos de este tipo de problemas. (Deckel, 2012)

Como consejos para evitar sufrir el ataque por inyección SQL se puede considerar lo siguiente:

Evitar caracteres especiales utilizados en consultas sql; revisar los valores de las consultas, incluso si el contenido de la misma es entero es necesario pasarlo entre comillas simples; atribuir la menor cantidad de privilegios a los usuarios que tengan acceso al código de la aplicación, estos deberán tener los permisos justos para que interactúen con la información y así evitar eventos no programados; programar de forma correcta, una medida a tomar en cuenta para evitar ataques de esta naturaleza es aplicar una buena programación con conceptos básicos y sobre todo dedicarle interés al proyecto en el que se está trabajando. (pressroom, 2013)

El sistema web debe tener las bases suficientes tanto en lo que tiene que ver con el diseño como con su estructuración, el sistema también debe ser sometido a las pruebas

necesarias para evitar fallos de seguridad o cualquier tipo de inconvenientes al momento de su implementación.

Es recomendable tener en cuenta ciertas situaciones a la hora de desarrollar software: realizar el análisis respectivo con el objetivo de adquirir el conocimiento suficiente para evitar accesos no verificados en el sistema; por lo general la información ingresada por el usuario debe ser validada en la parte del servidor; emplear una estrategia de validación de las entradas, las mismas que se deben realizar de acuerdo a los requerimientos solicitados, además se debe tener presente la utilización de los firewall ya que estos nos permiten detectar ataques. (Domínguez, 2015)

Se han registrado también ataques DOS (DoS, Denialofservice), el proposito de estos ataques consisten en impedir el acceso a los recursos de las empresas por tiempo indefinido.

Los ataques DOS pueden afectar el funcionamiento de los servidores que tenga acceso a internet, y así desprestigiar las empresas o compañías que trabajan a través del internet. (Roldan, 2014)

También existen los ataques DDOS (Distributed Denial of Service) los cuales aparecen cuando muchos equipos ejecutan el ataque DOS (Coup, 2017)

Los ataques DDOS se pueden contrarrestar de forma sencilla, pues se debe identificar las direcciones ip de los computadores que envían varias peticiones al servidor y bloquearlos, por lo general los computadores que realizan este tipo de ataques son computadores personales los cuales están infectados con virus que permiten a los ciber delincuentes tener el control de los mismos. (Barredo, 2016)

En sistemas operativos Linux existe un firewall llamado iptables, este se inicia junto con el sistema manteniéndose activo todo el tiempo permitiendo aplicar a toda la red las reglas que se le hayan configurado anteriormente.

Una regla muy importante es la protección contra ataques dos, esta regla tiene como objetivo rechazar las conexiones desde equipos que tienen más de 80 conexiones establecidas, se podría elevar el limite pero podría provocar inconvenientes con clientes legítimos que normalmente requieren establecer un gran número de conexiones.

La mayoría de los ataques dos que se basan en tcp se realizan con una alta tasa de transferencia de paquetes, es por eso que hay que procesar y bloquear la mayor cantidad de paquetes por segundo como sea posible.

La seguridad de la información para una organización depende de diferentes frentes: físico, referente al alojamiento de información; el social, que tiene relación con el grado de discrecionalidad del personal que manipula la información, y el lógico, que tiene que ver con la configuración de los niveles de accesibilidad y disposición. (Monsalve-Pulid, 2014)

Como Administrador de Bases de Datos, de esa forma debe actuar el encargado del desarrollo del software para realizar las validaciones respectivas, la persona que esté a cargo del desarrollo y la implementación de la base de datos debe tener presente conservar la integridad de la misma ya que es donde se va a almacenar toda la información que se solicitara a los clientes y usuarios a través de la sistema web que se vaya a implementar.

En el Gobierno Autónomo Descentralizado Provincial de Los Ríos existe la siguiente infraestructura de servidores. En la **Tabla 1** se detallan los mismos:

Tabla 1

Listado de servidores del Gobierno Autónomo Descentralizado Provincial de los Ríos

SERVIDOR	CARACTERISTICAS
Servidor de Correo	El cual se encarga de la administración de los e-mail de los usuarios y los clientes.
	1 servidor físico local
	2 servidores en la nube
Servidor Proxy	Es el cual reconoce el usuario que está realizando la petición..
	1 servidor virtual
Servidor Web	Almacena páginas en formato HTML, los cuales proporcionan información a los clientes que accedan a sus servicios.
	3 servidores físicos web
	2 servidores virtuales en la nube
Servidor de Base de Datos	Se encarga de gestionar las bases de datos de los clientes que realizan peticiones al servidor.
	1 servidor físico de bases de datos
Servidores Geográficos	Como ya expresamos anteriormente, hay servidores compartidos con información cartográfica.
	1 servidor físico
Servidores de Aplicaciones	Recientemente también se han popularizado servidores especializados de aplicaciones web.
	2 servidores físicos
	2 servidores virtualizados
Servidor de Virtuales	Servidor Físico que corre VMWARE ESXI con equipos virtualizados de contingencia
	4 servidores virtuales
Servidor DNS	1 servidor windows 2012 Server
Servidor de Telefonía	2 denwa IP

Servidor de Storage	1 videos 2 almacenamiento de archivos (nas)

Nota: De los 25 servidores que conforman el DataCenter de esta institución, 7 están expuestos directamente al internet.

Es así como de forma técnica se ha caracterizado un esquema seguro, este debe corresponder al ajuste de niveles de confidencialidad, integridad y disponibilidad de información, según lo referencia la norma ISO 27001.

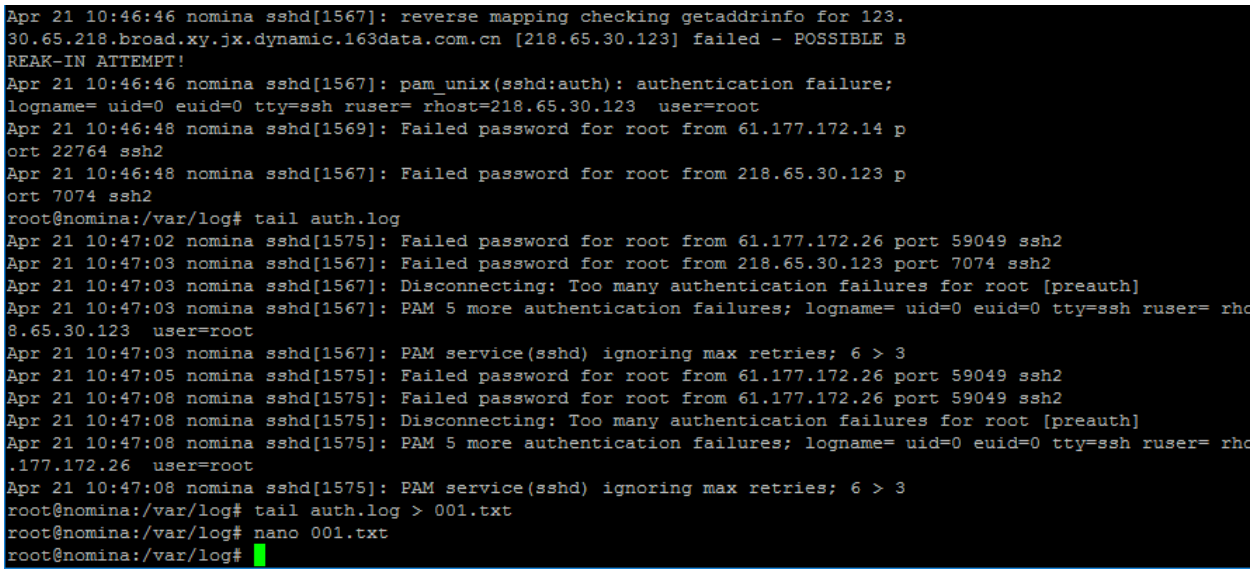
En la actualidad, la determinación del nivel de inseguridad visto desde una óptica de vulnerabilidad y riesgo de la información, trasciende los niveles de su operatividad o uso, de forma que es muy necesario interpretar sus unidades de portabilidad y los medios por los que se está transmitiendo, donde se abren nuevas configuraciones para el fraude, alteración y uso indebido. (Monsalve-Pulid, 2014)

Los ataques dirigidos a las aplicaciones web que se encuentran alojadas en los servidores son muy comunes en la actualidad, el objetivo de estos ataques consiste en extraer información confidencial de las empresas o infectan a los servidores con cualquier tipo de virus y así perjudicar las instituciones.

Cuando hablamos de servidores web resulta de mucha importancia realizar la comprobación de los archivos log, estos proporcionan información relevante sobre el estado en que se encuentran los servidores. Los archivos log se encargan de registrar varios servicios de los sistemas operativos entre los cuales se pueden mencionar ftp telnet entre otros. Hay que tener en cuenta que si los intrusos logran acceder a los servicios con éxito obtendrán los mayores privilegios del sistema por lo que quedara expuesto de manera total. (Roldan, 2014)

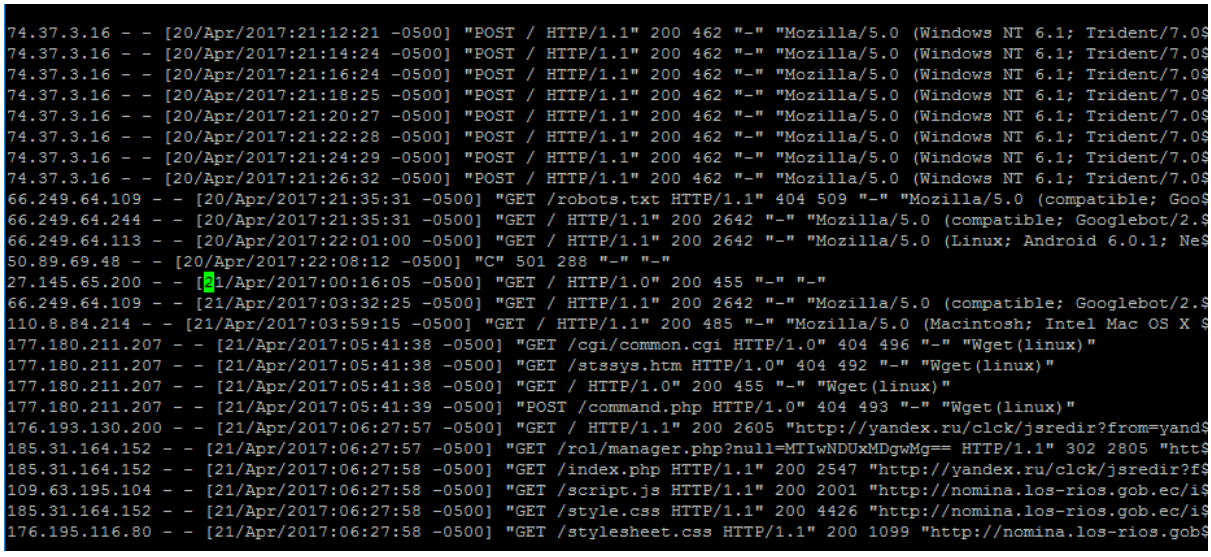
La imagen que se muestra a continuación se observa un archivo log que contiene registro de un servidor apache:

Figura 1. Captura de Pantalla de Chequeo de Log de Servidor de Nominas



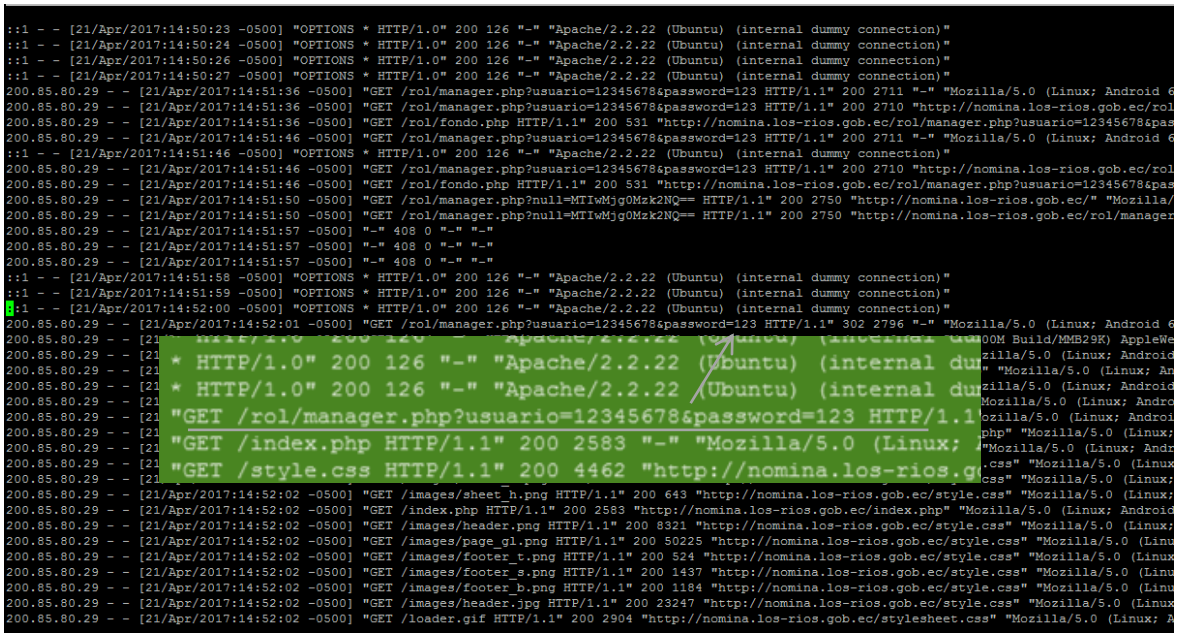
Autor: José Lema

Figura 2. Captura de Pantalla de Chequeo de Log de Servidor de Nominas



Autor: José Lema

Figura 3. Captura de Pantalla de Chequeo de Log de Servidor de Nominas



Autor: José Lema

Comando utilizado:

root@nomina:/var/log/apache2# nano access.log

Con esto se puedo observar el log de los accesos, el cual muestra varios intentos de ataques por inyección por el 21 de abril del 2017, aproximadamente a las 14:00

Para tener una evidencia de ataques, se ha realizado una reunión con el administrador de seguridades, Ing. Daniel Burbano, quien indicó que la revisión de los archivos log constantemente nos permite tener una certeza de la situación en que se encuentra nuestro servidor.

En los sistemas operativos Linux se encuentran dos archivos que contienen los registros importantes los cuales son los siguientes:

/var/log/secure: En este archivo se encuentra información sobre los accesos que se realizan en el servidor en cuestión.

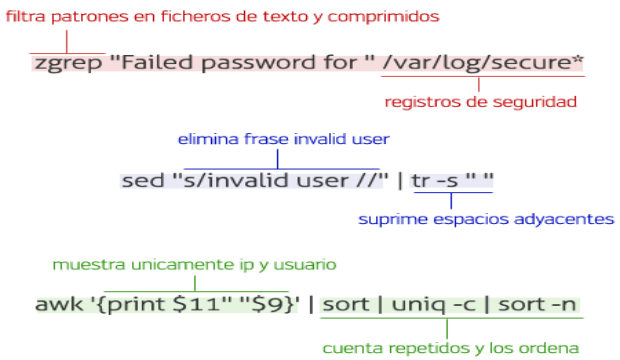
/var/log/messages: En este archivo se registran mensajes que contiene información más profunda.

Por lo general en el directorio /etc/syslog.conf se encuentra un programa el cual se llama logrotate.conf, este tiene como objetivo comprimir los archivos log cuando estos ocupan mucho espacio o cuando ha transcurrido mucho tiempo desde que se crearon.

Los sistemas de registro de logs son de mucha importancia en nuestros equipos de cómputo, porque nos permiten detectar si alguien está intentando acceder a nuestro sistema, y si ha conseguido ver lo que este ha hecho. También hay que señalar el directorio /var/log/secure, es aquí donde se encuentra la información de los accesos al servidor. (Salomón, 2012)

Se muestra a continuación una imagen explicitaría de un filtrado de patrones de texto en archivos muy útil en estos casos de revisión de logs:

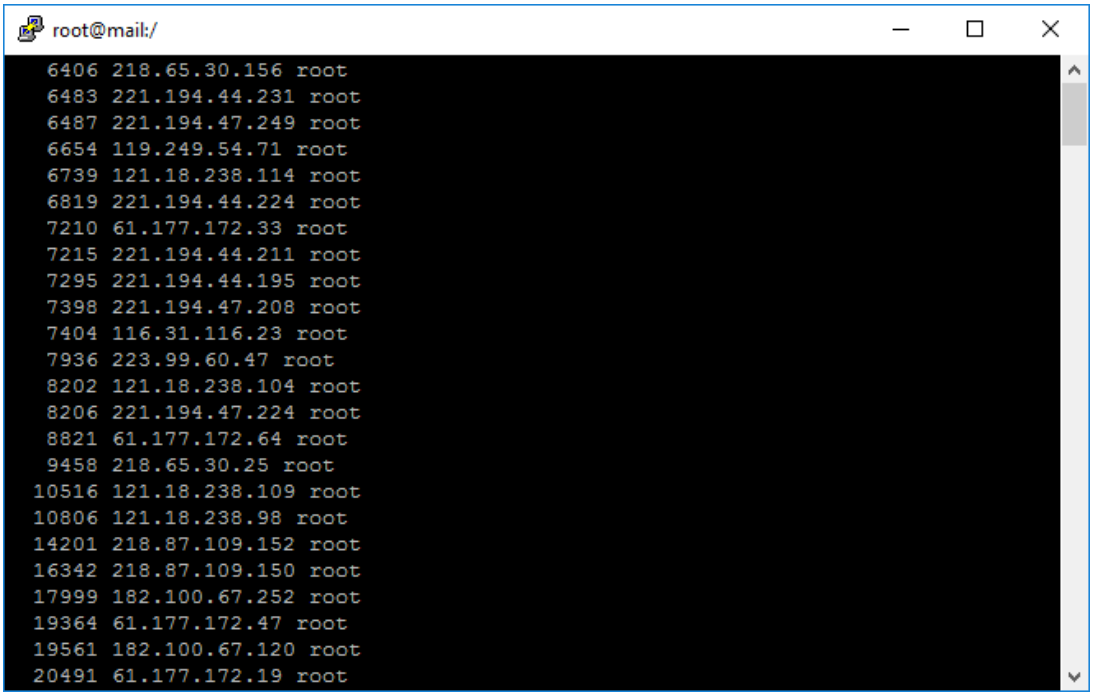
Figura 4. Comandos útiles para listar intentos de conexión



Autor: J. Román Hernández

Esto nos mostrara detalladamente una lista con los intentos realizados a los servidores.

Figura 5. Revisión de intentos de ataques históricos en el servidor de correos



Autor: José Lema

Existen los sistemas de prevención de intrusos (IPS), estos analizan constantemente el tráfico de las redes con el objetivo de obtener información y a la vez realizar acciones preventivas para así mantener las redes protegidas de cualquier actividad que este destinada a proporcionar daños y perjuicios a los servicios que forman parte de la institución.

Los IPS/IDS se pueden clasificar según su fuente de información: Red (Network IDS/IPS): los IPS/IDS de red analizan las redes mediante la obtención del trafico especifico utilizando técnicas para analizar paquetes de datos; Host (Host IDS/IPS): estos analizan la forma en la que se comporta un sistema operativo y los detalles relacionados con la seguridad de los mismos. Los IPS/IDS también se clasifican según el tipo de respuesta activada; Pasiva estos sistemas se encargan de generar una notificación al encargado de la administración pero no hay una modificación en el entorno del servidor. Estos sistemas son conocidos como IDS (Sistemas de Detección de Intrusos); Activa: Se encargan de emitir una alerta cuando detectan actividad sospechosa, además también realizan acciones correctivas que pueden

tener cambios en el entorno que se está analizando, como bloquear un tráfico de información o finalizar una conexión actual entre otras.

Estos sistemas son conocidos como IPS (Sistemas de Prevención de Intrusos). (Acosta, 2014)

Existen herramientas que nos ayudan a encuentran vulnerabilidades entre las cuales tenemos las siguientes:

- Nessus: es el escáner de vulnerabilidades que trae herramientas para realizar auditorías en los sistemas con el objetivo de encontrar problemas de seguridad.
- John the Ripper: es una herramienta que se encarga de descifrar contraseñas mediante fuerza bruta se desarrolló para sistemas Linux, pero también funciona correctamente en sistemas operativos MAC y Windows.
- OpenVas: es una suite de software que tiene como objetivo integrar servicios y herramientas para el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos.

Se ha recurrido a utilizar la herramienta OpenVas para analizar los servidores que están siendo objeto de nuestro estudio como son el servidor de Correos y el servidor de Nominas del Gobierno Autónomo Descentralizado Provincial de Los Ríos.

Figura 6. Resultados del escaneo a los Servidores de Correos y Nominas

SERVIDOR DE CORREOS

2 Results per Host

2.1 181.211.131.229

Host scan start Wed May 31 06:52:03 2017 UTC
Host scan end Wed May 31 07:06:58 2017 UTC

Service (Port)	Threat Level
general/tcp	Low
general/tcp	Log
general/CPE-T	Log
2828/tcp	Log
21/tcp	Log
2000/tcp	Log
1723/tcp	Log

SERVIDOR DE NOMINAS

2 Results per Host

2.1 181.211.131.228

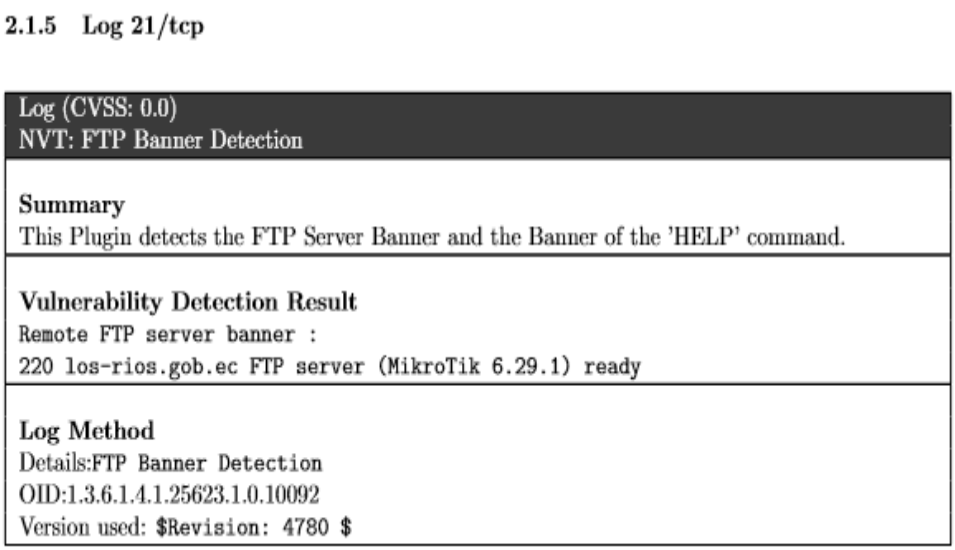
Host scan start Wed May 31 06:14:48 2017 UTC
Host scan end Wed May 31 06:18:34 2017 UTC

Service (Port)	Threat Level
general/tcp	Log
general/CPE-T	Log
2828/tcp	Log
2000/tcp	Log
1723/tcp	Log

Autor: José Lema

Como resultado se obtuvo un análisis detallado sobre las vulnerabilidades a las que se encuentran expuestos los servidores antes mencionados, a continuación, se detallan los resultados del análisis respectivo:

Figura 7. Vulnerabilidad en puerto 21/tcp



2.1.5 Log 21/tcp

Log (CVSS: 0.0)
NVT: FTP Banner Detection

Summary
This Plugin detects the FTP Server Banner and the Banner of the 'HELP' command.

Vulnerability Detection Result
Remote FTP server banner :
220 los-rios.gob.ec FTP server (MikroTik 6.29.1) ready

Log Method
Details:FTP Banner Detection
OID:1.3.6.1.4.1.25623.1.0.10092
Version used: $Revision: 4780 $

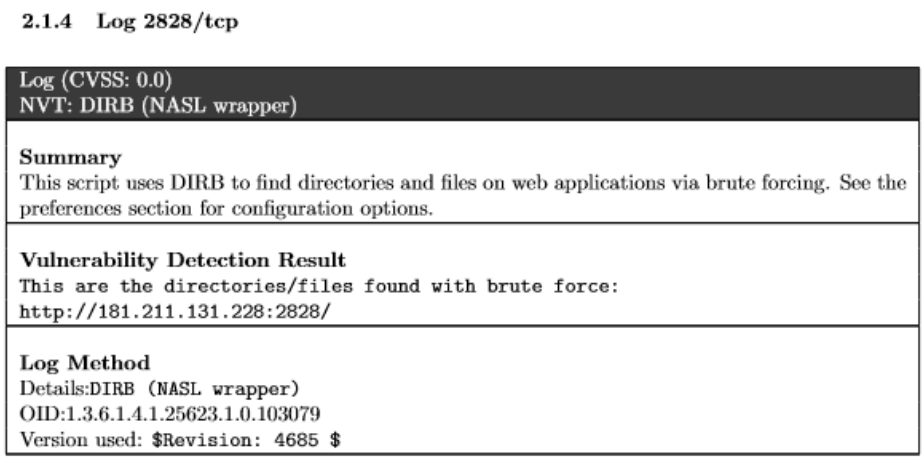
Autor: José Lema

El resultado de este análisis muestra las vulnerabilidades a la cual está expuesto el servidor ftp que se encuentra en el puerto 21/tcp, hay que tener en cuenta que los servidores ftp son vulnerables por que la transferencia de archivos a través de estos es mediante texto plano, por lo cual se muestra muy frágil para ser objeto de ataques. FTP es un protocolo de comunicaciones el cual permite transferir datos a través de los sistemas que se encuentran funcionando mediante la conexión de una red tcp de forma que se puede interactuar desde un equipo cliente a un equipo servidor y viceversa independientemente del sistema operativo que se esté utilizando.

Un problema muy común en este tipo de protocolos es no ofrecer máxima seguridad porque su prioridad es ofrecer mayor velocidad de conexión, debido a esto tanto la información del usuario como la del servidor y la transferencia de cualquier archivo quedan expuestos a posibles ataques.

Como prevenciones podemos mencionar las siguientes: configurar los permisos del servidor de modo que usuarios remotos no puedan tener los mismos privilegios que un usuario root; limitar los accesos remotos al servidor, porque al momento de crear un nuevo usuario simultáneamente se crea un nuevo agujero para la entrada de archivos de dudosa procedencia, además hay que tener en cuenta que la transferencia de archivos a través de este protocolo se realiza sin encriptar por lo cual es un blanco fácil para los atacantes; Cambiar las contraseñas por defecto del FTP, porque lo único que conseguimos es brindar facilidades a los posibles atacantes ; utilizar distintas contraseñas para cada propósito.

Figura 8. Vulnerabilidad en puerto 2828/tcp



2.1.4 Log 2828/tcp

Log (CVSS: 0.0) NVT: DIRB (NASL wrapper)
Summary This script uses DIRB to find directories and files on web applications via brute forcing. See the preferences section for configuration options.

Vulnerability Detection Result
`This are the directories/files found with brute force:`
`http://181.211.131.228:2828/`

Log Method Details:`DIRB (NASL wrapper)` OID:1.3.6.1.4.1.25623.1.0.103079 Version used: `$Revision: 4685 $`

Autor: José Lema

En el puerto 2828/tcp se ha logrado acceder a directorios del servidor de correos utilizando ataque de fuerza bruta a través de DIRB el cual es una herramienta que sirve para listar directorios ocultos de un servidor mediante fuerza bruta.

El objetivo de este tipo de ataques es probar diferentes combinaciones hasta dar con la clave de cifrado que se ha utilizado para encriptar un documento, cuanto más complicada sea la contraseña existirá mayor dificultad para vulnerarla mediante este sistema de ataque, muchas veces se necesitan horas o incluso meses de procesos de cálculo de ordenador para dar con la clave otras veces no se llega a vulnerar.

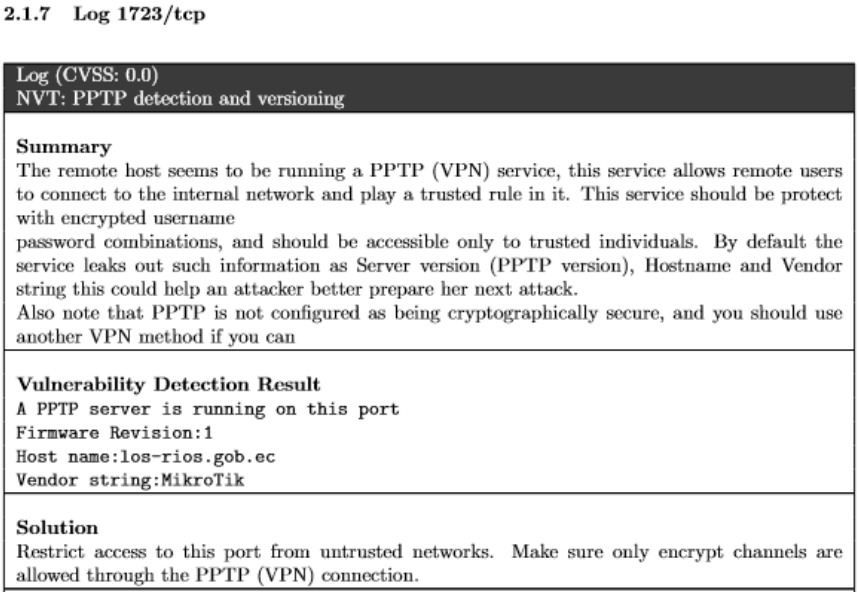
Como soluciones podemos decir que debemos usar todo el espacio disponible para las contraseñas, si esta puede tener una longitud máxima de 12 caracteres, usaremos los doce, intercalándolos mayúsculas y minúsculas con números, además si el sistema lo permite usaremos caracteres especiales como asteriscos y guiones, también evitar en lo posible utilizar contraseñas que sean fáciles de detectar por factores sociales, de actualidad o comodidad. (López, 2010)

Es recomendable la utilización de software para la exploración de puertos, en una red extensa la utilización de este tipo de software podría ayudar con la identificación de vulnerabilidades potenciales, sin embargo, se debe mencionar que este tipo de herramientas es utilizado por los hackers que intentan comprometer la seguridad, por ello es recomendable bloquear los puertos que no se utilizan y proteger del acceso no autorizado a los que se encuentran en estado abierto.

El análisis en el puerto 1723/tcp muestra la vulnerabilidad a la que está expuesto, porque en este puerto se encuentra ejecutándose un servidor mediante el protocolo PPTP. El protocolo PPTP (Point to Point Tunneling Protocol) Protocolo de Túnel Punto a Punto es un protocolo de comunicaciones el cual permite el intercambio seguro de datos de un cliente a

un servidor formando una red privada virtual. La utilización de una VPN básicamente consiste en encapsular los paquetes de datos que salen de una LAN o del equipo del usuario remoto. (Pellejero, 2006)

Figura 9. Vulnerabilidad sobre Protocolo PPTP



2.1.7 Log 1723/tcp

Log (CVSS: 0.0)
NVT: PPTP detection and versioning

Summary
The remote host seems to be running a PPTP (VPN) service, this service allows remote users to connect to the internal network and play a trusted rule in it. This service should be protect with encrypted username
password combinations, and should be accessible only to trusted individuals. By default the service leaks out such information as Server version (PPTP version), Hostname and Vendor string this could help an attacker better prepare her next attack.
Also note that PPTP is not configured as being cryptographically secure, and you should use another VPN method if you can

Vulnerability Detection Result
A PPTP server is running on this port
Firmware Revision:1
Host name:los-rios.gob.ec
Vendor string:MikroTik

Solution
Restrict access to this port from untrusted networks. Make sure only encrypt channels are allowed through the PPTP (VPN) connection.

Autor: José Lema

Una de las ventajas de utilizar Protocolos PPTP es que minimiza la necesidad del uso de sofisticados y caros equipos de telecomunicaciones para permitir la comunicación de equipo portátiles y remotos.

Como solución el análisis no refleja que debemos restringir el acceso a redes no confiables, si bien es cierto que la utilización de este protocolo permite el tráfico seguro de datos también hay que tener en cuenta que puede ser objeto de ataques.

Los protocolos PPTP operan en el nivel de enlace del modelo OSI por lo cual emplean cifrado nodo a nodo el cual permite a dos ordenadores construir una VPN entre ellos, hay que tener en cuenta que un ataque que ha sido realizado a nivel de enlace con éxito tiene control sobre todas las capas superiores. (Albacete, 2015)

Como se menciona anteriormente los protocolos PPTP trabajan a nivel de enlace, así una manera de resolver estas vulnerabilidades es configurando los aparatos físicos como switch o router correctamente para proporcionar mayor seguridad. En muchas ocasiones no es necesario adquirir nuevas tecnologías para contrarrestar ataques, simplemente se debe aplicar políticas de seguridad a los dispositivos con los que se está trabajando. Además, hay que tener presente que tipo de protección se tiene con respecto al malware, ciertos proveedores de servicios proporcionan a sus clientes escáneres anti-malware para asegurarse que no estén descargando virus o troyanos, para así evitar cualquier tipo de daños incluso a dispositivos físicos.

Conclusión

Como resultado del análisis realizado a los servidores del Gobierno Autónomo Descentralizado Provincial de Los Ríos se concluye que existen problemas por solucionar en cuanto a la seguridad, este trabajo solo se tomó una muestra de registros logs y se realizó el análisis con la herramienta OpenVas a 2 servidores, esto es al servidor de correos y al servidor de nóminas, por ser los más críticos.

La revisión de logs debe realizarse de manera periódica para estar al tanto de las actividades que presenten los servidores y controlar los riesgos existentes por vulnerabilidades que aparecen en los servicios que dispone el G.A.D. Provincial.

A través del escaneo realizado con la herramienta OpenVas, por la efectividad de los resultados obtenidos, se debe implementar una política de revisión periódica para mantener nuestros datos y equipos seguros, porque solamente habían optado por cerrar puertos desde un equipo firewall de borde.La institución no cuenta con un sistema para detectar intrusos en los servidores con el fin, de realizar acciones programadas que brinden mayor seguridad a los servidores que forman parte de la institución.

Bibliografía

Acosta, D. (16 de Septiembre de 2014). *pcihispano*. Obtenido de pcihispano: https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-v-sistemas-de-deteccionprevencion-de-intrusiones-idsips/

Albacete, J. F. (2015). *Seguridad en equipos informáticos.* Malaga: ic Editorial.

Barredo, Á. (09 de 09 de 2016). *hipertextual.com.* Obtenido de hipertextual.com: https://hipertextual.com/2016/09/ataque-ddos-dos-diferencias

Coup, A. (12 de Marzo de 2017). *Segiridad España.* Obtenido de Segiridad España: http://es.ccm.net/contents/22-ataque-por-denegacion-de-servicio

Deckel, A. (2012). *INYECTANDO CODIGOS A MY SQL.* Michigan.

Domínguez, A. A. (Viernes, 21 de Agosto de 2015). *www.seguridad.unam.mx.* Obtenido de www.seguridad.unam.mx: http://www.seguridad.unam.mx/documento/?id=35

Duarte, E. (11 de Julio de 2012). *capacityacademy*. Obtenido de capacityacademy: http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

García, C. A. (2013). *Transmisión de información por medios convencionales e informáticos.* Bogota: ALFA Y OMEGA.

Monsalve-Pulid, J. A. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *SCIELO*, 5.

Peirano, M. (2015). *El pequeño libro rojo del activista en la red.* Madrid: AMAZON.

Pellejero, I. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN.* Madrid: MARCOMBO S.A.

pressroom. (26 de Diciembre de 2013). *hostalia.* Obtenido de hostalia: https://pressroom.hostalia.com/white-papers/ataques-inyeccion-sql

Roldan, A. (2014). *SEGURIDAD DE LA INFRAESTRUCTURA TECNOLOGICA.* MANISALES.

Salomón, R. E. (2012). *El gran libro de Debian GNU/Linux.* Barcelona: Marcombo Ediciones Técnicas.

Sarubbi, J. P. (2008). *Seguridad Informatica Tecnicas de defensa comunes bajo variantes del sistema operativo Unix.* Buenos Aires: Universidad Nacional de Lujan.