IMPLEMENTAR Y FORTALECER REDES COMPUTACIONALES MEDIANTE HERRAMIENTAS OPEN SOURCE PARA LAS PYMES EN ECUADOR.

Veintimilla Valverde Allan M.; Manjarrez Fajardo Darwin A.
Escuela Superior Politécnica del Litoral
almavein@espol.edu.ec; damanjar@espol.edu.ec

ABSTRACTO

El presente proyecto integrador tiene como objetivo el brindar un fortalecimiento de entornos GNU/Linux basados en el modelo de defensa en profundidad, es decir un fortalecimiento de sistemas computacionales por capas. Dicho proyecto menciona las debilidades de entornos generales, los cuales con fortalecidos y mostrados en ejemplos de configuración y funcionamiento, se estará proporcionado practicas para mantener el entorno lo más seguro posible.

En definitiva este trabajo se recomienda a todos aquellos que deseen reforzar conceptos, así como para los que necesiten una base desde la que partir a la hora de fortalecer un entorno Linux.

OBJETIVOS

- ✓ Analizar técnicas de Defensa en Profundidad computacional.
- ✓ Implementar herramientas o complementos prácticos de distribución libre, con el fin de fortificar el entorno de redes y sistemas.
- ✓ Analizar ventajas entre sistemas de entornos computacionales estándar y entornos robustos ejecutándose.

METODOLOGÍA

Para la realización se usará como base el Sistema Operativo Debian GNU/Linux para establecer pilares para un sistema robusto. Se implementará un entorno de red cliente-servidor integradas por dos computadoras y un router para la simulación de una red utilizadas en entornos pymes generales.

Implementaremos también un esquema que representa una configuración de firewall de dos patas, un servidor centralizado de log y gestión de almacenamiento de dichos log, donde instalaremos parámetros de seguridad integral para un manejo de esquemas de seguridad.

Una vez de haber analizado las diferentes herramientas y haber configurado e implantado fortalecimiento en el entorno procederemos a sacar nuestras respectivas conclusiones de los resultados de cada tipo de herramienta, usos, ventajas, desventajas, aplicaciones y limitaciones, para que finalmente poder establecer claramente recomendaciones y observaciones para futuros usos.

IMPLEMENTACIÓN

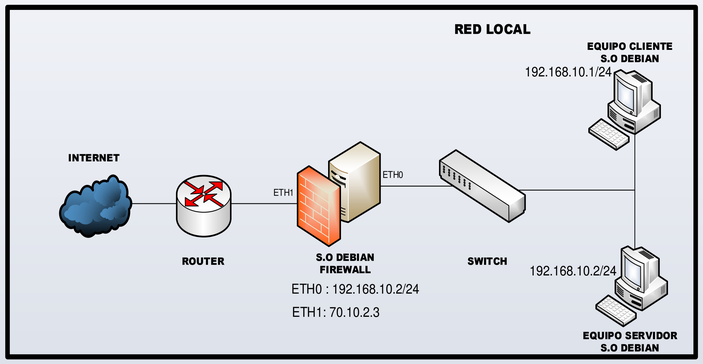


Ilustración 1: *Esquema de red con firewall de dos patas*

Implementación	Saliente	Entrante
Permitir tráfico ICMP	✓	X
Permitir consultas DNS	✓	✓
Permitir consultas HTTP/HTTPS	✓	✓
Permitir Otras consultas	X	X

Tabla1: Servicios implementados en firewall

Requerimiento	Implementación	Aplicación
Administración de Usuarios.	Gestión de Permisos y Usuarios	Servidor - Cliente
Seguridad de gestor de arranque.	Protección con contraseña de GRUB	Protección
Seguridad en sistema de Particiones.	Gestión de Particiones – Cifrado LUKS	Todos los Equipos
Seguridad en sistema de archivos.	GPG	Servidor
Gestor de registro de eventos.	Rsyslog - Logrotate	Servidor - Cliente

Tabla1: Fortalecimiento implementados en red interna

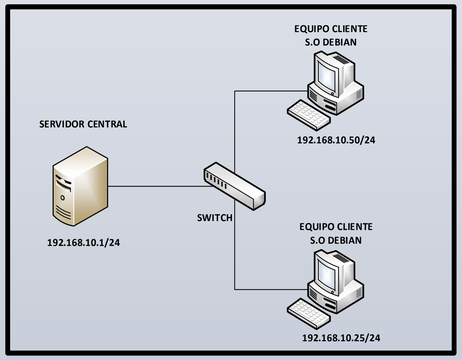
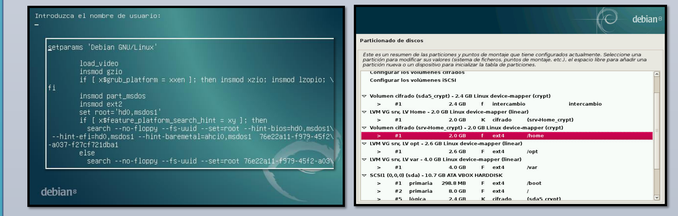
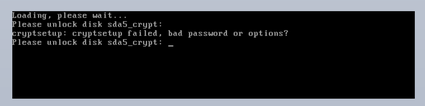
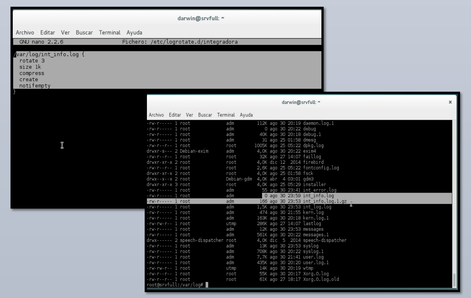


Ilustración 2: *Esquema de red interna.*







CONCLUSIONES Y RECOMENDACIONES

- ❑ 1. La selección de un sistema operativo de distribución GNU/Linux es por su principal beneficio de controlar el funcionamiento de su equipo y asegurar el comportamiento de todos sus programas con los sistemas de gestión de permisos.
- ❑ 2. La protección del sistema de arranque ayuda a prevenir de accesos físico desde medios removibles y control de los parámetros de arranque y acceso y en integración con un cifrado de sistemas de ficheros, permite la proteger los datos de los sistemas de archivos incluso si es removido físicamente los discos.
- ❑ 3. La implementación de seguridad en el perímetro de la red, consiste en implementar políticas de seguridad en los equipos de comunicación, los equipos son instalados entre la red interna y la externa, por lo cual la adquisición de un equipo firewall genera costos elevados para una red pequeña que desea mantener una seguridad del tráfico de la red, por lo cual implementar *Iptables* reduce costos y se mantiene el mismo servicio de filtrado de paquetes.
- ❑ 4. Saber que monitorizar el contenido de los logs de los servidores a medida que progresan es fundamental para detectar y solucionar problemas de forma preventiva, además el detectar velocidades de crecimiento del log inusuales es una característica que le ayudará a saber si su servidor está funcional y proporcionando servicio a un ritmo normal.
- ❑ 5. La implementación no garantiza que el sistema resultado de la integración sea 100% seguro. Para aumentar el porcentaje debemos usar un sistema de mejora continua en referente a las nuevas técnicas que van apareciendo en las tecnologías de la información.
- ❑ 6. Al usar herramientas Open Source nos permite adaptarnos a las necesidades actuales, y una ventaja de aprender en comunidad, sin la necesidad de presupuestar el coste de mantenimiento de software y personal encargado.

REFERENCIAS

[1] Wikilibros, (2011, Enero 3). Seguridad Informática [Online]. *https://es.wikibooks.org/wiki/Seguridad_inform%C3%A1tica/Lo_que_afecta_a_las_distribuciones_de_Gnu/Linux.*

[2] Guillermo Rigotti, Universidad Nacional del Centro de Buenos Aires, (2012, Diciembre 11). Capas del Modelo OSI. [Online]. *www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOsi.pdf.*

[3] Observatorio Tecnológico, Instituto Nacional de Tecnologías Educativas y Formación de Profesorado (2008, Febrero 25) Seguridad Básica en Linux [Online]. http://recursostic.educacion.es/observatorio/web/en/software/software-general/562-elvira-misfud.

[4] Red Hat (2007, Marzo 3) Seguridad del BIOS y del gestor de arranque. [Online]. *http://lists.openshift.redhat.com/docs/manuals/enterprise/RHEL-5-manual/es-ES/Deployment_Guide/s1-wstation-boot-sec.html#.*

[5] P. Fábrega Martínez, (2009, Marzo 31), Seguridad en el arranque [Online] *http://www.bdat.net/documentos/grub/x337.html.*

[6] Guillermo Grandes (2014, Octubre 06). Diagrama Linux netfilter iptables /Online/ https://commons.wikimedia.org/wiki/File:Diagrama_linux_netfilter_iptables.png

[7] Rubén Velasco (2014, Abril) Configuración de firewall en linux con iptables. [Online]. http://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables

[8] Daniel Omar Rodríguez, (2008, Enero 31), Mejores prácticas y herramientas para monitoreo de bitácoras de Unix [Online]. http://danielomarrodriguez.blogspot.com/2008/01/mejores-practicas-y-herramientas-para.html

[9] Rsyslog (2013, Mayo 24) Newbie guide to rsyslog [Online]. http://www.rsyslog.com/guides-for-rsyslog

[10] Linux Config.org (2014, marzo) logrotate - manual page. [Online]. http://linuxconfig.org/logrotate-8-manual-page

RECONOCIMIENTO

En especial a todos los profesores que conocí en la transición de mi formación profesional de mi carrera, por tener el don de compartir sus conocimientos, experiencias y mantener motivado mi ganas de aprender mas cada día.

INFORMACIÓN ADICIONAL

Este trabajo nos proporciona la importancia de su uso para fortalecer las infraestructuras de redes en pequeñas y medianas empresas, analizando vulnerabilidades de seguridad general que un administrador de redes y sistemas puede encontrar a lo largo de su carrera profesional.