ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Trabajo de Unidad de Integración Curricular, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Hardenización Integral del Servidor DELL PowerEdge R7515 en Software y Hardware para Reforzar la Seguridad de la Información en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC) en Quito.

AUTORES: Cando Santo, Alexis Paul y Moyano Álvarez, Darwin Darío

DIRECTOR: Ing. Caicedo Altamarino, Fernando Sebastián

LATACUNGA

2024

ASPECTOS GENERALES

Objetivos

Objetivo general

- Desarrollar e implementar políticas integrales de seguridad para la hardenización de servidores, abarcando tanto aspectos de software como de hardware, con el propósito de garantizar la protección de la información en la Dirección de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre (DTIC).

Objetivos

Objetivos específicos

- Realizar un análisis de los diferentes mecanismos, herramientas y protocolos para brindar seguridad a los servidores de datos.
- Aplicar los mecanismos de seguridad para la hardenización, identificados a través de la investigación bibliográfica, con el propósito de garantizar la protección de la información almacenada en el servidor
- Realizar pruebas de funcionamiento y elaborar un manual de usuario de los mecanismos de seguridad implementados en el proceso de hardenización, con el propósito de asegurar su correcto funcionamiento y facilitar su utilización por parte del personal.

Planteamiento del Problema

En el ámbito militar ecuatoriano, la DTIC juega un papel crucial en la gestión de datos y operaciones, pero el uso de un servidor DELL expone a posibles amenazas cibernéticas. La vulnerabilidad de estos servidores podría resultar en robo de datos e interrupción de servicios críticos, comprometiendo la seguridad nacional. Se propone un plan de fortalecimiento para proteger la información y mejorar las capacidades tecnológicas de la Fuerza Terrestre.

Justificación

La Hardenización Integral de servidores es crucial a nivel global debido al incremento de ataques cibernéticos en diversos sectores. A nivel nacional, la Dirección de Tecnologías de la Información y Comunicaciones (DTIC) busca fortalecer la seguridad del servidor que alberga datos críticos de la Fuerza Terrestre. Este proceso no solo protege la información, sino que también establece un estándar de seguridad para toda la institución militar, fortaleciendo su posición frente a los desafíos en ciberseguridad.

Alcance

La DTIC necesita fortalecer sus sistemas informáticos para proteger la información crítica del personal militar. Hardenizar el servidor es clave, configurando puertos para protocolos seguros y actualizando el sistema operativo y la memoria RAM. Se realizarán pruebas de seguridad, se detectarán y corregirán vulnerabilidades, y se proporcionará un manual para el mantenimiento y la seguridad continua. También se establecerán listas de control de acceso y se crearán copias de seguridad fuera del servidor principal.

MARCO TEÓRICO

El marco teórico se ha construido en 3 ejes principales que son Seguridad de la información Amenaza y Herramientas de seguridad informática, con la finalidad de ir de un aspecto general a un aspecto especifico.

Seguridad de la Información	Amenaza	Herramientas de seguridad informática
Integridad	Amenaza física	Software Libre
Disponibilidad	Amenaza Lógica	FirewallD
Confidencialidad		Usuarios

Seguridad de la Información

La seguridad de la información implica proteger los datos contra accesos no autorizados, alteraciones o pérdidas, asegurando su confidencialidad, integridad y disponibilidad.

Integridad

Disponibilidad

Confidencialidad

AMENAZA

Una amenaza es cualquier evento o situación que tiene el potencial de causar daño o perjuicio a un sistema, organización o individuo.

Amenaza física Riesgo de daños físicos a los servidores debido a desastres naturales, fallos eléctricos o manipulación malintencionada.

Amenaza lógica Peligros relacionados con la seguridad de la información almacenada en los servidores, como virus, malware, ataques de hackers o vulnerabilidades de software.

Herramientas de la seguridad informática

Fail2ban: Fail2ban es una herramienta de seguridad que protege los servidores contra ataques automatizados al detectar y bloquear direcciones IP que realizan intentos de inicio de sesión maliciosos o repetidos.

FAIL2BAN

SNORT

Snort es un sistema de detección de intrusos que monitorea el tráfico de red en busca de actividad maliciosa, basado en reglas predefinidas. Cuando detecta una amenaza, genera alertas y puede tomar medidas para bloquearla o mitigarla. Es ampliamente utilizado en redes para proteger contra intrusiones y ataques cibernéticos.

FirewallD

Firewalld es una herramienta de gestión de firewall comúnmente utilizada en sistemas Linux, incluyendo Ubuntu. Permite configurar y administrar reglas de firewall de manera dinámica, establecer zonas de red con diferentes niveles de confianza y controlar el tráfico de red. Con Firewalld en Ubuntu, los administradores pueden definir reglas para abrir o cerrar puertos, permitir o bloquear tráfico específico y gestionar listas de direcciones IP permitidas o bloqueadas, proporcionando así una capa adicional de seguridad para el sistema.

METODOLOGÍA E IMPLEMENTACIÓN

Metodología

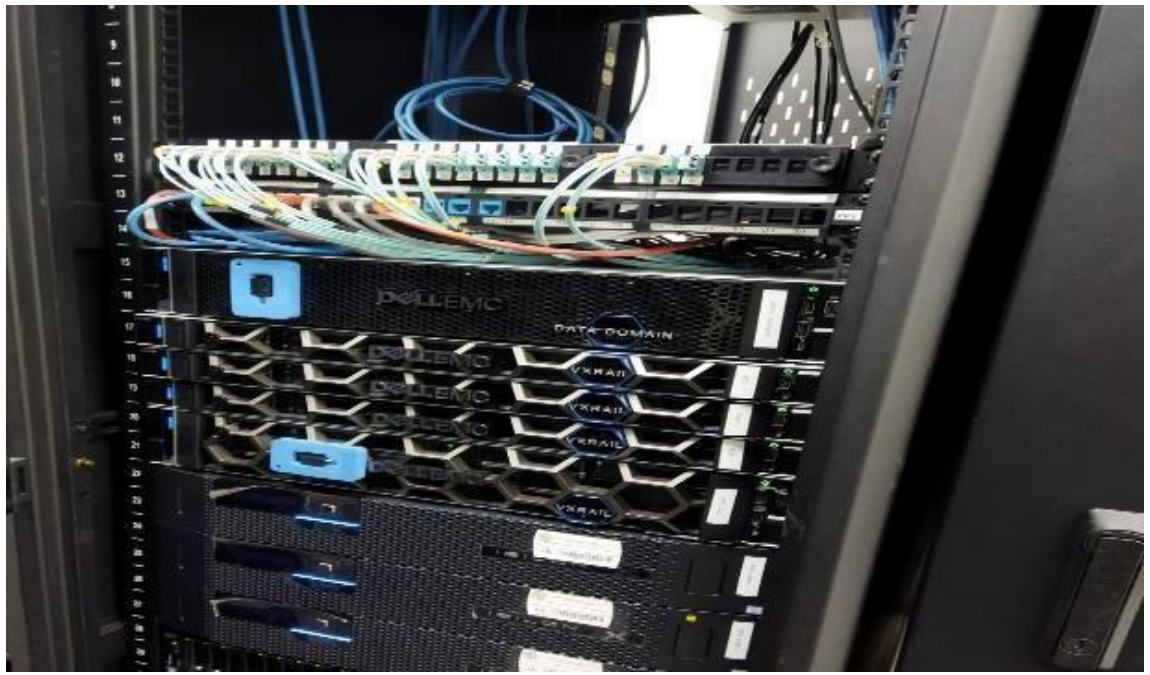
La metodología seguida implicó una evaluación exhaustiva del entorno físico y lógico del servidor, centrada en identificar vulnerabilidades y áreas de mejora. Posteriormente, se implementaron acciones concretas para fortalecer su seguridad y rendimiento, utilizando herramientas y técnicas específicas de endurecimiento y monitoreo, como Firewalld, Fail2Ban y Snort, seleccionadas por su capacidad para mitigar riesgos y detectar intrusiones, respectivamente.

Implementación

Se llevó a cabo un análisis del entorno físico del data center de la DTIC de la Fuerza Terrestre, identificando deficiencias en seguridad. Se mejoró el entorno físico interviniendo en el cableado, alimentación y ubicación del Proliant DL380 G7 para mejorar su rendimiento y seguridad.

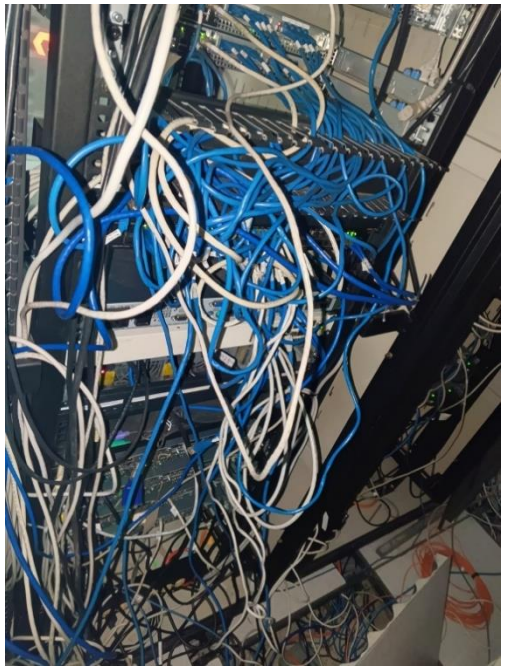
Se utilizo software libre como Fail2Ban y Snort.

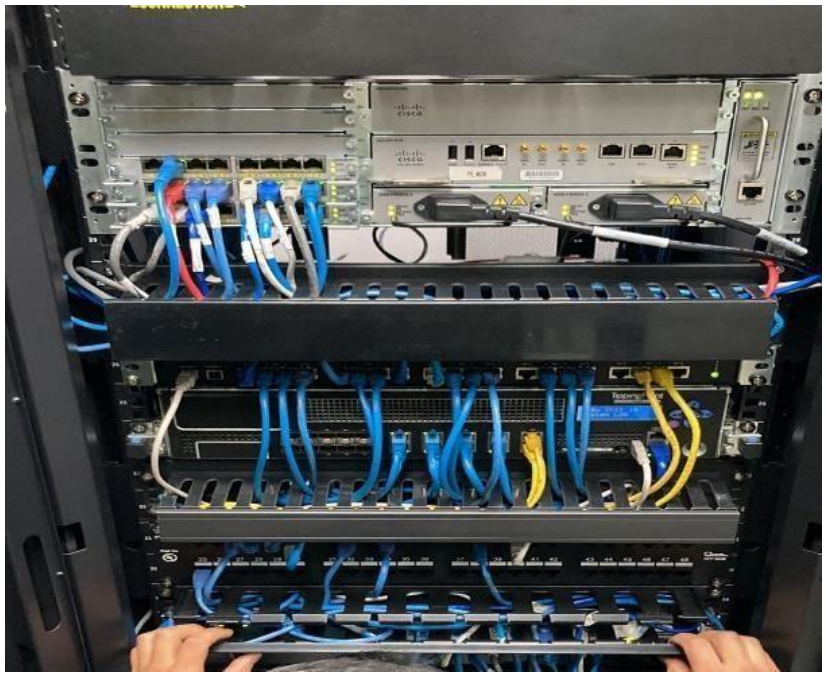
Se implementaron medidas adicionales como FirewallD y se verificó la eficacia de Snort en la detección de actividades maliciosas.



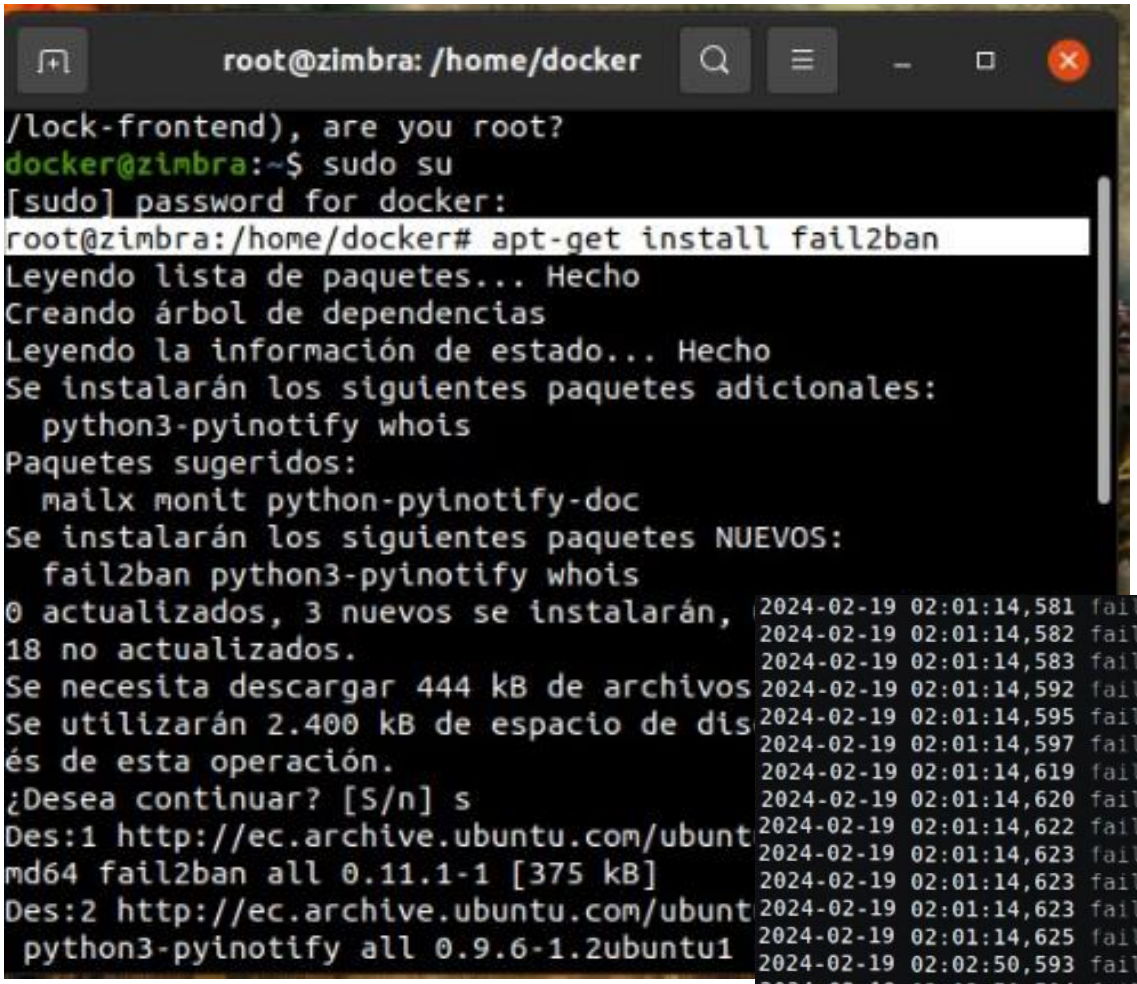
PRODUCTO FINAL

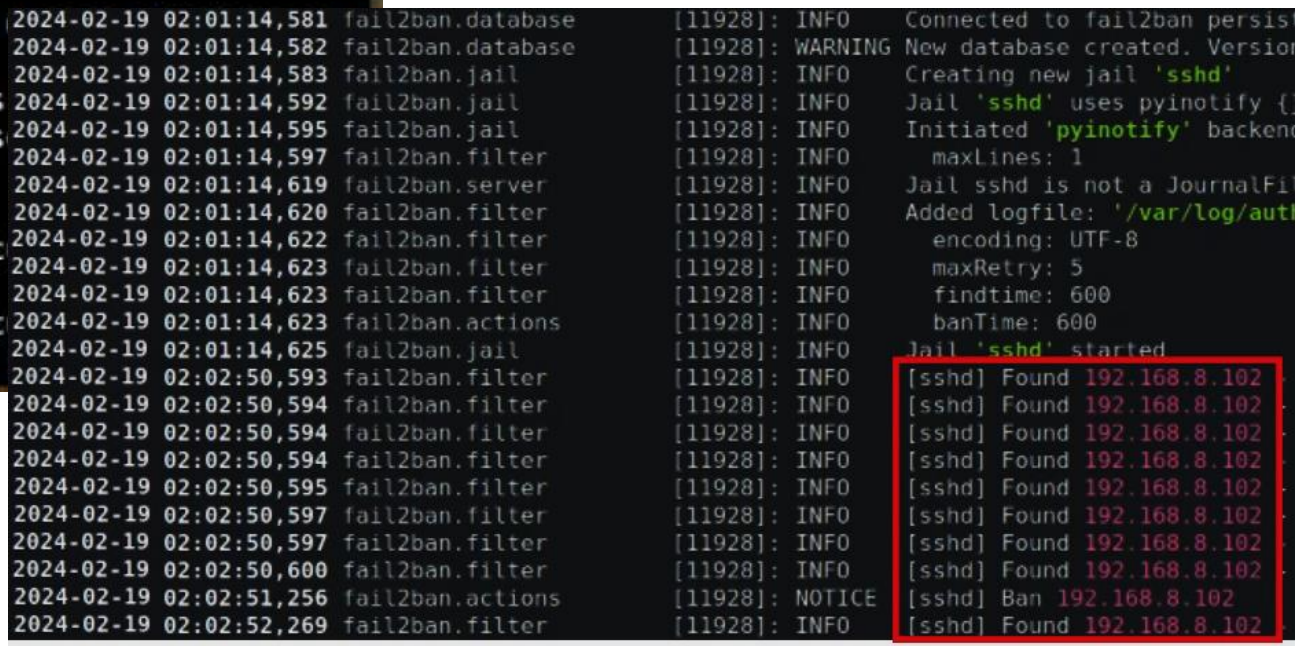
Se obtuvo un entorno físico del data center que ha sido mejorado en términos de seguridad y rendimiento. El servidor Proliant DL380 G7 ha sido intervenido y optimizado para garantizar su óptimo funcionamiento, con medidas de mantenimiento y endurecimiento implementadas, incluyendo el uso de software libre como Fail2Ban y Snort para fortalecer su seguridad.





Además, se han llevado a cabo pruebas prácticas para verificar el funcionamiento de las herramientas implementadas, asegurando su eficacia en la prevención de ataques de fuerza bruta y la detección de intrusos en la red. Se han configurado restricciones de acceso remoto y se han agregado reglas de filtrado avanzadas para mejorar aún más la seguridad del entorno.


root@zimbra: /home/docker
/lock-frontend), are you root?
docker@zimbra:~$ sudo su
[sudo] password for docker:
root@zimbra:/home/docker# apt-get install fail2ban
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
python3-pyinotify whois
Paquetes sugeridos:
mailx monit python-pyinotify-doc
Se instalarán los siguientes paquetes NUEVOS:
fail2ban python3-pyinotify whois
0 actualizados, 3 nuevos se instalarán,
18 no actualizados.
Se necesita descargar 444 kB de archivos
Se utilizarán 2.400 kB de espacio de dis
és de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://ec.archive.ubuntu.com/ubunt
md64 fail2ban all 0.11.1-1 [375 kB]
Des:2 http://ec.archive.ubuntu.com/ubunt
python3-pyinotify all 0.9.6-1.2ubuntu1


2024-02-19 02:01:14,581 fail2ban.database [11928]: INFO Connected to fail2ban persis
2024-02-19 02:01:14,582 fail2ban.database [11928]: WARNING New database created. Versio
2024-02-19 02:01:14,583 fail2ban.jail [11928]: INFO Creating new jail 'sshd'
2024-02-19 02:01:14,592 fail2ban.jail [11928]: INFO Jail 'sshd' uses pyinotify {
2024-02-19 02:01:14,595 fail2ban.jail [11928]: INFO Initiated 'pyinotify' backen
2024-02-19 02:01:14,597 fail2ban.filter [11928]: INFO maxLines: 1
2024-02-19 02:01:14,619 fail2ban.server [11928]: INFO Jail sshd is not a JournalFi
2024-02-19 02:01:14,620 fail2ban.filter [11928]: INFO Added logfile: '/var/log/aut
2024-02-19 02:01:14,622 fail2ban.filter [11928]: INFO encoding: UTF-8
2024-02-19 02:01:14,623 fail2ban.filter [11928]: INFO maxRetry: 5
2024-02-19 02:01:14,623 fail2ban.filter [11928]: INFO findtime: 600
2024-02-19 02:01:14,623 fail2ban.actions [11928]: INFO banTime: 600
2024-02-19 02:01:14,625 fail2ban.jail [11928]: INFO Jail 'sshd' started
2024-02-19 02:02:50,593 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:50,594 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:50,594 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:50,594 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:50,595 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:50,597 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:50,597 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:50,600 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102
2024-02-19 02:02:51,256 fail2ban.actions [11928]: NOTICE [sshd] Ban 192.168.8.102
2024-02-19 02:02:52,269 fail2ban.filter [11928]: INFO [sshd] Found 192.168.8.102

El sistema de monitoreo y detección de intrusos basado en Snort se ha complementado con la instalación de FirewallD para controlar el tráfico de red. Se han establecido notificaciones por correo electrónico para alertar sobre posibles actividades maliciosas detectadas por Snort, brindando así una capa adicional de seguridad y permitiendo una respuesta rápida ante posibles amenazas.

```
root@zimbra:/home/docker# sudo firewall-cmd --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="192.168.124.1/15" service name="ssh" accept
```

```
28/02-23:14:12.986940  [**] [1:19910316:1] Alguien esta haciendo ping [**] [Pri
ority: 0] {ICMP} 192.168.1.138 -> 192.168.1.148
```

CONLUSIONES

- ✓ Se realizó una investigación exhaustiva sobre los mecanismos y herramientas disponibles para garantizar la seguridad de los servidores de datos. Se concluyó que la instalación y uso conjunto de Snort y Fail2Ban en el servidor de la DTIC en Quito constituye una estrategia integral y efectiva para este propósito.
- ✓ A través de la investigación, se optó por Snort y Fail2Ban para fortalecer la seguridad del servidor. Se implementó FirewallD para controlar el tráfico de red y se crearon grupos de usuarios para una gestión eficiente de recursos y acceso a la red. Snort detecta y alerta sobre actividades maliciosas, mientras que Fail2Ban bloquea automáticamente direcciones IP sospechosas, reduciendo el riesgo de intrusiones no autorizadas y protegiendo la integridad de los datos almacenados.

CONLUSIONES

- ✓ Se realizaron pruebas para evaluar la eficacia de los mecanismos de seguridad durante el proceso de endurecimiento. Además, se desarrolló un manual de usuario detallado para orientar sobre la configuración, uso y mantenimiento de estos mecanismos. Esto asegura que el personal esté capacitado para utilizar eficazmente las medidas de seguridad implementadas y garantiza su correcto funcionamiento continuo.

RECOMENDACIONES

- ✓ Durante el proceso de endurecimiento, es esencial documentar cada paso para la reconfiguración en futuras modificaciones.
- ✓ Antes de implementar los mecanismos de seguridad en producción, se recomienda realizar pruebas en ambientes seguros para evaluar su rendimiento.
- ✓ Es fundamental utilizar fuentes confiables al analizar los mecanismos de seguridad para garantizar su eficacia.

GRACIAS