Instrumento	*Práctica de ejercicios*

Alumno: Alan David Garcia Zamorano	**Fecha: 19/05/2023**
Carrera: Ingenieria en Desarrollo y Gestion de Software	**Grupo: IDGS91D**
Asignatura: Seguridad en el Desarrollo de Aplicaciones	**Unidad temática: Unidad 1. Principios de Codificación Segura**
Profesor: Geovanni Machuca Pereida	

I.- Ejercicios a resolver:

II.-Procedimientos y resultados:

Gusanos – Stuxnet (Irán, 2010)

En enero de 2010, los inspectores de la Agencia Internacional de Energía Atómica que visitaban una planta nuclear en Natanz, Irán, notaron con desconcierto que las centrifugadoras usadas para enriquecer uranio estaban fallando. Curiosamente, los técnicos iraníes que reemplazaban las máquinas también parecían asombrados.

El fenómeno se repitió cinco meses después en el país, pero esta vez los expertos pudieron detectar la causa: un malicioso virus informático.

El "gusano" ahora conocido como Stuxnet tomó el control de 1000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse.

Fue la primera vez que un ataque cibernético logró dañar la infraestructura del "mundo real".

Manera en la que se ejecutó este gusano:

1- Stuxnet penetró en la red

Según la firma de seguridad cibernética Symantec, Stuxnet probablemente llegó al programa nuclear de Natanz de Irán en una memoria USB infectada.

Alguien habría tenido que insertar físicamente el USB a una computadora conectada a la red. El gusano penetró así en el sistema informático de la planta.

2- El gusano se propagó a través de las computadoras

Una vez dentro del sistema informático, Stuxnet buscó el software que controla las máquinas llamadas centrifugadoras.

Las centrífugas giran a altas velocidades para separar componentes. En la planta de Natanz, las centrifugadoras estaban separando los diferentes tipos de uranio, para aislar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares.

3- Stuxnet reprogramó las centrifugadoras

El gusano encontró el software que controla las centrifugadoras y se insertó en él, tomando el control de las máquinas.

Stuxnet llevó a cabo dos ataques diferentes. En primer lugar, hizo que las centrifugadoras giraran peligrosamente rápido, durante unos 15 minutos, antes de volver a la velocidad normal. Luego, aproximadamente un mes después, desaceleró las centrifugadoras durante unos 50 minutos. Esto se repitió en distintas ocasiones durante varios meses.

4- Destrucción de las máquinas

Con el tiempo, la tensión provocada por las velocidades excesivas causó que las máquinas infectadas, unas 1000, se desintegraran.

Durante el ataque cibernético, alrededor del 20 por ciento de las centrifugadoras en la planta de Natanz quedaron fuera de servicio.

Prevención

Mantener el sistema operativo y el software actualizados ya que Stuxnet aprovechó una vulnerabilidad en el protocolo de Windows. Actualizar el sistema operativo y el software con los últimos parches y actualizaciones de seguridad habría ayudado a mitigar el riesgo de explotación de esa vulnerabilidad.

Mantener el uso de unidades USB y otros dispositivos de almacenamiento extraíbles al mínimo ayuda a reducir el riesgo de que el malware se introduzca en su ordenador a través de un dispositivo de almacenamiento extraíble infectado. Y junto con las muchas otras ventajas de utilizar una VPN, una conexión cifrada ayuda a ocultar su identidad y a protegerse de los ataques de repetición.

Sin embargo, aunque a menudo se necesita una VPN, no sustituye a un software antivirus específico con escaneo de amenazas en tiempo real que puede frustrar los ataques antes de que causen daños. Los mejores paquetes de ciberseguridad cuentan con herramientas de eliminación de malware especializadas, como los eliminadores de troyanos, que pueden poner en cuarentena e incluso purgar las amenazas nuevas y emergentes.

Troyanos – Bizarro (Brasil, 2021)

El troyano bancario de origen brasileño Bizarro es un malware que ha atacado a más de 70 bancos en todo el mundo y 22 de ellos son entidades españolas, siendo así el país más afectado por este ciberataque.

La empresa de seguridad Kaspersky descubría este nuevo peligro e informaba de forma pública a todas las empresas del sector bancario. Dando a conocer que ya ha afectado en especial a países como España, Alemania, Francia, Italia, Portugal Argentina y Chile.

El ataque está ahora mismo en proceso, lo que significa que todavía no se ha frenado. Los delincuentes están empleando distintas técnicas para el análisis y la detección si el ordenador ha sido infectado.

Lo que sí se puede frenar es la prevención de la infección. *Bizarro* se distribuye por medio de paquetes MSI (Microsoft Installer), estos se descargan por medios de enlaces de correos que suelen ir a la carpeta de *spam*.

Prevención

Si queremos evitar ser infectados hay que tener mucho cuidado con ver sobre qué enlaces se hace click en los mails que se reciben. Y desconfiar de cualquier link que no sea de confianza.

Tener autenticación de dos factores en aplicaciones bancarias y utilizar contraseñas únicas no cosas como fecha de cumpleaños o nombre.

Spyware - APT29 (2020)

APT29, los hackers que buscaban robar información de la vacuna Covid-19

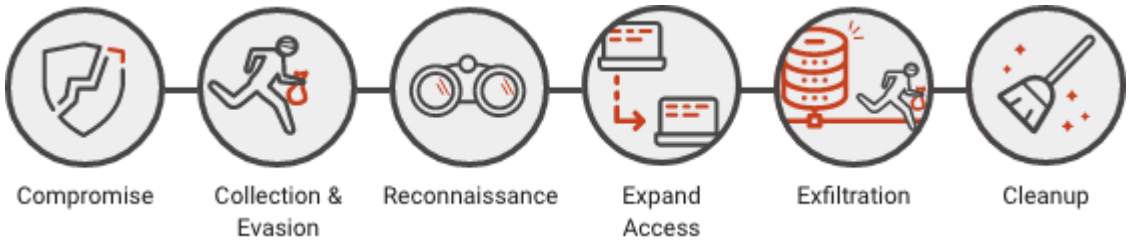
Se denunciaron ataques contra científicos nacionales que forman parte de una campaña global del grupo informático ruso, «que busca usurpar los secretos de la búsqueda de la vacuna contra la Covid-19».

Todos los expertos consultados por este periódico aseguran que «estamos ante uno de los mejores grupos organizados». No obstante, se desconoce sus intenciones, el número de componentes de su ejército y a sueldo de quién trabajan.

Su rastro de ataques guarda un patrón. No buscan dinero, no buscan secuestrar ordenadores o hacer caer servidores. Su mira apunta alto: Espionaje gubernamental, información privilegiada y poder.

Según las agencias de ciberseguridad de EEUU, Reino Unido y Canadá, el objetivo de estos ataques no sólo consiste en robar información y propiedad intelectual sobre el desarrollo de la posible vacuna, sino también afectar a la respuesta contra el coronavirus apuntan los responsables de seguridad.

Según el Centro de ciberseguridad nacional del Reino Unido APT29 ha utilizado el malware WellMess o WellMail para acceder a los ordenadores de los investigadores y así obtener la información necesaria sobre la vacuna de la Covid-19.



Prevención

Para prevenir este tipo de malware hay que tener siempre actualizados nuestro sistema operativo, contar con antivirus, no descargar aplicaciones poco confiables, tener precaución con los correos y enlaces sospechosos.

Adware – Fireball (2017)

En 2017, surgió una nueva amenaza en el horizonte digital, un malware tan potente que fue comparado con una bola de fuego. No se trataba de un adware cualquiera; Fireball tenía el poder de convertir los navegadores en zombis, secuestrándolos para generar ingresos publicitarios y propagarse aún más.

Fireball fue la creación de Rafotech, una gran agencia de marketing digital con sede en Pekín, China. Las víctimas no eran individuos, empresas o gobiernos concretos, sino cualquier persona con conexión a Internet. La escala del ataque fue asombrosa, con más de 250 millones de ordenadores infectados en todo el mundo.

El impacto financiero de Fireball fue significativo. Los costes derivados de la eliminación del malware y las pérdidas derivadas de la interrupción de la productividad se sumaron rápidamente. Dado el gran número de personas afectadas, el peaje financiero fue inmenso.

Los datos comprometidos afectaban principalmente a la configuración del navegador y a los hábitos de navegación de los usuarios. Pero Fireball también podía ejecutar cualquier código en los ordenadores de las víctimas, lo que potencialmente podía llevar a formas más graves de compromiso de los datos.

Prevención

- Mantenga sus dispositivos actualizados: Las actualizaciones de software suelen contener parches para vulnerabilidades de seguridad. Actualizar regularmente sus dispositivos le asegura estar protegido contra las amenazas conocidas.
- Instale un software antivirus fiable: Un gran antivirus para Windows 11, como Norton, Bitdefender, McAfee, Panda, o Kaspersky, proporciona una capa adicional de seguridad, ayudando a detectar y eliminar software malicioso.
- Tenga cuidado con las descargas: Descargue únicamente software y archivos de fuentes fiables para evitar instalar accidentalmente adware u otro software malicioso.
- Lea antes de hacer clic: Asegúrese de leer todos los términos y condiciones antes de instalar software, especialmente el gratuito, ya que puede incluir adware no deseado.

Ransomware – WannaCry (2017)

Los cibercriminales responsables del ataque aprovecharon una debilidad en el sistema operativo Microsoft Windows mediante un malware supuestamente desarrollado por la *Agencia de Seguridad Nacional de Estados Unidos*.

Conocido como EternalBlue, este ataque fue publicado por un grupo de hackers llamado *The Shadow Brokers* antes del ataque de WannaCry.

Microsoft publicó un parche de seguridad que protegía los sistemas de los usuarios contra este exploit casi dos meses antes de que comenzara el ataque de ransomware WannaCry. Por desgracia, muchas personas y organizaciones no

actualizan periódicamente sus sistemas operativos, por lo que quedaron expuestas al ataque.

Aquellos que no habían ejecutado una actualización de Microsoft Windows antes del ataque no pudieron beneficiarse del parche, y la vulnerabilidad explotada por EternalBlue los dejó expuestos al ataque.

Cuando ocurrió por primera vez, la gente asumió que el ataque de ransomware WannaCry se había propagado al principio a través de una campaña de phishing (una campaña de phishing es aquella en la que correos electrónicos de spam con enlaces o archivos adjuntos infectados inducen a los usuarios a descargar malware). Pero fue el exploit EternalBlue el responsable de la propagación de WannaCry, y funcionaba a la par con DoublePulsar, la "puerta trasera" (backdoor) que se instalaba en las computadoras afectadas (que se utilizaban para ejecutar WannaCry).

Los atacantes exigían un rescate en bitcoins por valor de 300 dólares. Más adelante, aumentaron el rescate en bitcoins a un valor de 600 dólares. A las víctimas del ataque de ransomware WannaCry se les comunicó que, si no pagaban el rescate en un plazo de tres días, sus archivos se eliminarían para siempre.

Prevención

- Actualice el software y el sistema operativo periódicamente.
- No haga clic en enlaces sospechosos.
- Nunca abra archivos adjuntos de correos electrónicos que no sean de confianza.

- No descargue archivos de sitios web que no sean de confianza.
- Evite el uso de dispositivos USB desconocidos.

Doxing – Sony Pictures (2014)

Los hackers se hicieron con datos confidenciales e incluso películas. El hecho es, que este grupo conocido como #GOP logró acceder a la intranet de Sony Pictures y se hizo con un sinfín de información, desde contraseñas hasta "varios Terabytes" de archivos y documentos internos de la compañía, además del acceso anticipado a varias películas que aún no han sido estrenadas en cartelera. De nuevo, una pesadilla para la empresa.

La primera consecuencia que se pudo ver en la red fue la filtración de 5 películas de Sony Pictures que aún no han sido estrenadas, obtenidas gracias a las copias internas que manejan estas empresas para enviar a personas o agencias en específico. Las películas filtradas son:

- Fury, protagonizada por Brad Pitt.
- Annie, protagonizada por Cameron Diaz.
- Mr. Turner, con Timothy Spall.
- Still Alice, protagonizada por Julianne Moore.
- To Write Love on Her Arms, con Rupert Friend.

Este fue el inicio de las represalias de #GOP contra Sony Pictures y, aun así, todavía no se conoce cuáles son las demandas que ha hecho el grupo de hackers al gigante del cine.

Los problemas de Sony Pictures han ido más allá una semana más tarde. Durante los últimos siete días los hackers no se han detenido ni quedado dormidos en sus amenazas. Han liberado una serie de documentos internos relacionados a los salarios de algunos ejecutivos, incluyendo el CEO De la compañía, Michael Lynton, que gana 3 millones de dólares al año, además de las quejas y condiciones de trabajo de muchos empleados.

También han liberado direcciones de domicilio de los trabajadores y números de seguro social, mientras aseguran que esta es solo la punta del iceberg. Tienen mucha información confidencial más por compartir.

Un grupo de analistas de seguridad informática llamado "AlienVault" se ha dedicado a analizar el malware con el que fue atacado Sony Pictures, y descubrieron que fue compilado entre los días 22 y 24 de noviembre, y el texto de la programación fue escrito mediante caracteres coreanos. Esto quizás no sea prueba suficiente para involucrar a un gobierno completo en el ataque, pero la verdad, no es de locos pensar que realmente Corea del Norte amenazó a Sony Pictures por la película, y cumplió su amenaza.

10/16/2014	7:59 PM	30208	passwords - Copy.xls
10/16/2014	6:38 PM	19456	PASSWORDS FOR LB.xlsx
10/16/2014	7:45 PM	19968	Passwords Mady.xls
10/16/2014	7:58 PM	32768	PASSWORDS Master-1 (3).xls
10/16/2014	7:58 PM	21504	Passwords Mst Sony 021211.xlsx
10/16/2014	7:58 PM	27475	Passwords Rosa 042414 (Autosaved).xlsx
10/16/2014	7:44 PM	25088	Passwords Rosa 101509 .xls
10/16/2014	7:58 PM	26112	Passwords to change.doc
10/16/2014	6:15 PM	53	passwords.txt
10/16/2014	7:44 PM	16384	passwords.xls
10/16/2014	7:29 PM	18321	passwords.zip
10/16/2014	6:16 PM	185	passwords.zip SSPCEB2005.txt
10/16/2014	7:58 PM	13923	Passwords1.docx
10/16/2014	6:48 PM	8714	Passwords1.xlsx
10/16/2014	7:46 PM	16896	PASSWORDS22.xls
10/16/2014	7:59 PM	19968	Passwords34.xlsx
10/16/2014	6:42 PM	33792	Passwords 110408.xls
10/16/2014	7:52 PM	13720	Passwordsddd.xlsx
10/16/2014	9:57 PM	17408	pawlowski password.xls
10/16/2014	7:35 PM	28287	payroll password email.pdf
10/16/2014	6:37 PM	24064	PRIEST Passwords.doc
10/16/2014	6:02 PM	54048	Public - IP Addressing 2.26.xlsx
10/16/2014	7:58 PM	26348	radha passwords.xlsx
10/16/2014	7:36 PM	26112	Rana's Passwords.doc
10/16/2014	7:03 PM	36112	remote users.txt
10/16/2014	8:07 PM	204562	ResetAccountPassword 14.log
10/16/2014	7:45 PM	13824	Reys Passwords.xls
10/16/2014	7:38 PM	18728	RFR Password Table - April 2011.pdf
10/16/2014	6:07 PM	12757	Security and Password Setting 1.xlsx
10/16/2014	6:04 PM	20522	Server Privileged Access.xlsx
10/16/2014	6:10 PM	35244	Social Password Log.xlsx
10/16/2014	7:40 PM	37	sonykeypassword.txt
10/16/2014	7:03 PM	1957	sp.la.spe.sca login script.txt
10/16/2014	7:27 PM	22528	SPE-MS Servers.xls
10/16/2014	7:04 PM	12	speconnect user pwd.txt
10/16/2014	5:56 PM	77166	SPEJ OH password.pdf
10/16/2014	7:51 PM	62464	SPI Employees Levels 401(k) sort passwordv2.xls
10/16/2014	7:48 PM	28160	SPIRIT Password History 16.xls
10/16/2014	7:06 PM	19013	sppbwa02 user.txt
10/16/2014	6:59 PM	10328	SSL Certs on Windows Servers.xlsx
10/16/2014	6:16 PM	26624	Stars User Password Horizon AfterGoLive 072407.xls
10/16/2014	7:35 PM	56320	Story Computer Passwords.doc
10/16/2014	7:54 PM	16999	Systems userids and passwords.xlsx
10/16/2014	6:21 PM	13945	territoriespassword.xlsx
10/16/2014	8:21 PM	1762816	The Interview Budget Final 10 10 13.pdf
10/16/2014	7:24 PM	172544	unix servers May 2014 v2.xls
10/16/2014	7:39 PM	9284	Unlock ID and reset password 110-9-10 INC0113716.xlsx
10/16/2014	6:17 PM	14336	UPS Login & Password.xls
10/16/2014	5:57 PM	16384	UserNames&Passwords.xls
10/16/2014	8:20 PM	93132	VARIANCE 061414 .pdf
10/16/2014	6:39 PM	13824	website passwords.xls
10/16/2014	6:18 PM	18245	YouTube login passwords.xlsx

Prevención

- Mantén la información personal privada: Limita la cantidad de información personal que compartes en línea.

- Utiliza configuraciones de privacidad adecuadas: Asegúrate de configurar adecuadamente las opciones de privacidad en tus perfiles de redes sociales y otras plataformas en línea.
- Sé cauteloso con los enlaces y archivos recibidos: No hagas clic en enlaces sospechosos ni descargues archivos adjuntos de fuentes desconocidas o no confiables.
- Utiliza contraseñas seguras y autenticación de dos factores: Asegúrate de utilizar contraseñas fuertes y únicas para todas tus cuentas en línea.
- Mantén tu software actualizado: Asegúrate de mantener tu sistema operativo, navegadores web y aplicaciones actualizadas con los últimos parches de seguridad.

Pishing – Facebook (2017)

Un grupo de hackers lanzó un ataque de phishing masivo dirigido a los empleados de Facebook. Los atacantes enviaron correos electrónicos de phishing a través de cuentas falsas de correo electrónico, haciéndose pasar por colegas legítimos dentro de la empresa.

Los correos electrónicos de phishing contenían enlaces maliciosos que, al hacer clic en ellos, redirigían a los empleados a páginas de inicio de sesión falsas que imitaban la apariencia de la auténtica página de inicio de sesión de Facebook. Una vez que los empleados ingresaban sus credenciales en estas páginas falsas, los atacantes las obtenían y podían acceder a las cuentas de los empleados.

Este ataque de phishing masivo afectó a alrededor de 30 empleados de Facebook, lo que permitió a los atacantes obtener acceso a ciertos sistemas internos de la empresa. Sin embargo, Facebook detectó rápidamente la actividad sospechosa y tomó medidas para mitigar los efectos del ataque.

Facebook llevó a cabo una investigación exhaustiva y trabajó para fortalecer sus medidas de seguridad y protección contra ataques de phishing similares en el futuro.

Además, la empresa notificó a los empleados afectados y les proporcionó asistencia en la protección de sus cuentas personales.

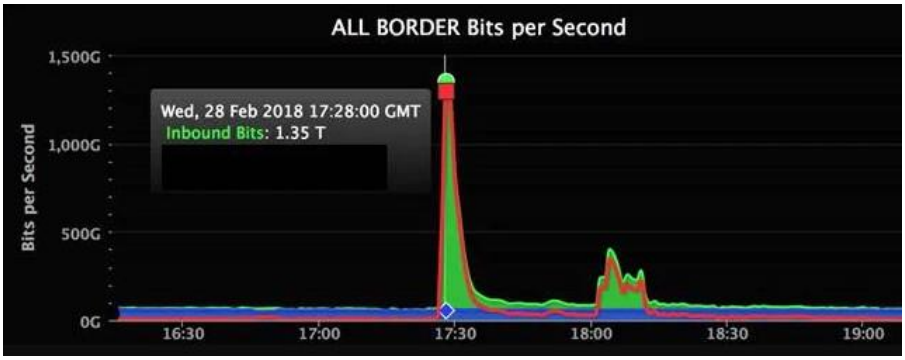
Prevención

- Presta atención a los indicios de un correo electrónico o mensaje sospechoso.
- Mantén tu software actualizado.
- Utiliza autenticación de dos factores.
- No hagas clic en enlaces sospechosos.

DDoS – GitHub (2018)

El ataque DDoS a GitHub ha tenido un nivel desconocido de 1,35 Tbps (126,9 millones de paquetes por segundo), casi el doble de la media de los mayores ataques registrados hasta ahora como el que tumbó Krebs on Security a 620 Gbps, el realizado al proveedor de hosting francés OVH que alcanzó casi los 800 Gbps o el mayor registrado hasta ahora contra el proveedor Dyn a 1,2 Tbps.

El enorme volumen de datos sobrepasó las computadoras de GitHub, lo que provocó que dejaran de responder y se desconectaran. En ese momento, GitHub recurrió al servicio especializado de mitigación de ataques DDos de Akamai para filtrar el tráfico malicioso, finalizando el efecto del ataque en pocos minutos. Hubo un segundo ataque que alcanzó un máximo de 400 Gbps, pero fue absorbido sin que el sitio cayera.



Prevención

- Considera la posibilidad de contratar servicios de mitigación DDoS de proveedores especializados.
- Configura firewalls y routers adecuadamente.
- Mantén un monitoreo constante de tu tráfico de red para detectar patrones y anomalías sospechosas que puedan indicar un ataque DDoS en curso.
- Establece límites de tráfico y ancho de banda para evitar que un ataque DDoS sobrecargue tus recursos.

III.-Bibliografía:

https://www.facebook.com/bbcnews. (2015, October 11). *El virus que tomó control de mil máquinas y les ordenó autodestruirse - BBC News Mundo*. BBC News Mundo; BBC News Mundo. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Buxton, O. (2022, July 14). *Stuxnet: ¿Qué es y cómo funciona?* Stuxnet: ¿Qué Es Y Cómo Funciona?; Avast. https://www.avast.com/es-es/c-stuxnet

Redacción. (2021, May 18). *Bizarro, el último troyano que ya ha atacado a más de 70 bancos*. La Vanguardia; La Vanguardia. https://www.lavanguardia.com/tecnologia/20210518/7462315/troyano-brasileno-ataca-varios-bancos-espanoles-mas-afectados-mmn.html

González, J. A. (2020, July 16). *APT29, los hackers que buscaban "robar" información de la vacuna Covid-19*. Ideal; Ideal. https://www.ideal.es/tecnologia/apt29-hackers-buscaba-20200717184455-ntrc.html

¿Qué es el adware? Los 7 ejemplos más terribles (2023). (2023, May 16). SoftwareLab. https://softwarelab.org/es/que-es-adware/

Kaspersky. (2023, April 19). *¿Qué es el ransomware WannaCry?* Latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware-wannacry

Protegerse del phishing en Facebook | Servicio de ayuda de Facebook. (2018). Facebook.com. https://es-es.facebook.com/help/phishing

https://www.facebook.com/MuySeguridad. (2018, March). *GitHub sufre el mayor ataque DDoS jamás registrado*. MuySeguridad. Seguridad Informática. https://www.muyseguridad.net/2018/03/02/ddos-contra-github/#:~:text=El%20ataque%20DDoS%20a%20GitHub%20ha%20tenido%20un,ahora%20contra%20el%20proveedor%20Dyn%20a%201%2C2%20Tbps.

RÚBRICA DE PRÁCTICA DE EJERCICIOS

Criterios	Escala de Calificación				
Procedimiento / Desarrollo y Resultados	70	60	35	8	0
(70 Puntos)	AUTÓNOMO (70 puntos) Evidenciar los razonamientos detallados y ordenados, así como las estrategias que se han empleado en el proceso de solución de los ejercicios solicitados. Además, debe presentar los resultados correctos obtenidos de cada ejercicio. Se detecta máxima una falta.	DESTACADO (60 puntos) Se detectan 2 faltas en los aspectos indicados.	SATISFACTORIO (35 puntos) Se detectan 3 faltas en los aspectos indicados.	COMPETENTE (8 puntos) Se detectan 4 o más faltas en los aspectos indicados. (8 puntos)	NO COMPETENTE El alumno no desarrolló el criterio
Formato y Ortografía	15	12	7	4	0
(15 puntos)	AUTÓNOMO (15 puntos) Sin errores ortográficos y el formato mínimo siguiente: - Tipo de letra legible, tamaño 12. - Interlineado 1.5 - Párrafos justificados - Paginado	DESTACADO (12 puntos) Se detectan 2 faltas en los aspectos indicados.	SATISFACTORIO (7 puntos) Se detectan 3 faltas en los aspectos indicados.	COMPETENTE (4 puntos) Se detectan 4 o más faltas en los aspectos indicados.	NO COMPETENTE El alumno no desarrolló el criterio
Datos de identificación	5	4	3	2	0
(5 puntos)	AUTÓNOMO (5 puntos) El alumno especifica los siguientes datos: - Alumno - Fecha - Carrera - Grupo - Unidad Temática - Asignatura - Profesor - Título de la práctica Se detecta máximo una falta.	DESTACADO (4 puntos) Se detectan dos faltas en los aspectos indicados	SATISFACTORIO (3 puntos) Se detectan tres faltas en los aspectos indicados.	COMPETENTE (2 puntos) Se detectan cuatro o más faltas en los aspectos indicados.	NO COMPETENTE El alumno no desarrolló el criterio
Bibliografía	10	8	5	2	0
(10 puntos)	AUTÓNOMO (10 puntos) Reporta la bibliografía que haya sido utilizada para la elaboración del reporte, de acuerdo a las normas establecidas por el APA (American Psychological Association) para citar autores. Se detecta máxima una falta.	DESTACADO (8 puntos) Se detectan 2 faltas en los aspectos indicados.	SATISFACTORIO (5 puntos) Se detectan 3 faltas en los aspectos indicados.	COMPETENTE (2 puntos) Se detectan 4 o más faltas en los aspectos inidicados.	NO COMPETENTE El alumno no desarrolló el criterio

Criterios	Clasificación					Puntos
Procedimiento / Desarrollo y Resultados	70	60	35	8	0	70
Formato y Ortografía	15	12	7	4	0	15
Datos de Identificación	5	4	3	2	0	5
Bibliografía	10	8	5	2	0	10
					Total de puntos	100 /100

Retroalimentación

Mr. Machuca Pereida
Señorito Alan, excelente trabajo, no hay mas que comentar. Sigue así.

Sab 27 May, 2023 at 4:12 pm