UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIOIN, FINANZAS E INFORMATICA

PROCESO DE TITULACIÓN

NOVIEMBRE 2023 – MARZO 2024

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTECIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

Los ataques informáticos y su incidencia en la seguridad de los servidores con sistemas operativos open source en la Universidad Técnica de Babahoyo

ESTUDIANTE:

CALERO ESPINOZA KLEYNER JAVIER

TUTOR:

ING. FABIAN EDUARDO ALCOSER CANTUÑA

AÑO 2024

ÍNDICE

Tabla de ilustraciones 4

Resumen 1

Abstract 1

Planteamiento Del Problema. 1

Justificación. 2

Objetivos Del Estudio. 3

Objetivo General. 3

Objetivos Específicos 3

Líneas De Investigación. 4

Marco Conceptual. 5

Redes 5

Servidores 5

Internet 5

Ataques informáticos 6

Seguridad informática 7

Sistemas operativos open source 7

Marco Metodológico. 15

Resultados. 22

Resultados de encuestas 22

Resultados de entrevista 28

Resultados del análisis de los servidores 29

Discusión De Resultados. 33

Conclusiones. 35

Recomendaciones. 36

Referencias 37

ANEXOS 38

Tabla de ilustraciones

ILUSTRACIÓN 1 SERVIDOR APACHE 8

ILUSTRACIÓN 2 SERVIDOR NGINX 8

ILUSTRACIÓN 3 POSTFIX 9

ILUSTRACIÓN 4 DOVECOT 9

ILUSTRACIÓN 5 TOMCAT 9

ILUSTRACIÓN 6 WILDFLY 9

ILUSTRACIÓN 7 MYSQL 10

ILUSTRACIÓN 8 POSTGRESQL 10

ILUSTRACIÓN 9 NEXTCLOUD 11

ILUSTRACIÓN 10 OWNCLOUD 11

ILUSTRACIÓN 11 NAGIOS 12

ILUSTRACIÓN 12 PROMETHEUS 12

ILUSTRACIÓN 13 ANSIBLE 13

ILUSTRACIÓN 14 PUPPET 13

ILUSTRACIÓN 15 MOODLE 13

ILUSTRACIÓN 16 OPEN EDX 14

ILUSTRACIÓN 17. ESCANEO DE LA IP DE LOS SERVIDORES. 30

ILUSTRACIÓN 18. ESCANEO DE VULNERABILIDADES CON NMAP. 30

ILUSTRACIÓN 19. ESCANEO REMOTO DE VULNERABILIDADES CON LYNIS 31

ILUSTRACIÓN 20. REVISIÓN DE VULNERABILIDADES CON OWASPZAP. 31

ILUSTRACIÓN 21. RESULTADO DE LAS VULNERABILIDADES. 32

ILUSTRACIÓN 24 EJECUCIÓN DEL ANÁLISIS DE VULNERABILIDADES 32

Resumen

El presente estudio tiene como objetivo examinar el patrón de ataques cibernéticos a la seguridad de servidores utilizando sistemas operativos de código abierto en la Universidad Técnica de Babahoyo (UTB). El objetivo principal es identificar las vulnerabilidades que no se han controlado en estos sistemas y su impacto en la seguridad de la información institucional. El trabajo investigado se centra en un contexto académico, donde la Universidad Tecnológica de Babahoyo sirve como instancia para evaluar ataques como malware, phishing y ransomware que afectan la integridad y confidencialidad de los datos institucionales. Se espera que el presente estudio sea beneficioso para las instituciones educativas y técnicas de Ecuador, ya que aporta una perspectiva indígena al cuerpo internacional de conocimientos. Los hallazgos obtenidos no sólo aumentarán el nivel de seguridad en la Universidad Tecnológica de Babahoyo, sino que probablemente se replicarán en otras escuelas de la región. El trabajo no solo contribuye a los estudios sobre ciberseguridad en entornos universitarios, sino que también presenta sugerencias prácticas para mejorar las configuraciones de seguridad en servidores de código abierto y, en consecuencia, proteger a las instituciones de educación superior contra riesgos cibernéticos dentro y fuera de la Universidad Tecnológica de Babahoyo.

Palabras Claves: ciberseguridad, opensource, servidores, seguridad, sistemas, universidad, firewall.

Abstract

The present study aims to examine the pattern of cyber attacks on server security using open source operating systems at the Technical University of Babahoyo (UTB). The main objective is to identify the vulnerabilities that have not been controlled in these systems and their impact on the security of institutional information. The work investigated focuses on an academic context, where the Babahoyo Technological University serves as an instance to evaluate attacks such as malware, phishing and ransomware that affect the integrity and confidentiality of institutional data. It is expected that the present study will be beneficial to educational and technical institutions in Ecuador, as it contributes an indigenous perspective to the international body of knowledge. The findings obtained will not only increase the level of security at the Babahoyo Technological University, but will probably be replicated in other schools in the region. The work not only contributes to studies on cybersecurity in university environments, but also presents practical suggestions to improve security configurations on open source servers and, consequently, protect higher education institutions against cyber risks inside and outside the Technological University of Babahoyo.

Keywords: cybersecurity, opensource, servers, security, systems, university, firewall.

Planteamiento Del Problema.

En el panorama actual, salvaguardar los sistemas informáticos se vuelve primordial ante la amenaza constante de ciberataques. Desde el malware hasta el phishing y el ransomware, diversos vectores maliciosos acechan, poniendo en riesgo instituciones vitales como la Universidad Técnica de Babahoyo. La integridad de su reputación, la prevención de posibles sanciones económicas y la continuidad sin interrupciones de sus funciones, reposan en la protección de datos sensibles, incluyendo registros estudiantiles, investigaciones y documentos financieros. La universidad debe responder con prontitud a esta situación y tomar medidas para salvaguardar sus servidores. Estos pasos incluyen un análisis de las amenazas, el diseño y aplicación de medidas de protección que sean efectivas, pero también lo suficientemente flexibles para hacer frente a los riesgos emergentes, y capacitar a los profesores y al personal en conciencia y prácticas de ciberseguridad. Es importante enfatizar que la seguridad de la tecnología de la información no es un proceso estático sino un proceso en evolución en respuesta a amenazas y desafíos cambiantes. Se hace evidente que se necesitan inversiones en recursos humanos y técnicos para garantizar la confidencialidad de documentos importantes y la plena funcionalidad de los sistemas informáticos. Todas las personas de esta universidad también pueden ayudar a mantener seguras sus computadoras, ya que tienen la responsabilidad. Se requerirán precauciones de seguridad por parte de cada usuario de los sistemas informáticos de la universidad para que la información conserve su integridad.

Justificación.

La seguridad informática ha emergido como un tema crítico, y comprender cómo los ataques informáticos afectan a los servidores con sistemas operativos de código abierto es esencial, especialmente en entornos académicos como una universidad. Los sistemas operativos de código abierto son cada vez más populares debido a su accesibilidad, costos reducidos y flexibilidad, lo que intensifica la importancia de evaluar su seguridad contra amenazas cibernéticas. La elección específica de la Universidad Técnica de Babahoyo como objeto de estudio proporciona un enfoque práctico y aplicado, permitiendo analizar de manera detallada cómo las características particulares de la institución inciden en la seguridad de sus servidores que utilizan sistemas operativos de código abierto.

Esta investigación encuentra justificación en su potencial contribución al conocimiento local. Se espera que la investigación ofrezca perspectivas valiosas para la comunidad académica y técnica local, así como para otras instituciones similares en la región. Además, la elección de un enfoque preventivo y proactivo proporciona la oportunidad de desarrollar estrategias concretas para fortalecer la seguridad informática, adaptadas a la realidad local. La importancia de la ciberseguridad en la educación superior aumenta la relevancia del estudio ya que las instituciones educativas almacenan información sensible que necesita ser protegida. Abordar los problemas de ciberseguridad en este contexto puede ayudar a crear un entorno educativo más seguro al aumentar la confianza en la integridad de los datos académicos y personales de los estudiantes y profesores.

.

Objetivos Del Estudio.

Objetivo General.

Analizar la incidencia y características de los ataques informáticos dirigidos a los servidores con sistemas operativos de código abierto en la Universidad Técnica de Babahoyo.

Objetivos Específicos.

- Identificar las vulnerabilidades de los sistemas operativos de código abierto que pueden ser explotadas por los atacantes.
- Evaluar el impacto de los ataques informáticos en la universidad, en términos de daños a la información, interrupciones en el servicio y costos económicos.
- Evaluar la eficacia de las medidas de seguridad existentes en los servidores con sistemas operativos de código abierto.

Líneas De Investigación.

Línea: Sistemas de información y comunicación, emprendimiento e innovación.

Esta línea de investigación proporciona una plataforma óptima para la creación de soluciones tecnológicas innovadoras, el fortalecimiento de la competitividad, el estímulo al emprendimiento y la promoción de una cultura arraigada en la innovación.

Sublínea: Redes y tecnologías inteligentes de software y hardware.

La sublínea de Redes y tecnologías inteligentes de software y hardware ofrece una gran oportunidad para la investigación en el ámbito de las TIC. Los resultados derivados de esta investigación tienen el potencial de generar un impacto positivo en la sociedad, contribuyendo al desarrollo de soluciones innovadoras que no solo incrementen la competitividad empresarial, sino que también impulsen iniciativas emprendedoras y fomenten la cultura de la innovación.

Marco Conceptual.

Redes

Las redes, en su naturaleza abierta y flexible, se erigen como infraestructuras fundamentales que posibilitan la interconexión fluida entre diversos nodos. Su esencia radica en la habilidad de distribuir recursos, compartir información y equilibrar el poder de manera dinámica. Este entramado de conexiones no solo facilita la comunicación y el intercambio de datos, sino que también fomenta la colaboración y la cooperación entre individuos y entidades, configurando un tejido interdependiente que impulsa el progreso y la innovación en múltiples ámbitos de la sociedad y la tecnología (Castells & Muñoz de Bustillo, 2006).

Servidores

Los servidores se conocen computadores conectados al internet donde se almacenan datos para su posterior uso. Esta interacción es factible a través de una red, de modo que la comunicación entre el servidor y los clientes se vuelva más eficiente. Es decir, los servidores son el foco de cualquier ambiente informático distribuido a gran escala porque sirven como nodos centrales y facilitan el acceso a recursos compartidos, desempeñando así un papel crucial para garantizar el funcionamiento eficaz y fluido de dichos entornos. (Stallings, 2004)

Internet

Internet es como una enorme red informática que conecta a miles de millones de dispositivos en todo el mundo. Imagina que es como una autopista gigante que permite que la información viaje de un lugar a otro de manera rápida y eficiente. Es como un sistema de tuberías que transporta datos de un lugar a otro. Internet también nos permite acceder a una gran cantidad de información y recursos. Puedes pensar en Internet como una enorme biblioteca virtual donde

puedes encontrar libros, artículos, videos y todo tipo de contenido. Es como tener acceso a un enorme almacén de conocimientos al alcance de nuestros dedos. (Tanenbaum & Wetherall, 2012).

Ataques informáticos

Un ataque informático se define como un acto intencional diseñado para comprometer la seguridad de un sistema o red informática con la intención de obtener acceso no autorizado, manipular, destruir datos o interferir con el funcionamiento adecuado del sistema. Estas acciones suelen realizarse mediante una variedad de técnicas y tácticas, como explotar vulnerabilidades de software, utilizar malware, ingeniería social o realizar ataques de fuerza bruta. El objetivo final de los ataques informáticos puede variar, desde el robo de información confidencial hasta la paralización de servicios críticos. La ciberseguridad juega un papel crucial en la prevención y mitigación de estos ataques, implementando medidas para fortalecer la resistencia de los sistemas y redes ante posibles amenazas digitales. (National Institute of Standards and Technology (NIST), 2023)

Tipos de ataques informáticos

- **Malware:** Software malicioso que puede infectar un sistema informático y causar daño. Algunos tipos de malware son virus, troyanos, gusanos y ransomware (SANS Institute, 2023)
- **Phishing:** Suplantación de identidad de una fuente legítima para engañar a los usuarios y obtener información personal o financiera (SANS Institute, 2023)
- **Denegación de servicio (DoS):** Ataque que busca sobrecargar un sistema o red con tráfico para hacerlo inoperable (SANS Institute, 2023)
- **SQL injection:** Inyección de código SQL malicioso en una aplicación web para acceder a datos no autorizados (SANS Institute, 2023)
- **Cross-site scripting (XSS):** Inyección de código JavaScript malicioso en una página web para atacar a usuarios que la visitan (SANS Institute, 2023)
- **Ataques de fuerza bruta:** Intentos repetidos de adivinar una contraseña o clave de seguridad ((SANS Institute, 2023)

Seguridad informática

La seguridad informática es la disciplina que se encarga de proteger los sistemas informáticos y redes de ataques y vulnerabilidades (National Institute of Standards and Technology (NIST), 2023)

Medidas de seguridad informática

- **Firewall:** Barrera de seguridad que controla el tráfico de red entrante y saliente (National Institute of Standards and Technology (NIST), 2023)
- **Antivirus:** Software que detecta y elimina malware (National Institute of Standards and Technology (NIST), 2023).
- **Actualizaciones de software:** Parches de seguridad que corrigen vulnerabilidades en el software (National Institute of Standards and Technology (NIST), 2023)
- **Copias de seguridad:** Respaldo de datos para restaurarlos en caso de un ataque o fallo del sistema (National Institute of Standards and Technology (NIST), 2023)
- **Control de acceso:** Restricción del acceso a recursos informáticos a usuarios autorizados (NIST, 2023).
- **Cifrado de datos:** Codificación de datos para que solo puedan ser leídos por usuarios autorizados (NIST, 2023).

Sistemas operativos open source

Los sistemas operativos open source son aquellos cuyo código fuente está disponible públicamente para que cualquiera pueda modificarlo y distribuirlo (Open Source Initiative., 2023) Algunos ejemplos populares de sistemas operativos open source son Linux, FreeBSD y OpenBSD.

Ventajas de los sistemas operativos open source

- **Seguridad:** La comunidad de usuarios puede revisar y mejorar el código fuente, lo que puede ayudar a identificar y corregir vulnerabilidades de seguridad (Open Source Initiative., 2023)
- **Flexibilidad:** El código fuente puede ser modificado para adaptarlo a las necesidades específicas de cada usuario (Open Source Initiative., 2023)
- **Costo:** La mayoría de los sistemas operativos open source son gratuitos (Open Source Initiative., 2023)

Desventajas de los sistemas operativos open source

- **Soporte:** No siempre hay soporte técnico oficial disponible (Open Source Initiative., 2023).
- **Compatibilidad:** No todo el software es compatible con sistemas operativos open source (Open Source Initiative., 2023)
- **Curva de aprendizaje:** Se requiere un mayor conocimiento técnico para usar y administrar sistemas operativos open source (Open Source Initiative., 2023)

Ejemplos de servidores opensource

Servidor web:

- **Apache:** Es el servidor web más popular del mundo, conocido por su estabilidad, seguridad y rendimiento. Es ideal para alojar sitios web estáticos y dinámicos, aplicaciones web y portales. (Apache Software Foundation, 2023)

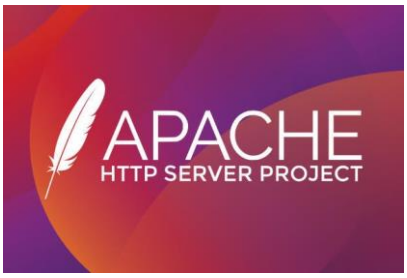


Ilustración 1 Servidor Apache

Obtenido de: https://www.openlogic.com/blog/apache-http-server

- **Nginx:** Se caracteriza por su alta velocidad, eficiencia y escalabilidad. Es una excelente opción para sitios web con alto tráfico y aplicaciones web que requieren un alto rendimiento. (Nginx, Inc., 2023)

Ilustración 2 Servidor NGINX

Obtenido de: https://extassisnetwork.com/tutoriales/comandos-de-nginx/

Servidor de correo electrónico:

- **Postfix:** Es un servidor de correo electrónico robusto, flexible y seguro. Ofrece una amplia gama de funcionalidades y es compatible con diferentes plataformas. (The Postfix Team, 2023)

Ilustración 3 POSTFIX

Obtenido de: https://medium.com/yavar/send-mail-using-postfix-server-bbb08331d39d

- **Dovecot:** Es un servidor de correo electrónico IMAP/POP3 ligero y eficiente. Se integra fácilmente con otros software y ofrece una buena experiencia de usuario. (Dovecot IMAP and POP3 server, 2023)

Ilustración 4 Dovecot

Obtenido de: https://www.dovecot.org

Servidor de aplicaciones:

- **Tomcat:** Es un contenedor de servlets y JSPs muy popular. Es compatible con diferentes plataformas y ofrece un alto rendimiento. (Apache Tomcat, 2023)

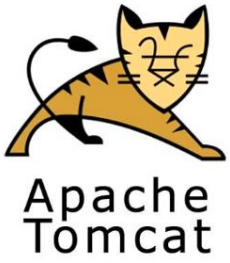


Ilustración 5 TOMCAT

Obtenido de: https://www.simplilearn.com/what-is-tomcat-article

- **WildFly:** Es un servidor de aplicaciones Java EE completo y flexible. Es compatible con diferentes plataformas y ofrece una amplia gama de funcionalidades. (WildFly, 2023)

Ilustración 6 WildFly

Obtenido de: https://www.ochobitshacenunbyte.com/2018/10/17/instalar-wildfly-en-centos-7/

Servidor de bases de datos:

- **MySQL:** Es un sistema de gestión de bases de datos relacionales muy popular. Es gratuito, de código abierto y ofrece un alto rendimiento. (MySQL, 2023)

Ilustración 7 MySQL

Obtenido de: https://blog.interfell.com/7-razones-para-elegir-mysql

- **PostgreSQL:** Es un sistema de gestión de bases de datos relacionales robusto, flexible y seguro. Es compatible con diferentes plataformas y ofrece una amplia gama de funcionalidades. (PostgreSQL Global Development Group, 2023)

Ilustración 8 PostgreSQL

Obtenido de: https://www.dongee.com/tutoriales/que-es-postgresql/

Servidor de almacenamiento en la nube:

- **Nextcloud:** Es una plataforma de colaboración y almacenamiento en la nube que ofrece una amplia gama de funcionalidades, como compartir archivos, sincronización de archivos, calendario, correo electrónico y más. (Nextcloud GmbH, 2023)

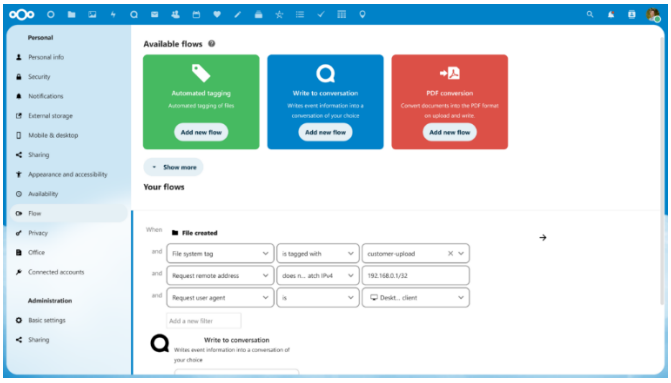


Ilustración 9 Nextcloud

Obtenido de: https://nextcloud.com/features/

- **OwnCloud:** Es una plataforma de colaboración y almacenamiento en la nube similar a Nextcloud. Ofrece una amplia gama de funcionalidades y es compatible con diferentes plataformas. (ownCloud GmbH, 2023)

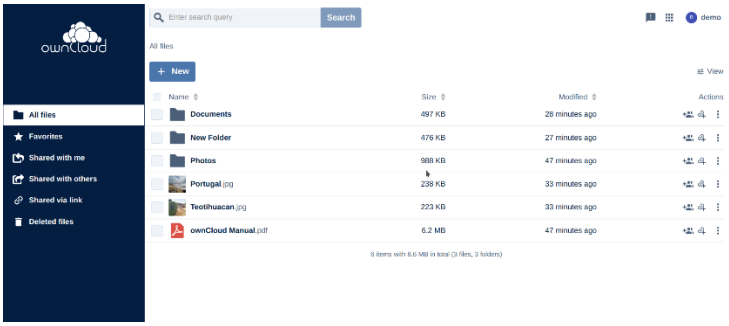


Ilustración 10 OwnCloud

Obtenido de: https://www.onlyoffice.com

Herramientas de monitorización:

- **Nagios:** Es una herramienta de monitorización de redes y servidores muy popular. Es gratuita, de código abierto y ofrece una amplia gama de funcionalidades. (Nagios Core Team, 2023)

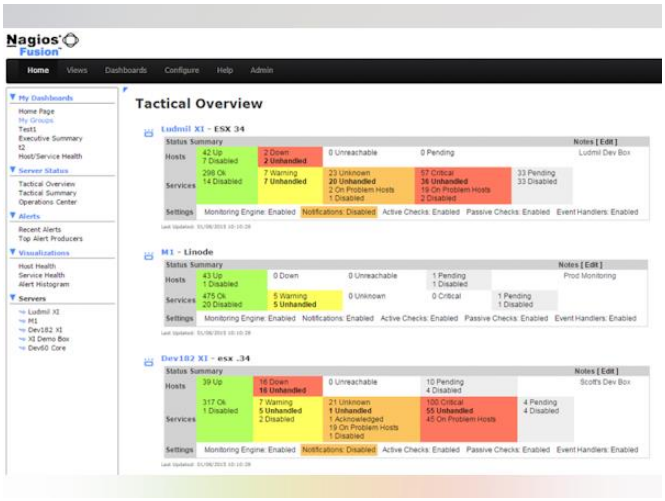


Ilustración 11 Nagios

Obtenido de: https://www.capterra.ec/software/152793/nagios-xi

- **Prometheus:** Es un sistema de monitorización de código abierto que ofrece una alta escalabilidad y flexibilidad. Es compatible con diferentes plataformas y ofrece una amplia gama de funcionalidades. (Prometheus, 2023)

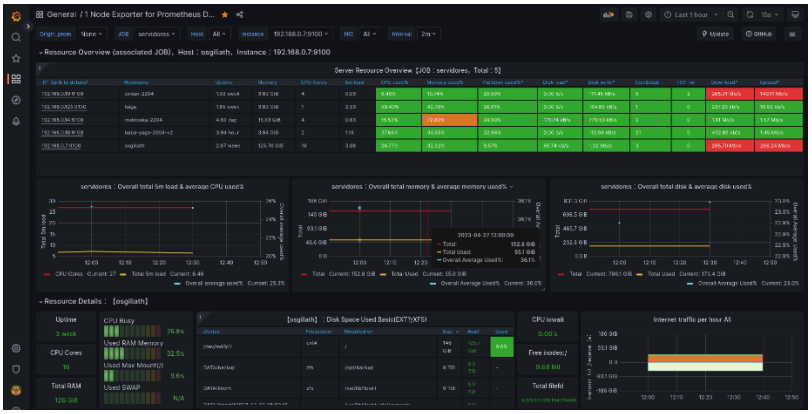


Ilustración 12 Prometheus

Obtenido de: https://elpuig.xeill.net/Members/vcarceler/articulos/monitorizacion-con-prometheus-y-grafana

Herramientas de gestión de configuración:

- **Ansible:** Es una herramienta de automatización de tareas que permite gestionar la configuración de servidores de forma centralizada. Es gratuita, de código abierto y ofrece una amplia gama de funcionalidades. (Ansible, 2023)

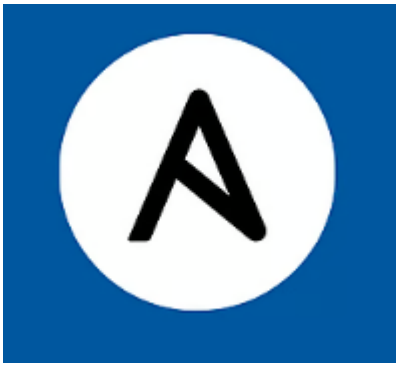


Ilustración 13 Ansible

Obtenido de: https://geekflare.com/es/connecting-windows-ansible-from-ubuntu/

- **Puppet:** Es una herramienta de gestión de configuración similar a Ansible. Es compatible con diferentes plataformas y ofrece una amplia gama de funcionalidades. (Puppet, 2023)

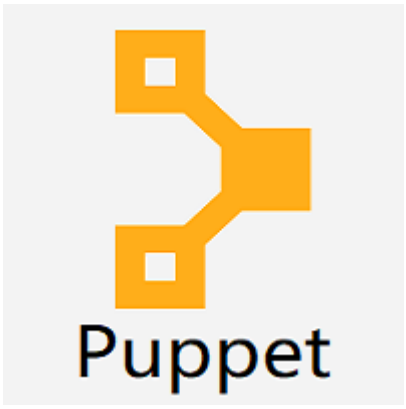


Ilustración 14 Puppet

Obtenido de: https://www.javatpoint.com/puppet

Plataformas de aprendizaje:

- **Moodle:** Es una plataforma de aprendizaje virtual (LMS) muy popular. Es gratuita, de código abierto y ofrece una amplia gama de funcionalidades. (Moodle, 2023)

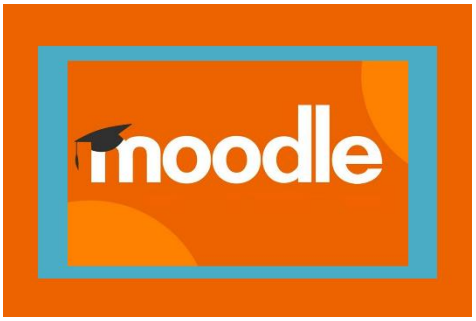


Ilustración 15 Moodle

Obtenido de: https://eiformacion.com/cuales-son-las-ventajas-de-moodle/

- **Open edX:** Es una plataforma de aprendizaje virtual similar a Moodle. Es compatible con diferentes plataformas y ofrece una amplia gama de funcionalidades. (Open edX, 2023)

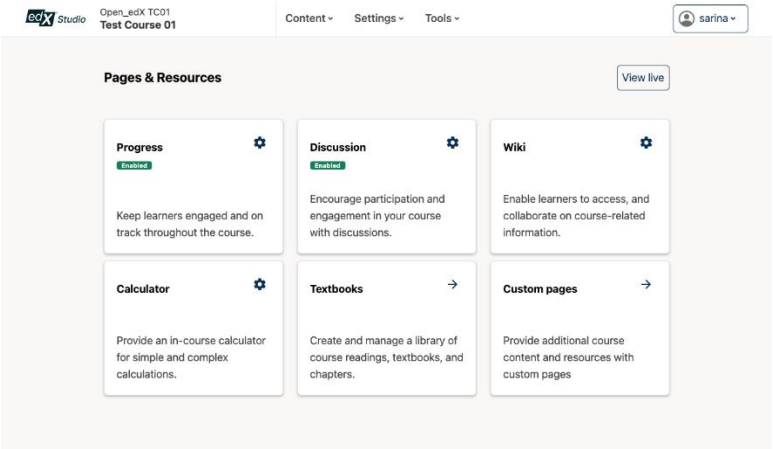


Ilustración 16 Open edX

Obtenido de: https://openedx.org/es/blog/configuring-3rd-party-discussion-experiences/

Marco Metodológico.

El marco metodológico define el enfoque y las estrategias que se utilizarán para realizar la investigación. En esta línea de investigación, se pueden utilizar diferentes marcos metodológicos, como:

- **Enfoque cuantitativo:** Medir la incidencia de los ataques informáticos en los servidores con sistemas operativos open source en la Universidad Técnica de Babahoyo.
- **Enfoque cualitativo:** Comprender las experiencias y percepciones de los administradores de servidores sobre los ataques informáticos y la seguridad de los sistemas operativos open source.
- **Enfoque mixto:** Combinar el análisis cuantitativo y cualitativo para obtener una visión más completa de la incidencia de los ataques informáticos en la Universidad Técnica de Babahoyo.

Técnicas:

Las técnicas son las herramientas que se utilizan para recolectar datos. Algunas de las técnicas que se pueden utilizar en esta línea de investigación son.

- **Entrevistas:** Profundizar en las experiencias y opiniones de los administradores de servidores sobre los ataques informáticos y la seguridad de los sistemas operativos open source.
- **Encuesta:** Obtener información sobre la frecuencia, tipos y consecuencias de los ataques informáticos sufridos por los servidores con sistemas operativos open source en la Universidad Técnica de Babahoyo.

Para llevar a cabo la práctica de la investigación en seguridad informática con un enfoque en servidores con sistemas operativos open source en la Universidad Técnica de Babahoyo, se utilizarán diversas herramientas especializadas. Estas herramientas incluirán:

- **OwasZap**: Se utilizará para realizar análisis de vulnerabilidades en los servidores, identificar posibles puntos débiles y evaluar la seguridad general de los sistemas operativos open source.
- **Metasploit**: Servirá como marco de desarrollo y ejecución de exploits, permitiendo simular ataques para evaluar la resistencia de los servidores ante posibles amenazas.
- **Wireshark**: Esta herramienta será empleada para el análisis de tráfico de red, facilitando la detección de posibles actividades maliciosas o anómalas en la comunicación entre los servidores y otras entidades de la red.
- **Autopsy**: Se utilizará para llevar a cabo análisis forense en caso de incidentes de seguridad, permitiendo la recuperación y examen de evidencia digital en los sistemas operativos open source.
- **Lynis**: Servirá como herramienta de auditoría de seguridad, analizando la configuración del sistema y proveyendo recomendaciones para mejorar la seguridad en servidores con sistemas operativos open source.

Instrumentos:

Los instrumentos son las herramientas que se utilizan para aplicar las técnicas de recolección de datos. Algunos de los instrumentos que se pueden utilizar en esta línea de investigación son:

1. Cuestionario de encuestas dirigidos a administradores de servidores y personal técnico de la universidad.

2. Guía de entrevista dirigida a el encargado del departamento de sistemas.

Cuestionario de preguntas de encuesta

1. ¿Considera usted que los servidores con sistemas operativos open source de la Universidad Técnica de Babahoyo han tenido ataques informáticos?

- Si
- No

2. ¿Qué tipos de ataques informáticos diría que son los más comunes en estos servidores?

(Marque todas las opciones que apliquen)

- Malware
- Phishing
- Denegación de servicio (DoS)
- SQL injection
- Cross-site scripting (XSS)
- Ataques de fuerza bruta

3. ¿En qué medida diría que los ataques informáticos han impactado en la Universidad Técnica de Babahoyo?

- Impacto grave
- Impacto muy grave
- Impacto moderado
- No ha habido impacto
- Impacto leve

4. ¿Qué medidas de seguridad diría que se implementan actualmente en los servidores con sistemas operativos open source de la universidad?

(Marque todas las opciones que apliquen)

- Firewall
- Antivirus
- Actualizaciones de software
- Copias de seguridad
- Control de acceso
- Cifrado de datos

5. ¿En qué nivel cree que las medidas de seguridad actuales son efectivas para prevenir y mitigar los ataques informáticos?

- Efectivas
- Muy efectivas
- No son efectivas
- Poco efectivas
- No son efectivas

6. ¿Qué dificultades diría que enfrenta la universidad para mejorar la seguridad de los servidores con sistemas operativos open source?

(Marque todas las opciones que apliquen)

- Falta de recursos financieros
- Falta de personal capacitado
- Falta de conocimiento técnico
- Falta de políticas de seguridad
- Falta de herramientas adecuadas

7. ¿Qué necesidades diría que tiene la universidad para mejorar la seguridad de los servidores con sistemas operativos open source?

(Marque todas las opciones que apliquen)

- Capacitación del personal
- Implementación de nuevas medidas de seguridad
- Actualización de hardware y software
- Desarrollo de políticas de seguridad
- Adquisición de herramientas de seguridad

8. ¿En qué medida diría que está satisfecho con la seguridad actual de los servidores con sistemas operativos open source de la universidad?

- No estoy satisfecho
- Poco satisfecho
- Satisfecho
- Muy satisfecho

9. ¿Qué recomendaciones diría que tiene para mejorar la seguridad de los servidores con sistemas operativos open source de la universidad?

---

10. ¿Existe la disponibilidad financiera de la autoridad para aplicar seguridad en los servidores opensource de la Universidad Técnica de Babahoyo?

- Si
- No

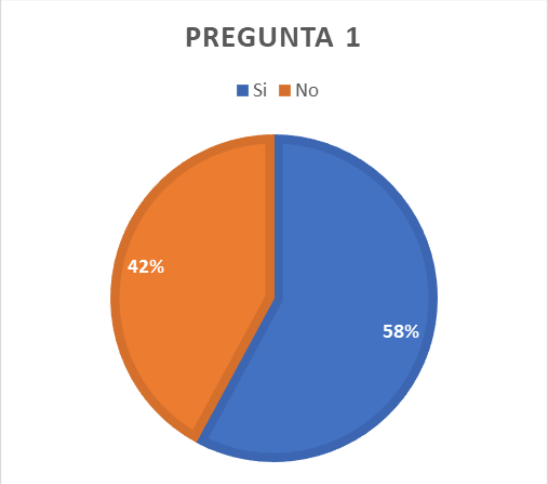
Guía de entrevista

- **¿En su experiencia, cuáles diría que son los tipos de ataques informáticos más comunes que sufren los servidores con sistemas operativos open source en la Universidad Técnica de Babahoyo?**
- **¿Qué medidas de seguridad se implementan actualmente para proteger estos servidores? ¿Considera que estas medidas son suficientes? ¿Por qué?**
- **¿Cuáles diría que son los principales desafíos que enfrenta la universidad para mejorar la seguridad de sus servidores con sistemas operativos open source?**
- **¿Qué recomendaciones o sugerencias tiene para mejorar la seguridad de estos servidores en la universidad?**
- **¿Qué herramientas o recursos utiliza para mantenerse actualizado sobre las últimas amenazas y vulnerabilidades de seguridad?**
- **¿Qué tipo de capacitación en seguridad informática recibe el personal que administra los servidores?**

Resultados.

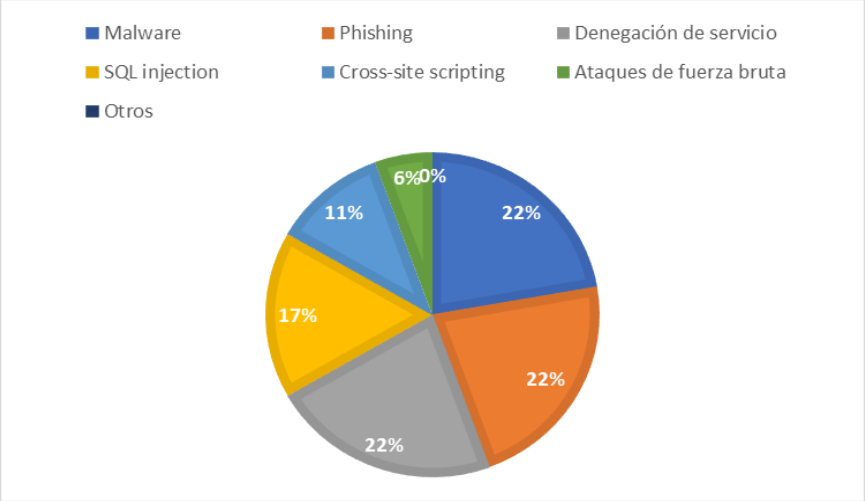
Resultados de encuestas

1. **¿Considera usted que los servidores con sistemas operativos open source de la Universidad Técnica de Babahoyo han tenido ataques informáticos?**



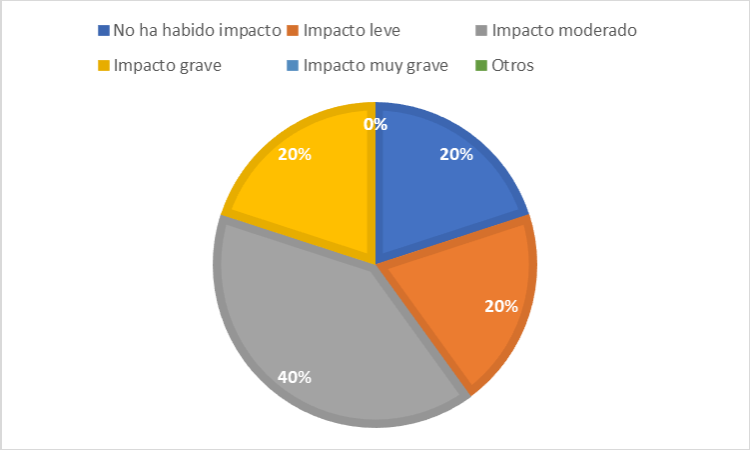
El 58% de los encuestados confirmó haber experimentado ataques, en contraste con el 42% que negó esta posibilidad. La notable predominancia de respuestas afirmativas refleja una percepción extendida sobre la incidencia de ataques informáticos en la universidad.

2. **¿Qué tipos de ataques informáticos diría que son los más comunes en estos servidores?**



Se observa que los tipos de ataques más comunes según la percepción de los encuestados son el malware, phishing y denegación de servicio seguidos por SQL injection con un 22% en los resultados de las encuestas. Otros tipos de ataques recibieron menor menciones, con porcentajes variables.

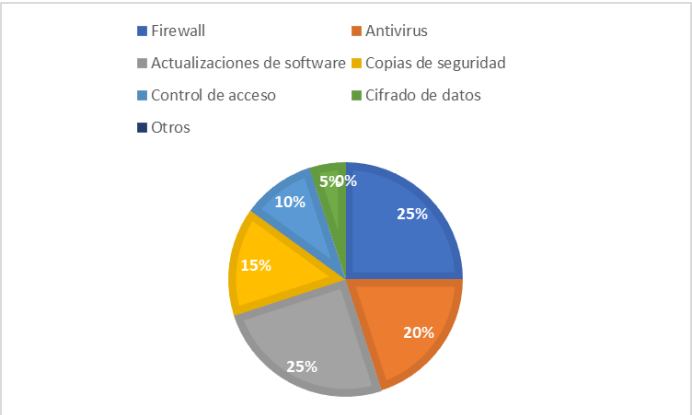
3. ¿En qué medida diría que los ataques informáticos han impactado en la Universidad Técnica de Babahoyo?



La encuesta revela que la mayoría de los encuestados (60%) consideran que los ataques informáticos han tenido un impacto significativo en la Universidad Técnica de Babahoyo. De ellos, el 40% indica un impacto grave, mientras que el 20% indica un impacto moderado.

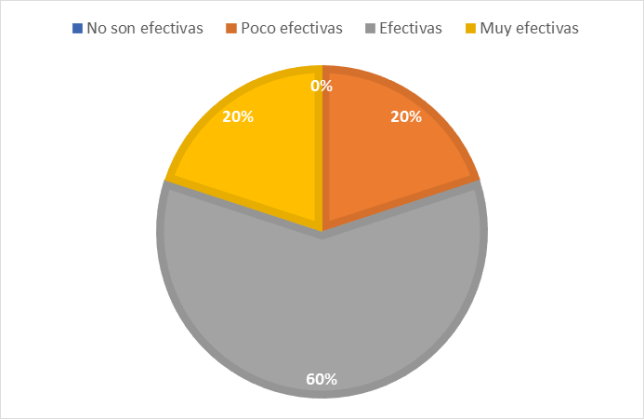
Es importante destacar que un 20% de los encuestados no percibe un impacto por parte de los ataques informáticos. Esto podría deberse a una falta de conocimiento sobre los eventos de seguridad informática o a que no se han visto directamente afectados.

4. ¿Qué medidas de seguridad diría que se implementan actualmente en los servidores con sistemas operativos open source de la universidad?



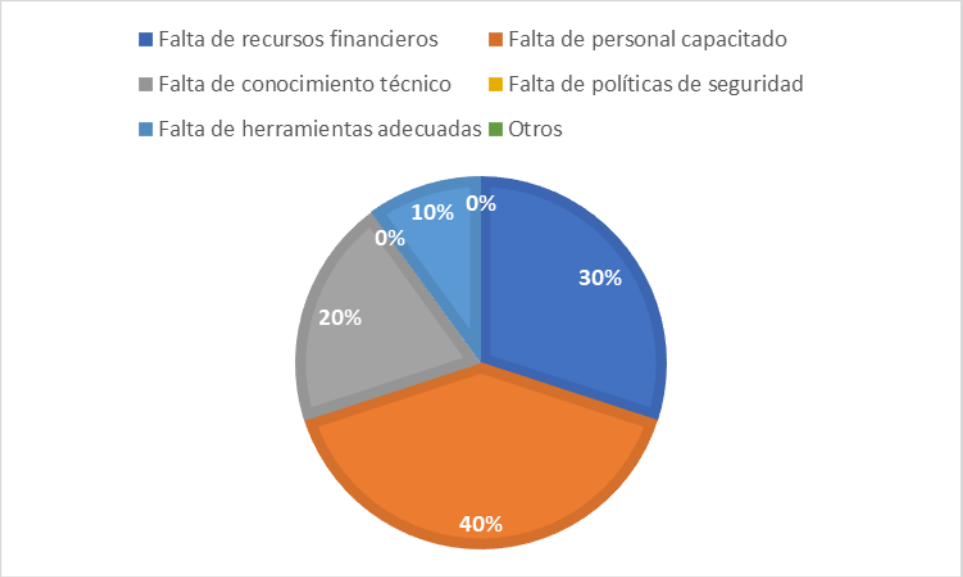
Los resultados revelan que las medidas de seguridad más frecuentemente empleadas en los servidores son el firewall y las actualizaciones de software, con un 25% de respuestas obtenidas en las encuestas. Estas son seguidas de cerca por el antivirus, con un 20%. Otros métodos, como las copias de seguridad (15%), el control de acceso (10%), y el cifrado de datos (5%), también fueron mencionados, aunque con menor frecuencia. Esto sugiere que si bien algunas medidas son más populares que otras, existe una diversidad en las estrategias de seguridad implementadas para proteger los servidores.

5. **¿En qué nivel cree que las medidas de seguridad actuales son efectivas para prevenir y mitigar los ataques informáticos?**



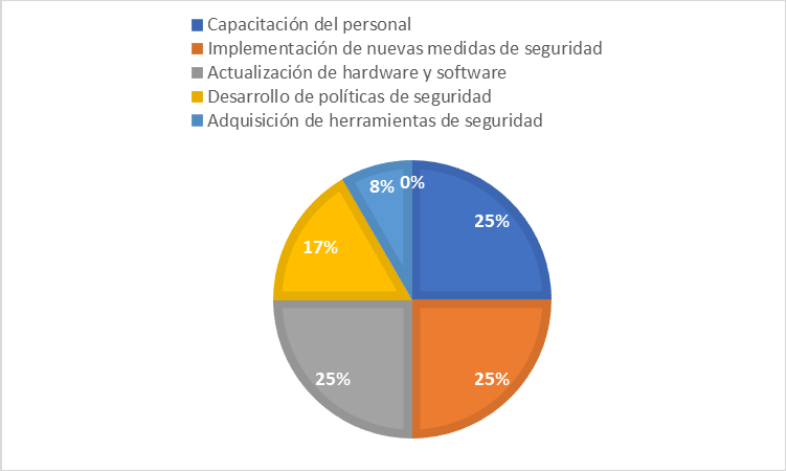
Los resultados indican una percepción mayoritariamente positiva sobre la efectividad de las medidas de seguridad actuales, con un 60% de los encuestados considerándolas efectivas y un 20% calificándolas como muy efectivas. Sin embargo, un 20% de los participantes también las percibe como poco efectivas. Este balance sugiere una evaluación diversa de la eficacia de las medidas de seguridad, destacando la necesidad de revisión y mejora continua para fortalecer aún más la resistencia contra posibles amenazas cibernéticas.

6. **¿Qué dificultades diría que enfrenta la universidad para mejorar la seguridad de los servidores con sistemas operativos open source?**



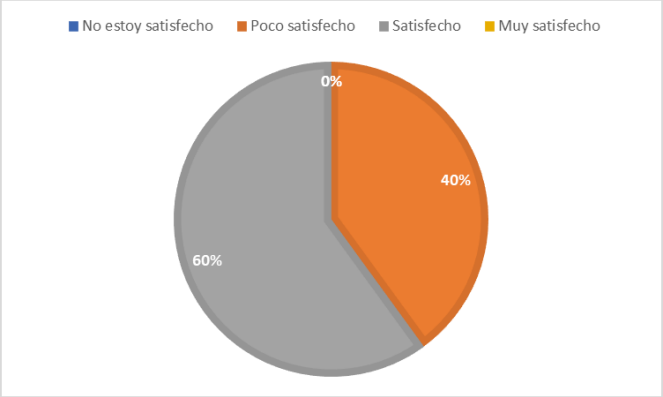
Los resultados resaltan que la carencia de personal capacitado es la dificultad más frecuentemente mencionada, con un 40% de los encuestados identificándola como un obstáculo. La limitación de recursos financieros también se presenta como un desafío significativo, obteniendo un 30% de menciones. Otras complicaciones, como la falta de conocimiento técnico, la ausencia de políticas de seguridad y la carencia de herramientas adecuadas, fueron señaladas en menor proporción. Este análisis subraya la importancia de abordar la capacitación del personal y la asignación de recursos financieros como aspectos cruciales para mejorar la seguridad de los servidores basados en sistemas operativos de código abierto.

7. ¿Qué necesidades diría que tiene la universidad para mejorar la seguridad de los servidores con sistemas operativos open source?



Los resultados obtenidos de la encuesta indican áreas clave que requieren atención para mejorar la seguridad de los servidores con sistemas operativos de código abierto en la Universidad Técnica de Babahoyo. En primer lugar, se destaca la necesidad urgente de capacitar al personal encargado de la administración de los servidores, ya que el 25% de los encuestados identificó la falta de conocimiento como un desafío significativo. Para fortalecer la seguridad, se sugiere la implementación de medidas adicionales, como un control de acceso más granular, el cifrado de datos y la adopción de sistemas de detección y prevención de intrusiones, con un respaldo del 25%. Además, mantener el hardware y software actualizado es imperativo, ya que el 25% de los participantes señaló la importancia de esta medida para corregir vulnerabilidades de seguridad conocidas. Asimismo, el desarrollo y la implementación de políticas de seguridad, junto con la realización de auditorías regulares y la adopción de un plan de respuesta a incidentes, fueron identificados como componentes críticos, sumando un 17%.

8. **¿En qué medida diría que está satisfecho con la seguridad actual de los servidores con sistemas operativos open source de la universidad?**



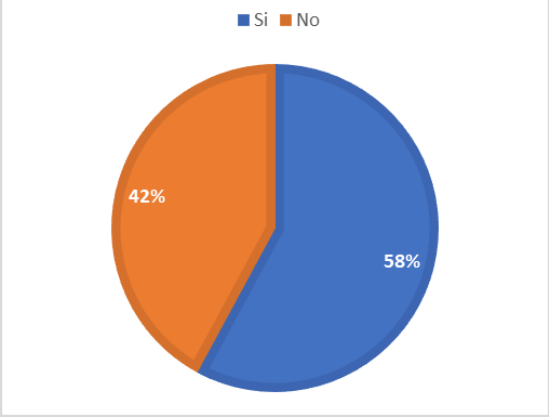
Los resultados indican que la mayoría de los encuestados (60%) se encuentra satisfecha con la seguridad actual de los servidores, mientras que un 40% se muestra poco satisfecho. No se registraron respuestas de "No estoy satisfecho" ni "Muy satisfecho". Este balance sugiere una evaluación generalmente positiva, pero también revela áreas de insatisfacción que podrían abordarse para mejorar la percepción global de la seguridad.

9. **¿Qué recomendaciones diría que tiene para mejorar la seguridad de los servidores con sistemas operativos open source de la universidad?**

Entre las recomendaciones más frecuentes se destacó la implementación de programas de concientización en seguridad informática para educar a estudiantes y personal, fortalecer la detección de intrusiones mediante sistemas avanzados de monitoreo, y colaborar con expertos externos para realizar auditorías de seguridad regulares. Asimismo, se subrayó la importancia de mejorar la gestión de parches y actualizaciones, desarrollar políticas de seguridad claras y comunicarlas eficientemente, así como fortalecer las medidas de control de acceso. También se sugirió la implementación de tecnologías de cifrado más robustas para proteger datos sensibles, y considerar la diversificación de la

infraestructura de servidores como medida para reducir la superficie de ataque. Estas recomendaciones reflejan la diversidad de enfoques que los participantes consideran esenciales para optimizar la seguridad de los servidores en el contexto universitario.

10. ¿Existe la disponibilidad financiera de la autoridad para aplicar seguridad en los servidores opensource de la Universidad Técnica de Babahoyo?



Según los resultados de la encuesta, el 58% de los encuestados indicaron que sí existe disponibilidad financiera por parte de la autoridad para aplicar seguridad en los servidores de código abierto de la Universidad Técnica de Babahoyo. Por otro lado, el 42% manifestó que no hay disponibilidad financiera para esta causa. Estos datos sugieren una división en las percepciones sobre la capacidad financiera para implementar medidas de seguridad en los servidores de la universidad.

Resultados de entrevista

Los resultados de la entrevista destacan diversos desafíos y estrategias relacionados con la seguridad de los servidores que utilizan sistemas operativos de código abierto en la Universidad Técnica de Babahoyo. En relación con los ataques informáticos más frecuentes, se mencionaron la suplantación, ataques DDoS y ataques al dominio. Respecto a las medidas de seguridad actuales, se subrayó la utilización de firewalls con sistemas de detección y prevención de intrusiones, aunque se señaló la carencia actual de licencias. Los principales desafíos identificados incluyen la limitada velocidad de soporte en comparación con sistemas licenciados y la dependencia de

comunidades externas para las actualizaciones de parches de seguridad. Las recomendaciones para mejorar la seguridad abogan por la implementación de licencias para los sistemas, la adopción de servidores de última generación y la utilización de firewalls más avanzados. Además, se destaca que el personal recibe capacitaciones anuales del proveedor de internet en este caso CEDIA, variando la frecuencia según las áreas de sistemas. Estos resultados resaltan la complejidad del panorama de seguridad y la importancia de abordar tanto las limitaciones actuales como las estrategias potenciales para fortalecer la seguridad de los servidores en la universidad.

Resultados del análisis de los servidores

En el transcurso de las prácticas realizadas, se llevaron a cabo diversas evaluaciones y escaneos en el entorno informático de la Universidad Técnica de Babahoyo. Estos procedimientos se centraron en examinar la configuración y la seguridad de los sistemas, abordando aspectos específicos como la resolución de nombres de dominio, la identificación de vulnerabilidades mediante el uso de scripts especializados, y la realización de auditorías remotas utilizando la herramienta Lynis. A continuación, se presentan los resultados detallados de estas prácticas, destacando los hallazgos significativos y proporcionando una visión integral de la postura de seguridad de los servidores con sistemas operativos de código abierto en la mencionada institución educativa.

Resultado de nslookup: La consulta de nslookup para el dominio sai.utb.edu.ec arrojó una respuesta no autoritativa, indicando que el servidor DNS utilizado (192.168.0.1) proporcionó información sobre la dirección IP asociada con el nombre de dominio. La dirección IP correspondiente es 190.15.129.133.

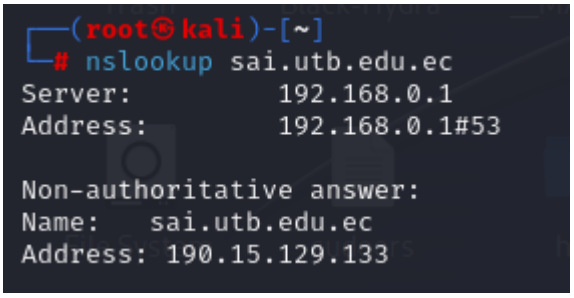


Ilustración 17. Escaneo de la IP de los servidores.

Resultado de nmap --script vulners: El escaneo realizado con Nmap y el script vulners en la dirección IP 190.15.129.133 revela que el puerto 53 (domain) está abierto y el servicio DNS está en ejecución. Asimismo, se encontró el puerto 443 (https) abierto, indicando la presencia de un servicio seguro. Sin embargo, el puerto 113 (ident) está cerrado. Además, 997 puertos TCP fueron filtrados y no se obtuvo respuesta. Estos resultados sugieren que el servidor tiene ciertas restricciones de firewall que limitan la visibilidad de los puertos.

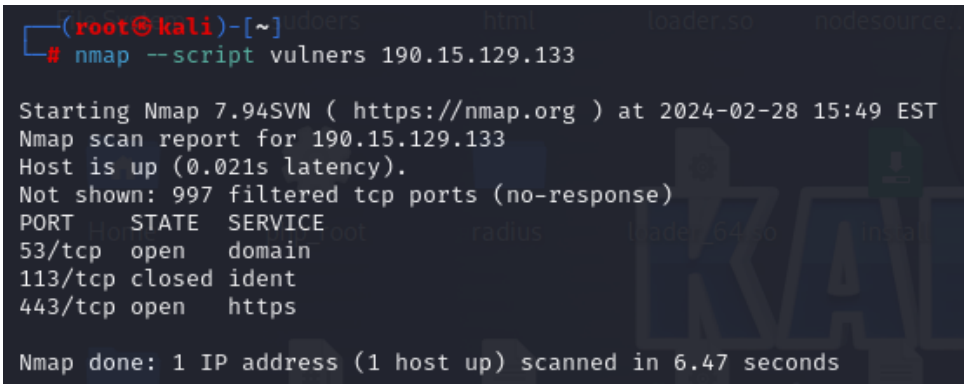


Ilustración 18. Escaneo de vulnerabilidades con Nmap.

Resultado de lynis audit system remoto: La ejecución del escaneo remoto con Lynis en la IP 190.15.129.133 involucra varios pasos. En primer lugar, se crea un archivo tarball conteniendo los archivos necesarios para el escaneo. Luego, este archivo se copia al servidor objetivo mediante SCP. Posteriormente, se ejecuta el comando de auditoría de Lynis en el servidor remoto. Finalmente, se limpian los archivos temporales y se recuperan los resultados del escaneo,

incluyendo el registro y el informe. Este enfoque proporciona una visión detallada del estado de seguridad del sistema remoto.

Ilustración 19. Escaneo remoto de vulnerabilidades con Lynis.

Una vez sabiendo dichas vulnerabilidades realizamos otro escaneo para poder ver más vulnerabilidades en los servicios alojados en estos servidores.

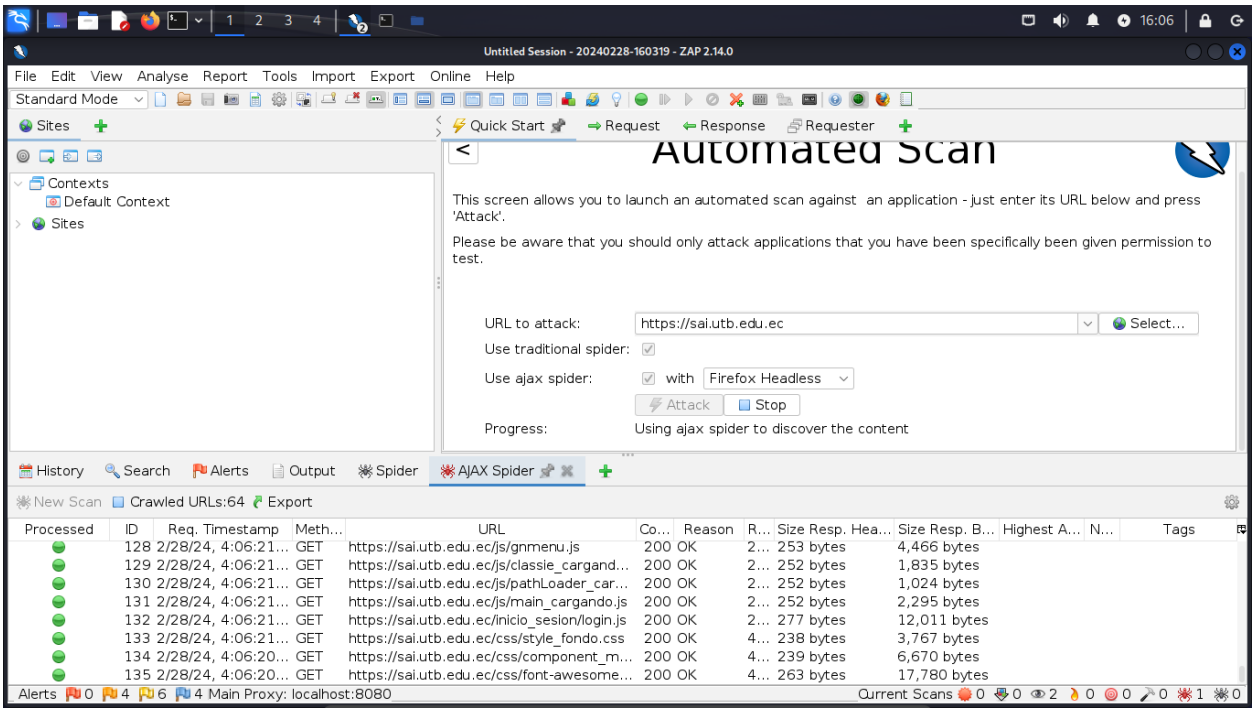


Ilustración 20. Revisión de vulnerabilidades con OwaspZap.

Se reciben alertas de posibles vulnerabilidades entre ellas de alto y medio riesgo.

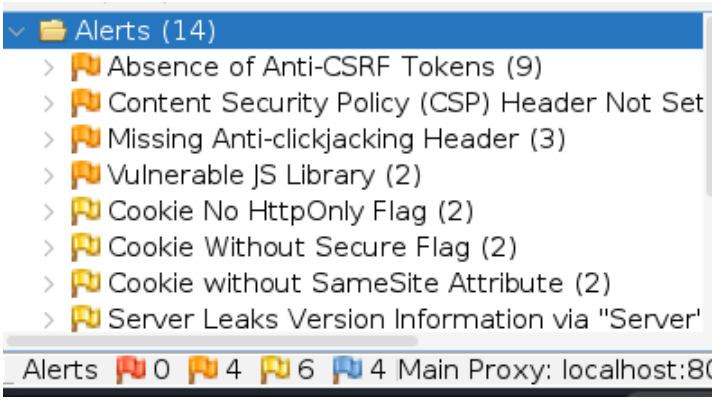


Ilustración 21. Resultado de las vulnerabilidades.

Descripción de las vulnerabilidades

- **Alto riesgo:**
    - **Ausencia de tokens anti-CSRF:** Permite a un atacante realizar acciones en nombre del usuario sin su consentimiento.
    - **Cabecera de la política de seguridad del contenido (CSP) no establecida:** Permite a un atacante inyectar código malicioso en la página web.
    - **Falta de encabezado anti-clickjacking:** Permite a un atacante superponer una página web falsa sobre la página web real para engañar al usuario.
- **Medio riesgo:**
    - **Biblioteca JS vulnerable:** Permite a un atacante ejecutar código arbitrario en el navegador del usuario.
    - **Cookie sin atributo samesite:** Permite a un atacante acceder a la cookie desde un sitio web diferente.
    - **Servidor que filtra información de la versión a través de "Servidor":** Permite a un atacante identificar el software del servidor y sus posibles vulnerabilidades.
    - **Cookie sin indicador de solo https:** Permite a un atacante interceptar la cookie en una conexión no segura.

Discusión De Resultados.

Los resultados obtenidos a través de la encuesta, entrevistas y análisis de los servidores en la Universidad Técnica de Babahoyo convergen para ofrecer una comprensión holística de la seguridad en los servidores con sistemas operativos de código abierto. La encuesta revela una prevalencia significativa de ataques informáticos, con el 58% de los encuestados reconociendo haber experimentado incidentes. Los tipos de ataques más comunes, como malware, phishing y denegación de servicio, ilustran la diversidad de riesgos a los que se enfrentan los servidores universitarios.

En términos de medidas de seguridad actuales, se observa una variedad de enfoques, siendo el firewall y las actualizaciones de software las más comunes. Sin embargo, se destaca la carencia de licencias en ciertas medidas, lo que plantea preocupaciones sobre la efectividad completa de las defensas implementadas. Los desafíos identificados, como la falta de personal capacitado y los recursos financieros limitados, se correlacionan con las dificultades destacadas en la entrevista, subrayando la necesidad de abordar estos obstáculos para mejorar la seguridad.

La evaluación de los servidores a través de nslookup, Nmap, OwasZAP y Lynis proporciona una visión técnica adicional. La presencia de vulnerabilidades de alto y medio riesgo, como la ausencia de tokens anti-CSRF y la falta de encabezados de seguridad, sugiere áreas críticas que requieren atención. El escaneo con Nmap revela una configuración específica de puertos y restricciones de firewall, mientras que el análisis de Lynis destaca vulnerabilidades potenciales en bibliotecas JS, cookies y filtrado de información de versión del servidor.

En conjunto, estos hallazgos resaltan la necesidad de un enfoque integrado para mejorar la seguridad. Las recomendaciones incluyen la implementación de licencias para medidas críticas, la

adopción de tecnologías avanzadas como firewalls más robustos, y la inversión en la capacitación continua del personal. La división de opiniones sobre la disponibilidad financiera sugiere la importancia de una gestión cuidadosa de los recursos para optimizar la seguridad.

Conclusiones.

- Se concluye que la Universidad Técnica de Babahoyo enfrenta una incidencia significativa de ataques informáticos, destacando la necesidad urgente de fortalecer las medidas de seguridad. La diversidad de ataques identificados subraya la importancia de implementar estrategias de seguridad multifacéticas, abordando tanto las vulnerabilidades técnicas como la concientización de los usuarios y las políticas de seguridad.
- La carencia de licencias en algunas medidas de seguridad y la división de opiniones sobre la disponibilidad financiera señalan áreas críticas para mejorar la inversión en recursos de seguridad, como la implementación de licencias y una gestión cuidadosa de los recursos financieros. La solicitud de equipos más avanzados y actualizados destaca la necesidad de modernizar la infraestructura tecnológica, crucial para mejorar la seguridad de los servidores con sistemas operativos de código abierto en la universidad.
- Los resultados muestran una alta incidencia de ataques informáticos, con un 58% de los encuestados reportando haber experimentado incidentes. La diversidad de los ataques, que van desde malware hasta denegación de servicio, subraya la necesidad de implementar medidas efectivas para salvaguardar la integridad y confidencialidad de los sistemas universitarios.
- La evaluación del software revela un enfoque integral para fortalecer la seguridad en servidores de código abierto. OwasZap y Lynis ofrecen análisis exhaustivos de vulnerabilidades y auditorías de seguridad, mientras que Metasploit simula ataques para probar la resistencia del sistema. Wireshark detecta actividades maliciosas en el tráfico de red, y Autopsy proporciona análisis forense en caso de incidentes, asegurando una respuesta completa ante posibles amenazas.

Recomendaciones.

- Se recomienda al Departamento de Tecnología de la Información establecer y mantener licencias actualizadas para todas las medidas de seguridad.
- Es recomendable para el Departamento de Recursos Humanos facilitar la formación continua del personal en prácticas de seguridad informática.
- En recomendación al Departamento Financiero, se sugiere asignar presupuestos específicos para la seguridad informática, priorizando la adquisición de licencias y la actualización de equipos.
- Se recomienda implementar un plan de respuesta a incidentes que incluya pasos claros y roles definidos en caso de ataques informáticos.

Referencias

Castells, Manuel., & Muñoz de Bustillo, Francisco. (2006). *La sociedad red : una visión global*. Alianza Editorial.

National Institute of Standards and Technology (NIST). (2023). *Cybersecurity Framework*. https://www.nist.gov/cyberframework.

Open Source Initiative. (2023). *What is Open Source?* . https://opensource.org/faq/.

SANS Institute. (2023). *SANS Top 25 Software Security Flaws*. https://www.sans.org/top25-software-errors/.

Stallings, W. (2004). *Comunicaciones y redes computadores* (7.ª ed.).

Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadoras*. Pearson Educación.

ANEXOS

Cuestionario de preguntas de encuesta

1. ¿Considera usted que los servidores con sistemas operativos open source de la Universidad Técnica de Babahoyo han tenido ataques informáticos?

- Si
- No

2. ¿Qué tipos de ataques informáticos diría que son los más comunes en estos servidores?

(Marque todas las opciones que apliquen)

- Malware
- Phishing
- Denegación de servicio (DoS)
- SQL injection
- Cross-site scripting (XSS)
- Ataques de fuerza bruta

3. ¿En qué medida diría que los ataques informáticos han impactado en la Universidad Técnica de Babahoyo?

- Impacto grave
- Impacto muy grave
- Impacto moderado
- No ha habido impacto
- Impacto leve

4. ¿Qué medidas de seguridad diría que se implementan actualmente en los servidores con sistemas operativos open source de la universidad?

(Marque todas las opciones que apliquen)

- Firewall
- Antivirus
- Actualizaciones de software
- Copias de seguridad
- Control de acceso

- Cifrado de datos

5. ¿En qué nivel cree que las medidas de seguridad actuales son efectivas para prevenir y mitigar los ataques informáticos?

- Efectivas
- Muy efectivas
- No son efectivas
- Poco efectivas
- No son efectivas

6. ¿Qué dificultades diría que enfrenta la universidad para mejorar la seguridad de los servidores con sistemas operativos open source?

(Marque todas las opciones que apliquen)

- Falta de recursos financieros
- Falta de personal capacitado
- Falta de conocimiento técnico
- Falta de políticas de seguridad
- Falta de herramientas adecuadas

7. ¿Qué necesidades diría que tiene la universidad para mejorar la seguridad de los servidores con sistemas operativos open source?

(Marque todas las opciones que apliquen)

- Capacitación del personal
- Implementación de nuevas medidas de seguridad
- Actualización de hardware y software
- Desarrollo de políticas de seguridad
- Adquisición de herramientas de seguridad

8. ¿En qué medida diría que está satisfecho con la seguridad actual de los servidores con sistemas operativos open source de la universidad?

- No estoy satisfecho
- Poco satisfecho
- Satisfecho
- Muy satisfecho

9. ¿Qué recomendaciones diría que tiene para mejorar la seguridad de los servidores con sistemas operativos open source de la universidad?

---

10. ¿Existe la disponibilidad financiera de la autoridad para aplicar seguridad en los servidores opensource de la Universidad Técnica de Babahoyo?

- Si
- No

Anexo 2

Guía de entrevista

- **¿En su experiencia, cuáles diría que son los tipos de ataques informáticos más comunes que sufren los servidores con sistemas operativos open source en la Universidad Técnica de Babahoyo?**
- **¿Qué medidas de seguridad se implementan actualmente para proteger estos servidores? ¿Considera que estas medidas son suficientes? ¿Por qué?**
- **¿Cuáles diría que son los principales desafíos que enfrenta la universidad para mejorar la seguridad de sus servidores con sistemas operativos open source?**
- **¿Qué recomendaciones o sugerencias tiene para mejorar la seguridad de estos servidores en la universidad?**
- **¿Qué herramientas o recursos utiliza para mantenerse actualizado sobre las últimas amenazas y vulnerabilidades de seguridad?**
- **¿Qué tipo de capacitación en seguridad informática recibe el personal que administra los servidores?**

Anexo 3

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD ADMINISTRACION FINANZAS E INFÓRMATICA
DECANATO

Babahoyo, 22 de febrero de 2024
D-FAFI-UTB-0216-2024

Ingeniero.
Marcos Oviedo Rodríguez, Ph.D.
RECTOR DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO
En su despacho. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El señor **KLEYNER JAVIER CALERO ESPINOZA,** con cédula de identidad No. **120776373-9** estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo NOVIEMBRE 2023 – ABRIL 2024, trabajo de titulación modalidad examen de carácter complexivo, previo a la obtención del grado académico profesional universitario de tercer nivel como INGENIERO EN SISTEMAS DE INFORMACIÓN**,** solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar su Estudio de Caso, en el Departamento de Dirección de Tecnológicas y Sistemas de Información de la Universidad Técnica de Babahoyo, en el cual su tema es: **"LOS ATAQUES INFORMÁTICOS EN LA SEGURIDAD DE LOS SERVIDORES CON SISTEMAS OPERATIVOS OPEN SOURCE EN LA UNIVERSIDAD TÉCNICA DE BABAHOYO".**

Atentamente,

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD ADMINISTRACION FINANZAS E INFÓRMATICA
DECANATO

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO
cc: Archivo

Recibido
23-02-2024
Recibido

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Ing. Marilyn Coloma Aguilar	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE

Anexo 4

Ilustración 22 Análisi de vulnerabilidades de los servidores OpenSources

Ilustración 23 Entrevistas en el departamentos de Sistemas

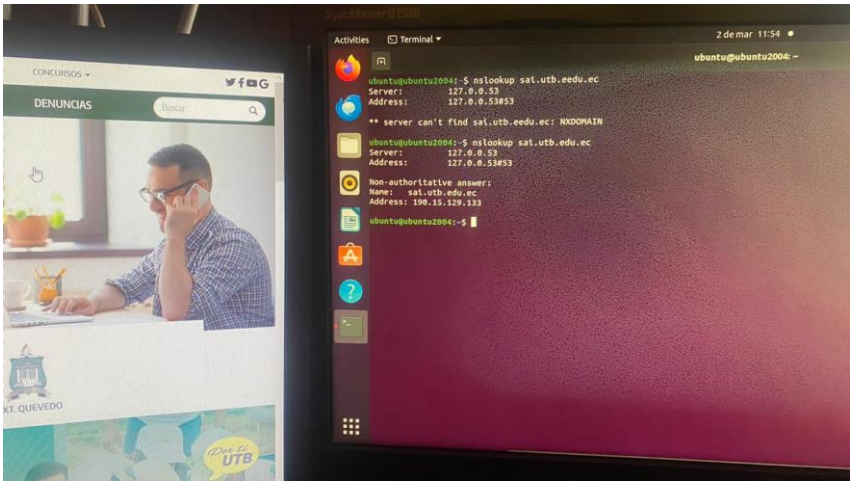


Ilustración 22 Ejecución del análisis de vulnerabilidades