Instituto Tecnológico y de Estudios Superiores de Monterrey
Escuela de Ingeniería y Ciencias

Auditoría de Seguridad y Plan de Mitigación: Caso Instituto Bilingüe La Silla

Presentación Ejecutiva de Resultados

Monterrey, Nuevo León. Fecha: 17 de Marzo de 2023

Socio Formador: Tecnogam

Carrera: Ingeniería en Ciencias de Datos y Matemáticas

Curso: Análisis de Criptografía y Seguridad

Equipo:

Gonzalo Garza Moreno	A01284950
Héctor David Bahena Garza	A01284661
Valeria María Serna Salazar	A01284960
Victor Hugo Garza Mantecón	A01284924
Kevin Antonio González Díaz	A01338316
Adalía Fernanda Aneiros Gutiérrez	A00832680

AGENDA

I. Introducción
II. Inventario
III. Topología de red
IV. Especificaciones de vulnerabilidades
V. Análisis de vulnerabilidades
VI. Plan de mitigación
VII. Costos totales
VIII. Conclusiones
IX. Referencias

I. INTRODUCCIÓN

La tecnología ha traído una serie de retos, amenazas y riesgos.

La importancia de la ciberseguridad se presenta; la protección de datos sensibles y confidenciales, tanto de empresas como de personas, es esencial.

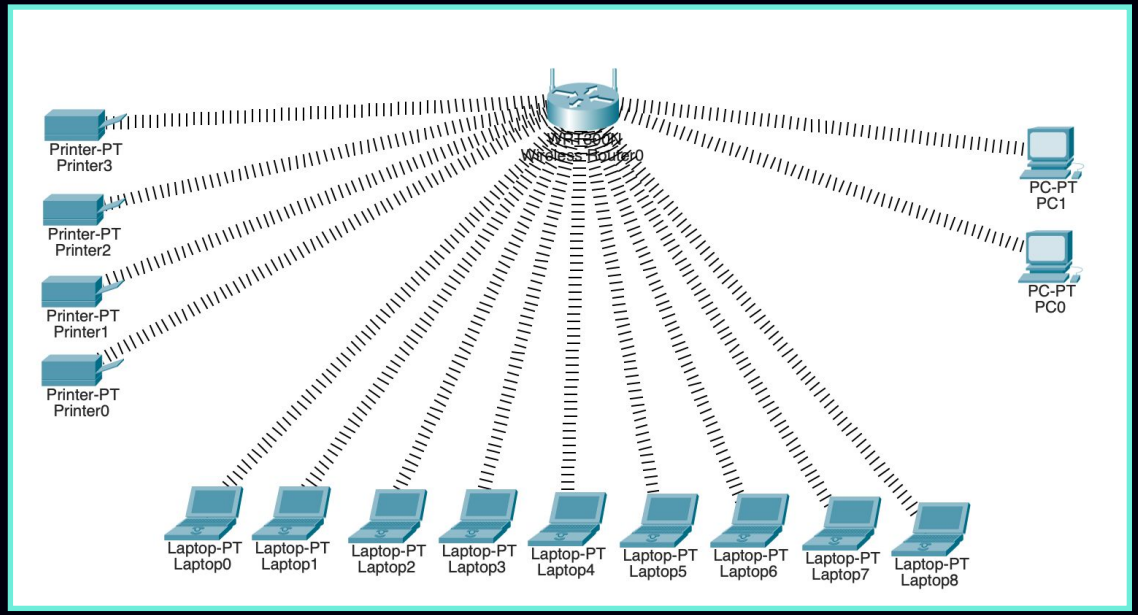
Durante el análisis de vulnerabilidades, se busca otorgar una solución con el objetivo de robustecer el sistema interno de la PyME elegida: **“Instituto Bilingue la Silla”**,

Presupuesto para invertir:
$15 000.

II. INVENTARIO

	PRODUCTO	CANTIDAD
	Computadora portátil Windows	10
	Computadora portátil Apple	1
	Computadora de escritorio Windows	2
	Impresora marca Xerox	4
	Teléfonos personales, relojes, entre otros	Los de todos los empleados

III. TOPOLOGÍA DE LA RED



IV

ESPECIFICACIONES SOBRE LAS VULNERABILIDADES

VULNERABILIDADES

	Vulnerabilidad	Puntuación de peligro	Hosts	CVE
1.	SSL Version 2 and 3 Protocol Detection	9.8	192.168.14.10 192.168.14.11 192.168.14.87 192.168.14.2	N/A
2.	Security Update for Microsoft Visual Studio Code (January 2023)	7.8	192.168.14.58	CVE-2023-21779
3.	SSL Certificate Signed Using Weak Hashing Algorithm	7.5	192.168.14.11 192.168.14.10 192.168.14.87 192.168.14.2	CVE-2004-2761
4.	SMB NULL Session Authentication	7.3	192.168.14.72	CVE-1999-0519 CVE-1999-0520 CVE-2002-1117
5.	IP Forwarding Enabled	6.5	192.168.14.1	CVE-1999-0511
6.	DHCP Server Detection	3.3	192.168.14.1	N/A
7.	Apple Mac OS X (Multiple Issues)	9.8 - 3.7	192.168.14.58	Varios
8.	Microsoft Windows (Multiple Issues)	10 - 8.1	192.168.14.87 192.168.14.2	N/A
9.	Apache Httpd (Multiple Issues)	9.8 - 7.5	192.168.14.58	CVE-2021-34798 CVE-2021-39275

ESPECIFICACIONES

Vulnerabilidad	Significado	Importancia	Posible solución
SSL version 2 and 3 Protocol Detection	La versión del Secure Sockets Layer utiliza un protocolo para encriptar con vulnerabilidades.	Es susceptible a un ataque, dejando al aire información sensible.	Asegurar que todas las computadoras tengan sus browsers actualizados.
Sistemas operativos no actualizados	Algunos sistemas operativos no están actualizados.	Las actualizaciones incluyen correcciones contra nuevas vulnerabilidades y amenazas.	Actualizar los sistemas y eliminar las aplicaciones en desuso.
SMB Null session authentication	SMB es un protocolo de intercambio en una red de archivos. El equipo permite el acceso sin autenticación.	Un atacante podría obtener acceso y acceder a información confidencial.	Permitir manualmente el acceso a ciertos usuarios, o dejar de compartir los archivos.

Vulnerabilidad	Significado	Importancia	Posible solución
IP forwarding enabled	La opción de reenvío de IP está habilitada, para permitir el aceptar y retransmitir datos y paquetes por un medio físico.	Un atacante puede aprovechar el reenvío de información para enrutar paquetes, evitando firewalls y filtros en la red, teniendo así acceso a la misma.	Deshabilitar la opción desde la terminal.
DHCP server detection	El DHCP asigna direcciones IP (información de los equipos en la red), por lo que cuenta con información importante y confidencial.	Un atacante podría acceder a esta información y por ende, conocer bien la red.	Mantener información importante fuera de la red o hacer un filtrado de la misma.
SSL certificate signed using weak hashing algorithm	Este certificado establece conexiones seguras entre el servidor y el cliente, pero tiene debilidades importantes.	Se puede exponer información confidencial y realizar ataques de phishing	Actualizar los certificados SSL, usar algoritmos de hash seguros y revocar certificados antiguos.

V

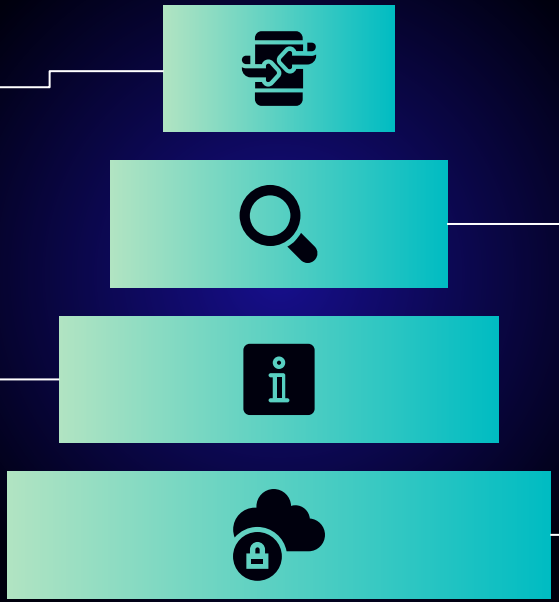
PLAN DE ANÁLISIS DE LAS VULNERABILIDADES

SISTEMAS OPERATIVOS NO ACTUALIZADOS

- Tener aplicaciones en desuso o softwares no actualizados genera vulnerabilidad.
- Se recomienda hacer backups periódicos.
- Las principales compañías de software notifican sobre las actualizaciones. Depende de nosotros darle continuidad.
- Que los empleados de la PyME tengan información básica sobre este tema, es fundamental.

IP FORWARDING ENABLED

Habilitar esta opción permite la conexión entre equipos, pero los atacantes pueden aprovecharse y analizar los puertos.



Existen analizadores de puertos para saber cuáles están abiertos, sus niveles de seguridad, etc.

Tipos de analizadores:

- Análisis de ping
- Análisis semiabiertos
- Análisis XMAS

Con esto será posible determinar si es necesario deshabilitarlos o instalar cortafuegos

DHCP SERVER DETECTION

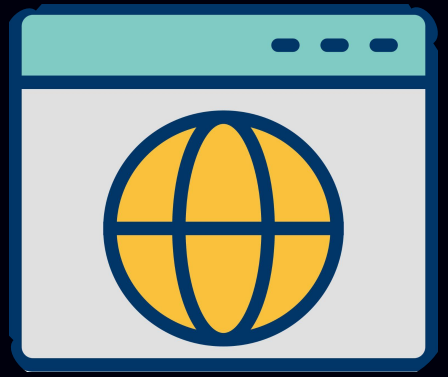
El Protocolo de Configuración Dinámica de Host simplifica la administración de la red.

Esto le abre el acceso a los atacantes: '**DHCP Spoofing**'. Se podrían enviar mensajes engañosos con direcciones falsificadas.

Solución: '**DHCP Snooping**'. Bloquea los servidores de DHCP maliciosos y protege la red de suplantaciones de identidad.

SSL VERSION 2 AND 3 PROTOCOL DETECTION

- Actualizar los browsers de todas las computadoras conectadas a la red de la organización.
- Hacer caso especial a Google Chrome y Mozilla FireFox.
- Se recomienda encender la opción de actualizaciones automáticas para evitar el problema en el futuro.



SSL CERTIFICATE SIGNED USING WEAK HASHING ALGORITHM

- Actualizar o buscar un nuevo proveedor de seguridad para almacenar, mandar y recibir información.
- Una opción para un nuevo proveedor es DigiCert. Es una compañía confiable y líder del mercado.
- Checar periódicamente el estatus de seguridad del algoritmo que utiliza el certificado que se tenga.

SMB NULL SESSION AUTHENTICATION

- Podría ser posible implementar herramientas de autenticación de red, Cisco, Fortinet, Azure, etc.

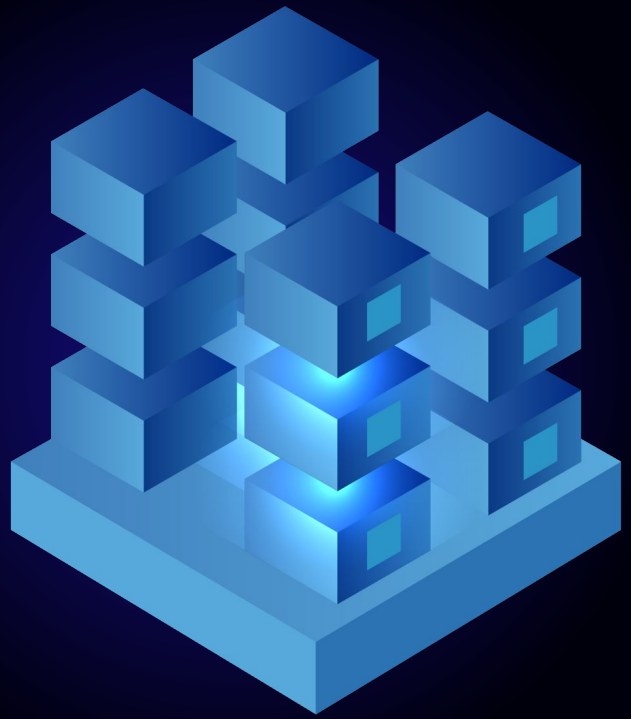
- Podría solucionarse también mediante el uso de VPN, firewalls, o segmentando la red.

- Mantener sistemas operativos de distintos equipos actualizados.

- También es posible manualmente revisar y administrar los archivos que están siendo compartidos por SMB.

VI

PLAN DE MITIGACIÓN



POSIBLES SOLUCIONES

Plática a Empleados

Sobre cultura de seguridad.

Deshabilitar el IP Forwarding

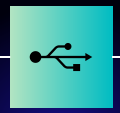
Para reducir riesgos de ataque.

Gestor de Contraseñas

Para mejorar la seguridad de las cuentas.

Descargar antivirus

Para proteger los equipos de ataques.



Adoptar el uso de USB

Como medio de transferencia de documentos.

Certificado SSL

Se necesita un nuevo certificado SSL con un algoritmo más fuerte

1. Plática a Empleados

Impartir una plática a empleados enfocada a buenas prácticas relacionadas con la ciberseguridad, como mantener software actualizado.

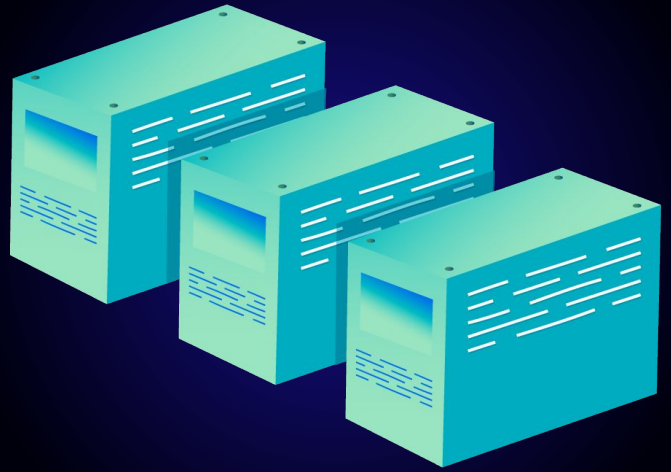
- Servicio gratuito
- No necesita atención continua
- Mejora también la eficiencia del trabajo
- Mejora la cultura general de los empleados

Costo: $0

2. Deshabilitar IP Forwarding

Proceso simple que mejora la seguridad de ciertos dispositivos de la red, como discutido anteriormente.

- Brinda mayor seguridad
- Podría requerir apoyo de un experto



Costo: $600

3. Gestor de Contraseñas

El uso de un gestor como BitWarden y el establecimiento de nuevas contraseñas (reemplazando contraseñas antiguas) seguras protegería contra ataques de fuerza bruta.

- Programa gratuito
- No necesita apoyo de un especialista de TI
- Construir el nuevo hábito de utilizar este programa podría tomar tiempo

Costo: $0

4. Descargar Antivirus

Los empleados son propensos a caer en ataques de tipo phishing.

Antivirus Norton: cuenta con un plan para empresas pequeñas y 20 dispositivos (250 dólares).

- Poco esfuerzo por parte de los empleados.
- Ofrece soporte técnico 24/7 para las personas.
- Es aplicable para cualquier sistema operativo.

Costo: $5,000

5. Usar USB

Uso de USB's para transferir los datos, a diferencia del correo electrónico que puede ser interceptado o manipulado, siendo vulnerable a los hackers y virus informáticos.

- Cifrado con contraseña, garantizando seguridad.
- Mayor capacidad de almacenamiento, permitiendo transferir grandes cantidades de datos.
- Transferencias de archivos más rápidas y fiables.

Costo: $400

6. Certificado SSL

Se necesita un nuevo certificado SSL que use un algoritmo más fuerte asegurándose de que el proveedor de certificación sea confiable.

DigiCert es una de las empresas más grandes y respetadas en el mercado de certificados SSL

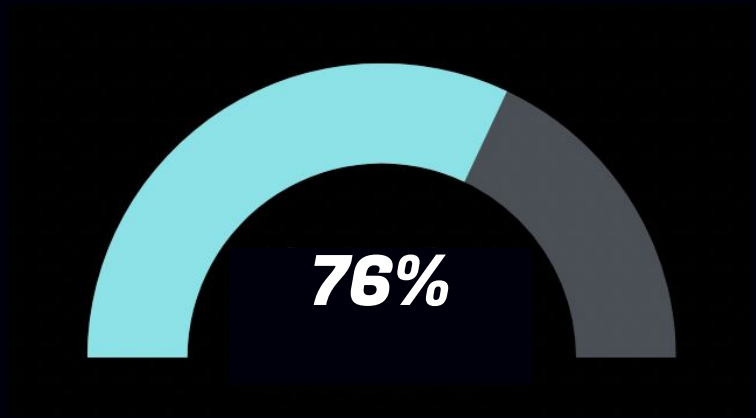
- Seguridad de la información
- Protección contra el phishing
- Confianza del usuario

Costo: $5 400

VII. COSTOS TOTALES

El costo del plan de mitigación en comparación con el presupuesto de la empresa:

$11,400 / $15,000



RIESGOS DE NO IMPLEMENTARSE

Pérdida económica

Pérdida de clientes

Sanciones legales

VIII. CONCLUSIONES

Concientizar

A las empresas de las vulnerabilidades de su red.

Prevenir

Para mitigar, o al menos reducir estos riesgos.

Implementar

Medidas de seguridad para lograr proteger sus datos valiosos

IX. REFERENCIAS

Nessus. (2023). What is Nessus: https://www.cs.cmu.edu/~dwendlan/personal/nessus.html#:~:text=What%20is%20Nessus%3F,have%20connected%20to%20a%20network.

Whittaker, Z. (2023, January 15). Norton LifeLock says thousands of customer accounts breached. https://techcrunch.com/2023/01/15/norton-lifelock-password-manager-data/

CVSS v3.1 User Guide. (2019). FIRST — Forum of Incident Response and Security Teams: https://www.first.org/cvss/user-guide

5 Classes of IPv4 Addresses [Class A, B, C, D and E]. (2023). https://www.meridianoutpost.com/resources/articles/IP-classes.php

SMB share full access by Everyone group CVE-1999-0519 Vulnerability Report. https://exchange.xforce.ibmcloud.com/vulnerabilities/1

Microsoft IIS Disabling SSL v3 Instructions – DigiCert.com. (2023). https://www.digicert.com/kb/ssl-support/iis-disabling-ssl-v3.htm

Hetler, A. (2022). 5 reasons software updates are important. https://www.techtarget.com/whatis/feature/5-reasons-software-updates-are-important

NA (2013) Instituto Bilingue la Silla: Nosotros
http://lasilla.edu.mx/

Tran, D. D., & Ogata, K. (2022). Formal verification of TLS 1.2 by automatically generating proof scores. Computers & Security, 123, 102909.

Lazar, Y. (2022b, octubre 16). DHCP Spoofing 101. Pentera.
https://pentera.io/blog/dhcp-spoofing-101/

¿Qué es el análisis de puertos y cómo funciona? (s. f.). Avast Antivirus.
https://www.avast.com/es-mx/business/resources/what-is-port-scanning

Klusaitė, L. (2022, 31 diciembre). ¿Qué es el port forwarding y cómo configurarlo? NordVPN.
https://nordvpn.com/es/blog/que-es-port-forwarding/

Harley, D. (2016, 11 abril). ¿Por qué el software es vulnerable? La importancia de los parches. We live security.
https://www.welivesecurity.com/la-es/2016/04/11/software-vulnerable-importanc ia-parches/

Feagin, R. D. (2015). *THE VALUE OF CYBER SECURITY IN SMALL BUSINESS*.

Huggett, C. (2022, 27 junio). *Going on the attack: Top five consequences of cyber security breaches*.

TechNative. Recuperado 17 de marzo de 2023, de

https://technative.io/going-on-the-attack-top-five-consequences-of-cyber-security-breaches/