Desarrollo de un sistema de seguridad informática a partir de una auditoría sobre una red empresarial

Development of a computer security system based on an audit of an enterprise network

Santiago Serna Ramírez[1]
Álvaro Montoya Londoño[2]
Yeiler Alberto Quintero Barco[3]
Cesar Felipe Henao Villa[4]
Frey De Jesús Castro Ramírez[5]

DOI: *https://doi.org/10.26495/icti.v9i2.2267*

RESUMEN

En los últimos años se produjeron muchos errores de ciberseguridad. Dada esta problemática, se realizó un escaneo de red con diferentes herramientas el cual permitió identificar vulnerabilidades para mitigarlas y evitar penetraciones mal intencionadas sin autorización o fallas presentadas en la red de la empresa Finanzas al Día S.A.S (nombre alterado por seguridad de la empresa auditada), para solventarlas y buscar la posible solución evitando pérdida de información o ataques al sistema. Teniendo en cuenta la metodología implementada la cual se basa en investigaciones descriptivas, que incluyen comprender las condiciones actuales y generales a través de información obtenida y precisa sobre las actividades financieras, los procesos de recopilación de datos y el personal.

PALABRAS CLAVE:
Ciberseguridad, Red, Seguridad, Software, SSL, Vulnerabilidades.

ABSTRACT

In recent years there have been many cybersecurity errors. Given this problem, a network scan was performed with different tools which allowed to identify vulnerabilities to mitigate them and avoid malicious penetrations without authorization or failures presented in the network of the company Finanzas al Día S.A.S. (name altered by security of the audited company), to solve them and seek the possible solution to avoid loss of information or attacks to the system. Taking into account the methodology implemented which is based on descriptive research, which includes understanding the current and general conditions through information obtained and accurate information on financial activities, data collection processes and personnel.

[1] *Corporación Universitaria Americana, Medellín, Colombia. sernasantiago6010@americana.edu.co*
[2] *Corporación Universitaria Americana, Medellín, Colombia. montoyaalvaro7450@americana.edu.co*
[3] *Corporación Universitaria Americana, Medellín, Colombia. yquintero@americana.edu.co https://orcid.org/0000-0002-4991-4976*
[4] *Corporación Universitaria Americana, Medellín, Colombia. chenao@coruniamericana.edu.co https://orcid.org/0000-0001-7426-2589*
[5] *Corporación Universitaria Americana, Medellín, Colombia, fcastro@coruniamericana.edu.co, https://orcid.org/0000-0003-0142-6006*

KEYWORDS:
Cybersecurity, Network, Security, Software, SSL, Vulnerabilities.

1. INTRODUCCIÓN

En la actualidad una gran cantidad de empresas incursionan cada vez más en nuevas tecnologías de la información, lo que trae como consecuencia diversos retos plasmados en la seguridad informática, uno de los medios por el cual se efectúan más ataques tanto externos como internos poniendo en riesgo la integridad de grandes empresas que han pasado por alto la importancia de la ciberseguridad como factor fundamental de la institución, donde se plantean prioridades sujetas a otros entornos empresariales sin escatimar la importancia de una red planteada lo mejor posible con todos los niveles de seguridad requeridos para operar con una excelente consistencia.

La informática como gran aliado de la efectividad a la hora de realizar operaciones de alta complejidad, siendo así una gran herramienta de trabajo que trae consigo una gran cantidad de beneficios al igual que también trae sus riesgos La problemática que abarca en gran amplitud principalmente al interior de la empresa por parte de los usuarios de esta, al tener una manipulación no apropiada ya que por este medio es por donde más se dan los ataques de ciberseguridad, claramente partiendo de que sea con o sin intención; son los usuarios quienes más puertas abiertas dejan a los delincuentes cibernéticos. Los crímenes efectuados desde el exterior de la empresa particularmente por fallos de seguridad y falta de un planteamiento y análisis de la estructura de red son uno de los principales riesgos que se tiene hoy en día.

La elaboración de este proyecto se realizó con el fin de identificar las vulnerabilidades de seguridad informática de una red empresarial de Finanzas al Día S.A.S para la mitigación de riesgos. Ya que las empresas con el pasar de los tiempos y al migrar a las nuevas tecnologías de la información traen consigo mismas una cantidad de problemas arraigados con la seguridad y la falta de conocimientos frente a este problema tan complejo y que cada vez toma más fuerza.

Este proyecto se elaboró basado en los resultados obtenidos en la auditoría de ciberseguridad en la empresa Finanzas al Día S.A.S. realizada con las herramientas necesarias para obtener la mayor cantidad de información, la cual permitió obtener resultados oportunos y así identificar los problemas que afectan directamente, arrojando un balance y la gravedad de la amenaza calificándola en tres niveles segmentados en alta, media y baja.

Esta investigación dio solución a uno de los problemas que se presenta a nivel de red, informando sobre el fallo de seguridad y así mismo dando la solución oportuna la cual dio como resultado la mitigación del riesgo de seguridad informática por medio de técnicas seguras y auditorias con los protocolos y herramientas necesarias.

En el ámbito empresarial donde se llevó a cabo dicho proyecto de auditoría de ciberseguridad enfocado en la red de Finanzas al Día S.A.S, para así tener conocimiento de todas las vulnerabilidades encontradas y poder ejecutar un plan de mitigación del riesgo presentado, ofreciendo una solución oportuna estandarizando la empresa a niveles de manejo de documentación financieras, los procesos internos, la recopilación de datos e información del personal; donde pueda ofrecer un servicio más seguro y confiable frente a los clientes.

Enfocados en las normativas y políticas de sistemas de información que se rigen no solo a nivel local sino a nivel mundial, donde se le da más importancia a las Tecnologías de la Información (TI) gracias

a sucesos históricos donde grandes empresas privadas y gubernamentales se han visto afectadas por el gran impacto de los ciberdelincuentes. Gracias a esto se ha empezado a tomar medidas de aseguramiento a nivel de seguridad de los datos, trayendo consigo nuevas tecnologías, protocolos, normativas y lineamientos que han aportado significativamente un valor agregado al avance en el tratamiento de datos brindando una mejoría perimetral a la seguridad de las redes.

En un diagnóstico inicial se pudieron evidenciar las siguientes dificultades y/o vulnerabilidades en la organización: Acceso total por los visitantes a la red empresarial, falta de respaldo de la información, debilidad en cifrados de encriptación, certificados SSL no convenientes para el tipo de tráfico, revelación de información confidencial (user, password) entre los empleados, falta de controles para el acceso de la información, acceso a la información por parte de cualquier empleado y ningún tipo de restricción sobre las páginas web, permitiendo accesos páginas inadecuadas.

Se evidenció que los visitantes tienen acceso a la red interna de la organización sin ningún tipo de restricción de la información, lo cual expone a la organización ya que podría alterar y/o eliminar información valiosa, la cual por falta de respaldo sería imposible su recuperación.

También se constató que en la empresa Finanzas al Día S.A.S se hacían publicas ciertas credenciales las cuales permitían accesos a información clasificada, lo cual permitía que cualquier empleado lograra acceder a dicha información y manipularla, lo que podría ocasionar posibles evasiones de responsabilidad y suplantación de identidad

Con base en los diagnósticos realizados en la red empresarial de Finanzas al Día SAS ¿cómo se puede mejorar los niveles de seguridad o disminuir los niveles de vulnerabilidad de la red empresarial de la organización Finanzas al Día S.A.S?

2. MARCO TEÓRICO

Se puede entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema puede estar protegido o es vulnerable. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros (Huerta, 2002).

El Sistema de Gestión de Seguridad de la Información ISO 27001 persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: Electrónicos En papel Audio y vídeo, etc. (ISOTools Excellence, 2015).

Aunque el malware no puede dañar el hardware de los sistemas o el equipo de red con una excepción que se conozca (vea la sección Android de Google), sí puede robar, cifrar o borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en el ordenador sin su conocimiento o permiso (Malwarebytes, s.f.).

La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web. Cuando llega a la base de datos del sitio web, ubicada en su servidor, la carga útil del

hacker entra en acción e interfiere en la base de datos, de modo que el hacker puede cumplir sus objetivos (Belcic, Avast, 2020).

El atacante envía una comunicación dirigida con el fin de persuadir a la víctima para que haga clic en un enlace, descargue un archivo adjunto o envíe una información solicitada, o incluso para que complete un pago (Belcic, Avast, 2020).

Doxing (o doxing) es la revelación de la información personal confidencial de alguien mediante su publicación en línea. Los hackers lo utilizan para acosar, amenazar o vengarse de alguien en línea. Los doxxers utilizan diversos métodos para recopilar información sobre sus víctimas (Latto, 2020).

Un exploit es un programa informático que se aprovecha de un error para provocar un comportamiento no intencionado. Estos comportamientos incluyen, por lo general, la toma del control de un sistema, la concesión privilegios de administrador al intruso o el lanzamiento de un ataque de denegación de servicio (DoS o DDoS). (PANDA SECURITY, s.f.)

Los ataques DDoS bloquean sitios web dado que tanto el objetivo como los equipos utilizados en la botnet son víctimas, los usuarios individuales reciben daños colaterales en el ataque, ya sus equipos se ralentizan y fallan mientras se encuentran bajo el control del hacker. (Avast Academy Team, 2016).

El ataque MIM más habitual, se utiliza un router WiFi para interceptar las comunicaciones del usuario. Además, puede husmear en las sesiones de forma silenciosa sin que la víctima sea consciente de nada. (Malenkovich, 2013)

SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas). (DigiCert, 2021)

Es una forma muy eficaz de garantizar una firma digital y la integridad del archivo. (Conpilar News, 2021)

Un típico enrutador funciona en un plano de control (en este plano el aparato obtiene información acerca de la salida más efectiva para un paquete específico de datos) y en un plano de reenvío (en este plano el dispositivo se encarga de enviar el paquete de datos recibidos a otra interfaz). (Bembibre, 2009)

Cuando se usa UDP, los paquetes se envían al destinatario. No hay garantía de que esté recibiendo todos los paquetes y no hay manera de volver a pedir un paquete si lo pierde, pero perder todo este costo general significa que las computadoras se pueden comunicar más rápidamente. (Ortiz, 2019)

3. MATERIALES Y MÉTODOS

De acuerdo a las técnicas aprendidas y las herramientas utilizadas se llevó a cabo el mejoramiento de la ciberseguridad, ya que se realizó un nuevo escaneo de la red empresarial estudiada, después de haber llevado a cabo el plan de mitigación de vulnerabilidades.

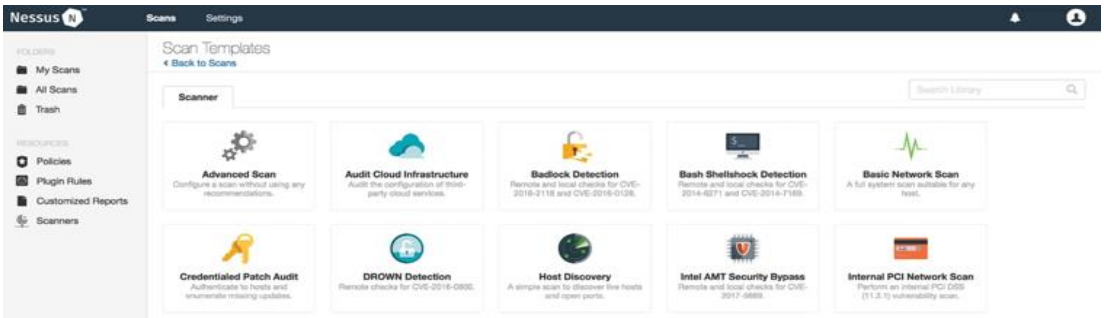
Figura 1. Evidencia de escaneo de red después de la mitigación de vulnerabilidades.

Fuente: Elaboración propia con base a pantallazo del software Nessus

Gracias a la herramienta Nessus la cual nos permite realizar un escaneo y así evidenciar la mitigación de las vulnerabilidades de categoría alta y media lo cual genera una mayor confiabilidad en el manejo de la información.

El análisis de seguridad de una red por parte de la herramienta Nessus, el cual se ejecuta con el fin de estudiar de una manera mucho más profunda, la seguridad que compone un sistema empresarial sustrayendo datos que trae consigo información valiosa para la mitigación de las vulnerabilidades que puedan existir en el sistema. Esta es una herramienta utilizada para el análisis de vulnerabilidades en diversos sistemas operativos, donde se opera con el fin de hallar puertos abiertos y poder generar exploits para atacarlo.

Figura 2. Herramientas de Nessus



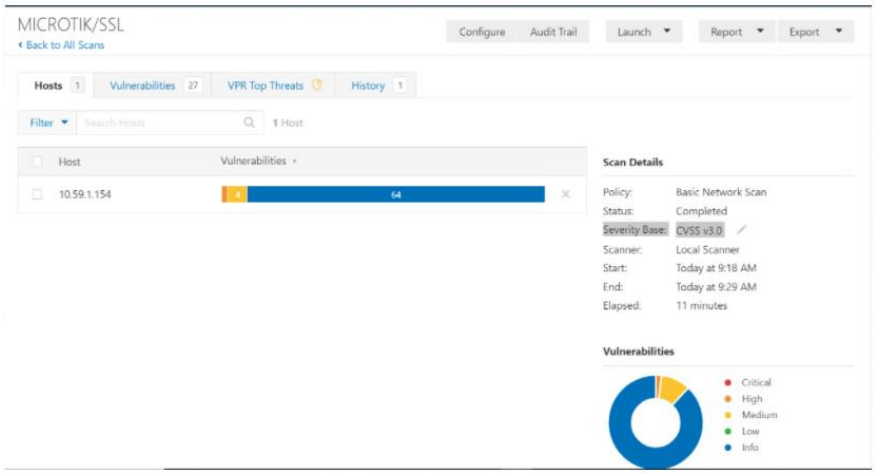
Fuente: Elaboración propia con base a pantallazo del software Nessus

.

4. RESULTADOS

En el análisis de la red empresarial se pudo evidenciar los diferentes tipos de vulnerabilidades encontradas gracias a las visitas realizadas a la empresa Finanzas al Día S.A.S| donde se clasifican según su riesgo.

Figura 3. Evidencia de vulnerabilidades encontrados



Fuente: Elaboración propia con base a pantallazo del software Nessus

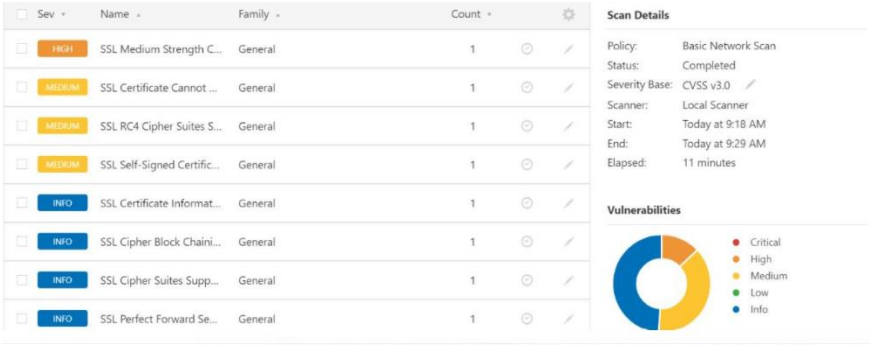
En la evidencia anterior podemos observar cada una de las vulnerabilidades y su clasificación según el riesgo: Alto (Vulnerabilidad con mayor riesgo de corrupción del sistema, donde el ataque se hace altamente efectivo), Medio (Vulnerabilidad con mediano riesgo de corrupción al sistema , donde se puede capturar información para generar un ataque efectivo), Bajo (Vulnerabilidad que presenta un riesgo bajo de ataque o robo de información por los pocos datos obtenidos) Vulnerabilidades de Información (Más llamadas vulnerabilidades ya que no representan un riesgo precario).

Vulnerabilidades Bajas: Son aquellas que suponen un riesgo real mínimo para los usuarios.

Vulnerabilidades Medias o Moderadas: Las vulnerabilidades moderadas se refieren a vulnerabilidades que tienen un riesgo bajo para la información y los recursos del sistema informático.
Vulnerabilidades Altas o Críticas: Las vulnerabilidades informáticas críticas son vulnerabilidades que permiten que las amenazas informáticas se produzcan y se propaguen sin la intervención del usuario.

¿Para qué sirve una suite criptográfica (cypher suite)?
Enfocándonos en las vulnerabilidades de Alto riesgo podemos evidenciar gracias a la herramienta utilizada, que la red es propensa a que los ciberdelincuentes efectúen ciertos daños donde se ve comprometida la información por falta de conocimiento sobre los Suites de Cifrado.

Figura 4. Evidencia de vulnerabilidades encontrados



Fuente: Elaboración propia con base a pantallazo del software Nessus

El ataque Sweet32 Birthday afecta el cifrado triple DES.

Figura 5. Suites de cifrado SSL de fuerza media compatibles (SWEET32)

Fuente: Elaboración propia con base a pantallazo del software Nessus

No se puede confiar en el certificado SSL del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las que la cadena de confianza se puede romper, como se indica a continuación:

Figura 5. Suites de cifrado SSL RC4 Compatibles (Bar Mitzvah

Fuente: Elaboración propia con base a pantallazo del software Nessus

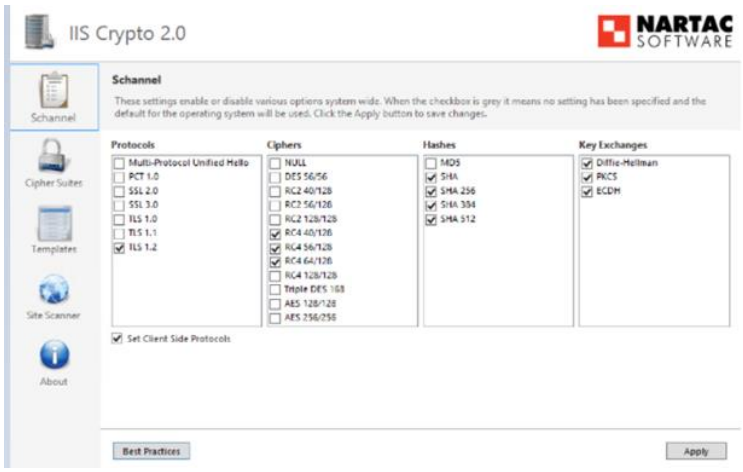
Figura 5. Certificado SSL autofirmado

Fuente: Elaboración propia con base a pantallazo del software Nessus

Figura 6. No se puede confiar en el certificado SSL

Fuente: Elaboración propia con base a pantallazo del software Nessus

Figura 7. Evidencia de tipos de cifrado usado



Fuente: Elaboración propia con base a pantallazo del software Nartac

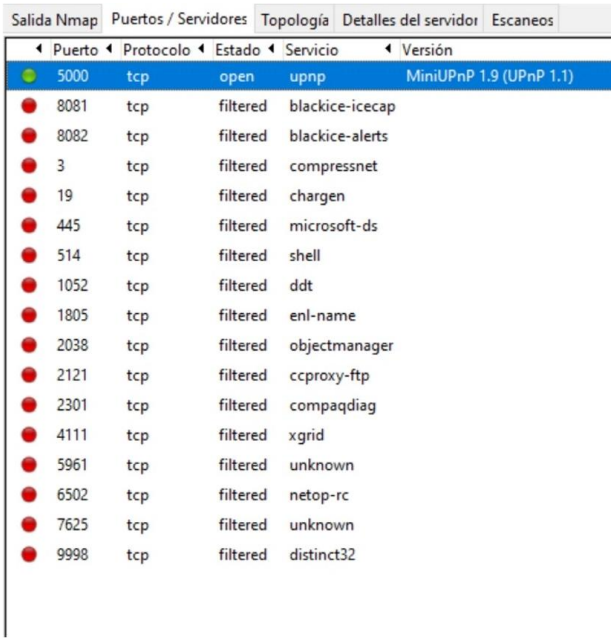
Gracias a la herramienta de **Nmap** se realizó un mapeo de red el cual nos arroja resultados muy interesantes con respecto a los servicios y servidores usados; debido a la seguridad de la empresa no nos fue permitido usar toda la evidencia encontrada

Figura 8. Evidencia de escaneo del servidor

Fuente: Elaboración propia con base a pantallazo del software Nmap

Se pudo deducir gracias al escaneo de puerto que se realizó que no tenía puertos abiertos

Figura 9. Evidencia de escaneo de puertos

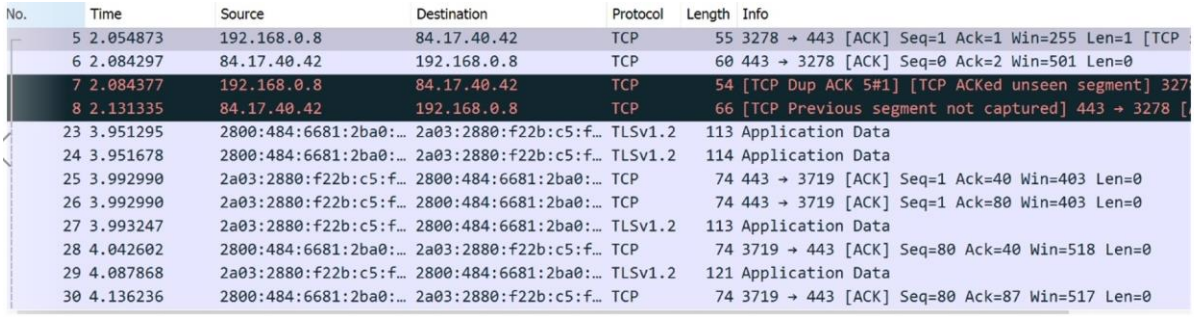


Puerto	Protocolo	Estado	Servicio	Versión
5000	tcp	open	upnp	MiniUPnP 1.9 (UPnP 1.1)
8081	tcp	filtered	blackice-icecap	
8082	tcp	filtered	blackice-alerts	
3	tcp	filtered	compressnet	
19	tcp	filtered	chargen	
445	tcp	filtered	microsoft-ds	
514	tcp	filtered	shell	
1052	tcp	filtered	ddt	
1805	tcp	filtered	enl-name	
2038	tcp	filtered	objectmanager	
2121	tcp	filtered	ccproxy-ftp	
2301	tcp	filtered	compaqdiag	
4111	tcp	filtered	xgrid	
5961	tcp	filtered	unknown	
6502	tcp	filtered	netop-rc	
7625	tcp	filtered	unknown	
9998	tcp	filtered	distinct32	

Fuente: Elaboración propia con base a pantallazo del software Nmap

Gracias a la herramienta utilizada llamada **Wireshark** logramos capturas de tráfico por los protocolos UDP y TCP el cual con una debida decodificación nos podría arrojar información muy valiosa lo cual perjudicaría gravemente la empresa

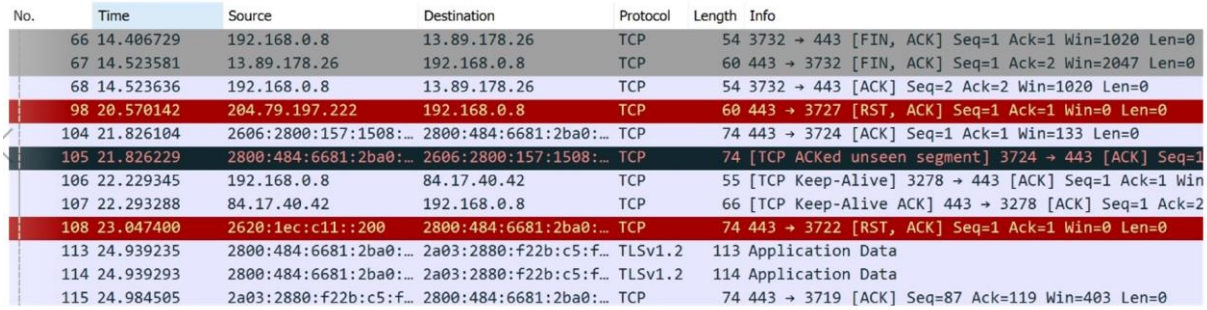
Figura 10. Evidencias de tráficos de red capturados



No.	Time	Source	Destination	Protocol	Length	Info
5	2.054873	192.168.0.8	84.17.40.42	TCP	55	3278 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP
6	2.084297	84.17.40.42	192.168.0.8	TCP	60	443 → 3278 [ACK] Seq=0 Ack=2 Win=501 Len=0
7	2.084377	192.168.0.8	84.17.40.42	TCP	54	[TCP Dup ACK 5#1] [TCP ACKed unseen segment] 327
8	2.131335	84.17.40.42	192.168.0.8	TCP	66	[TCP Previous segment not captured] 443 → 3278 [
23	3.951295	2800:484:6681:2ba0:…	2a03:2880:f22b:c5:f…	TLSv1.2	113	Application Data
24	3.951678	2800:484:6681:2ba0:…	2a03:2880:f22b:c5:f…	TLSv1.2	114	Application Data
25	3.992990	2a03:2880:f22b:c5:f…	2800:484:6681:2ba0:…	TCP	74	443 → 3719 [ACK] Seq=1 Ack=40 Win=403 Len=0
26	3.992990	2a03:2880:f22b:c5:f…	2800:484:6681:2ba0:…	TCP	74	443 → 3719 [ACK] Seq=1 Ack=80 Win=403 Len=0
27	3.993247	2a03:2880:f22b:c5:f…	2800:484:6681:2ba0:…	TLSv1.2	113	Application Data
28	4.042602	2800:484:6681:2ba0:…	2a03:2880:f22b:c5:f…	TCP	74	3719 → 443 [ACK] Seq=80 Ack=40 Win=518 Len=0
29	4.087868	2a03:2880:f22b:c5:f…	2800:484:6681:2ba0:…	TLSv1.2	121	Application Data
30	4.136236	2800:484:6681:2ba0:…	2a03:2880:f22b:c5:f…	TCP	74	3719 → 443 [ACK] Seq=80 Ack=87 Win=517 Len=0

Fuente: Elaboración propia con base a pantallazo del software Wireshark

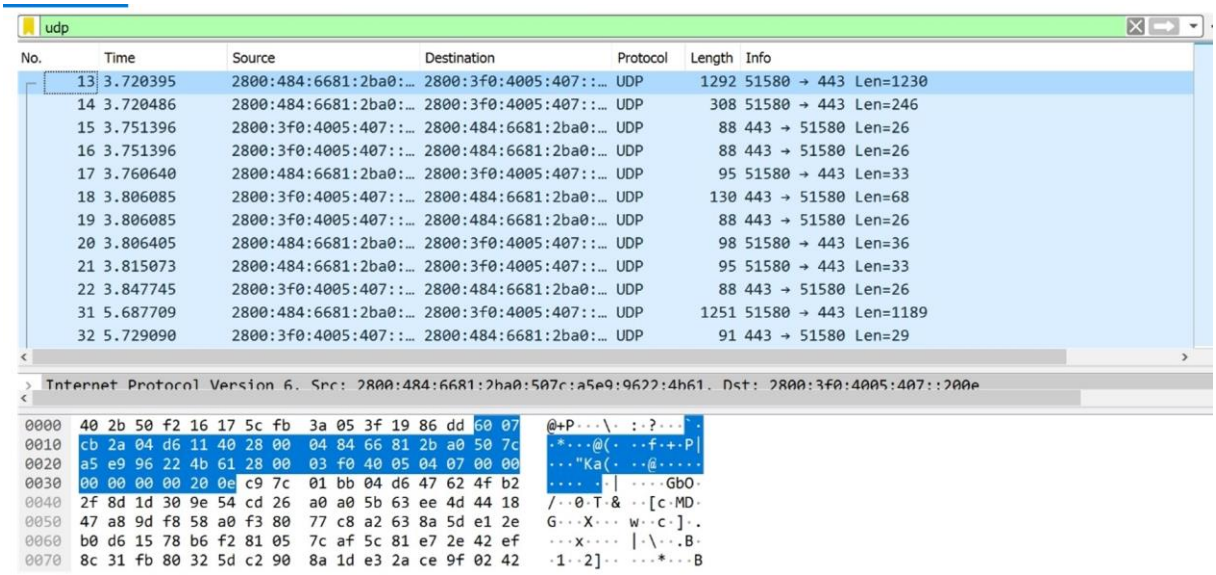
Figura 11. Evidencias de tráficos de red capturados 2



No.	Time	Source	Destination	Protocol	Length	Info
66	14.406729	192.168.0.8	13.89.178.26	TCP	54	3732 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
67	14.523581	13.89.178.26	192.168.0.8	TCP	60	443 → 3732 [FIN, ACK] Seq=1 Ack=2 Win=2047 Len=0
68	14.523636	192.168.0.8	13.89.178.26	TCP	54	3732 → 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0
98	20.570142	204.79.197.222	192.168.0.8	TCP	60	443 → 3727 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104	21.826104	2606:2800:157:1508:…	2800:484:6681:2ba0:…	TCP	74	443 → 3724 [ACK] Seq=1 Ack=1 Win=133 Len=0
105	21.826229	2800:484:6681:2ba0:…	2606:2800:157:1508:…	TCP	74	[TCP ACKed unseen segment] 3724 → 443 [ACK] Seq=1
106	22.229345	192.168.0.8	84.17.40.42	TCP	55	[TCP Keep-Alive] 3278 → 443 [ACK] Seq=1 Ack=1 Win
107	22.293288	84.17.40.42	192.168.0.8	TCP	66	[TCP Keep-Alive ACK] 443 → 3278 [ACK] Seq=1 Ack=2
108	23.047400	2620:1ec:c11::200	2800:484:6681:2ba0:…	TCP	74	443 → 3722 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	24.939235	2800:484:6681:2ba0:…	2a03:2880:f22b:c5:f…	TLSv1.2	113	Application Data
114	24.939293	2800:484:6681:2ba0:…	2a03:2880:f22b:c5:f…	TLSv1.2	114	Application Data
115	24.984505	2a03:2880:f22b:c5:f…	2800:484:6681:2ba0:…	TCP	74	443 → 3719 [ACK] Seq=87 Ack=119 Win=403 Len=0

Fuente: Elaboración propia con base a pantallazo del software Wireshark

Figura 12. Evidencias de tráficos de red capturados 3



udp

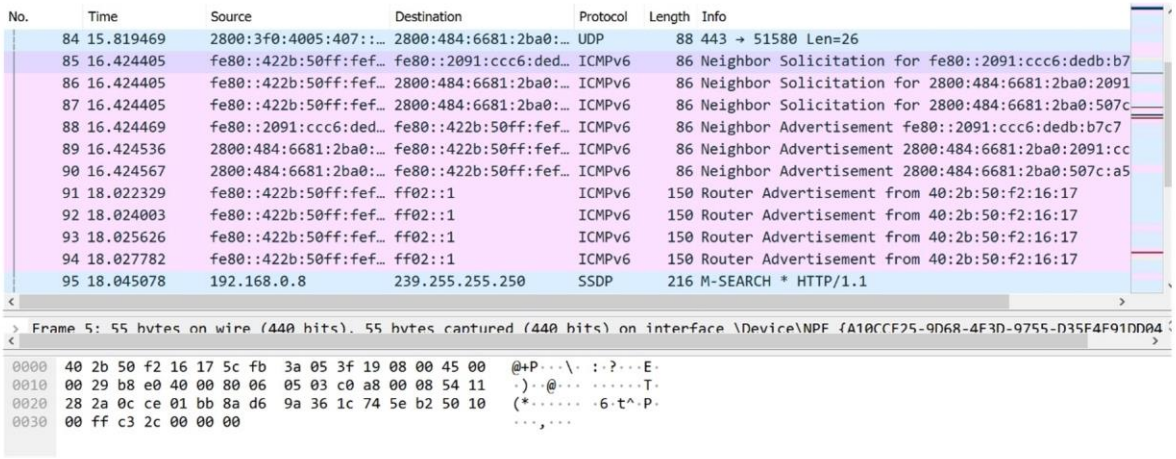
No.	Time	Source	Destination	Protocol	Length	Info
13	3.720395	2800:484:6681:2ba0:…	2800:3f0:4005:407::…	UDP	1292	51580 → 443 Len=1230
14	3.720486	2800:484:6681:2ba0:…	2800:3f0:4005:407::…	UDP	308	51580 → 443 Len=246
15	3.751396	2800:3f0:4005:407::…	2800:484:6681:2ba0:…	UDP	88	443 → 51580 Len=26
16	3.751396	2800:3f0:4005:407::…	2800:484:6681:2ba0:…	UDP	88	443 → 51580 Len=26
17	3.760640	2800:484:6681:2ba0:…	2800:3f0:4005:407::…	UDP	95	51580 → 443 Len=33
18	3.806085	2800:3f0:4005:407::…	2800:484:6681:2ba0:…	UDP	130	443 → 51580 Len=68
19	3.806085	2800:3f0:4005:407::…	2800:484:6681:2ba0:…	UDP	88	443 → 51580 Len=26
20	3.806405	2800:484:6681:2ba0:…	2800:3f0:4005:407::…	UDP	98	51580 → 443 Len=36
21	3.815073	2800:484:6681:2ba0:…	2800:3f0:4005:407::…	UDP	95	51580 → 443 Len=33
22	3.847745	2800:3f0:4005:407::…	2800:484:6681:2ba0:…	UDP	88	443 → 51580 Len=26
31	5.687709	2800:484:6681:2ba0:…	2800:3f0:4005:407::…	UDP	1251	51580 → 443 Len=1189
32	5.729090	2800:3f0:4005:407::…	2800:484:6681:2ba0:…	UDP	91	443 → 51580 Len=29

Internet Protocol Version 6, Src: 2800:484:6681:2ba0:507c:a5e9:9622:4b61, Dst: 2800:3f0:4005:407::200e

```
0000  40 2b 50 f2 16 17 5c fb  3a 05 3f 19 86 dd 60 07   @+P···\· :·?···`·
0010  cb 2a 04 d6 11 40 28 00  04 84 66 81 2b a0 50 7c   ·*···@(· ··f·+·P|
0020  a5 e9 96 22 4b 61 28 00  03 f0 40 05 04 07 00 00   ···"Ka(· ··@·····
0030  00 00 00 00 20 0e c9 7c  01 bb 04 d6 47 62 4f b2   ···· ·|· ····GbO·
0040  2f 8d 1d 30 9e 54 cd 26  a0 a0 5b 63 ee 4d 44 18   /··0·T·& ··[c·MD·
0050  47 a8 9d f8 58 a0 f3 80  77 c8 a2 63 8a 5d e1 2e   G···X··· w··c·]··
0060  b0 d6 15 78 b6 f2 81 05  7c af 5c 81 e7 2e 42 ef   ···x···· |·\···B·
0070  8c 31 fb 80 32 5d c2 90  8a 1d e3 2a ce 9f 02 42   ·1··2]·· ···*···B
```

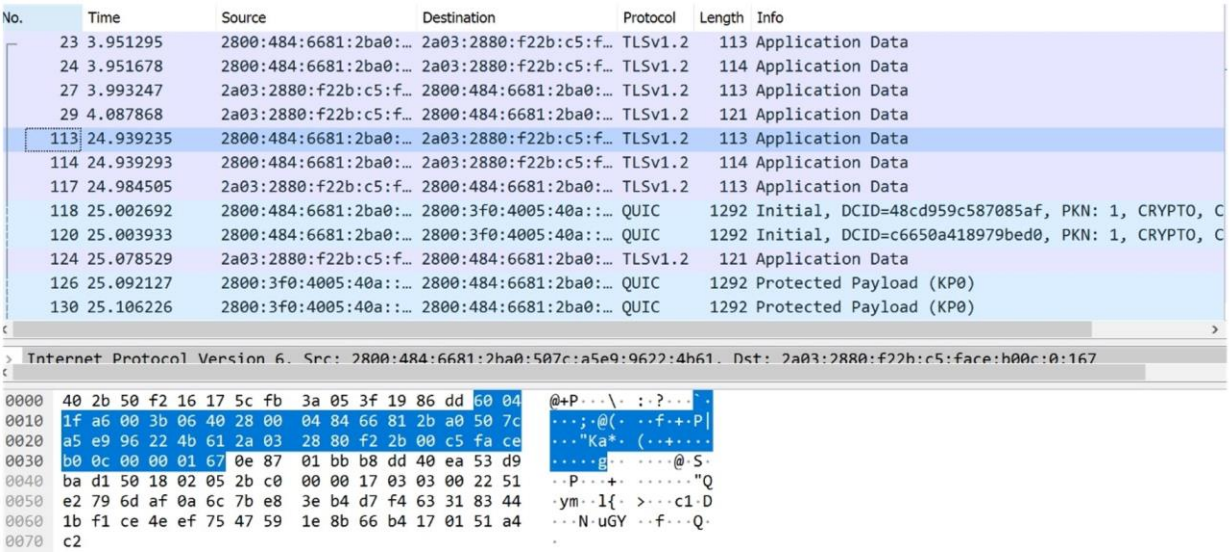
Fuente: Elaboración propia con base a pantallazo del software Wireshark

Figura 13. Evidencias de tráficos de red capturados 4



Fuente: Elaboración propia con base a pantallazo del software Wireshark

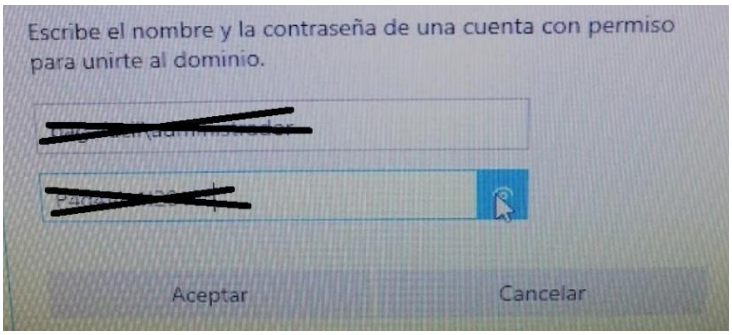
Figura 14. Evidencias de tráficos de red capturados 5



Fuente: Elaboración propia con base a pantallazo del software Wireshark

Se logró capturar información muy valiosa como contraseñas y usuarios de servidores, documentos de usuarios, firmas digitales, números de cuentas entre otros. La cual no se puede mostrar por seguridad y privacidad de la empresa Finanzas al Día S.A.S.

Figura 15. Evidencias de tráficos de red capturados 5



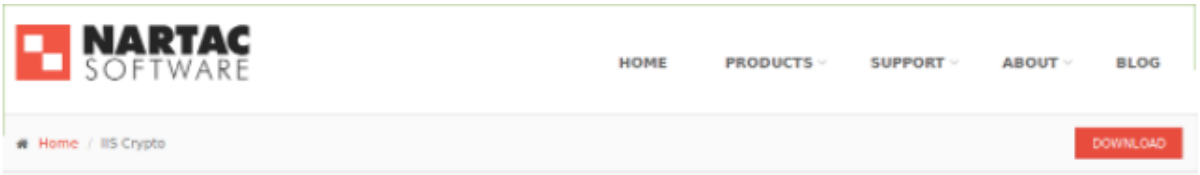
Fuente: Elaboración propia

5. DISCUSIÓN

De acuerdo al plan de mitigación de riesgos se procedió a la ejecución del proceso de configuración de la aplicación afectada, con esta se evita el uso de cifrado RC4, utilizando los nuevos modos de cifrado autentificados y así habilitando el uso de TLS 1.2 con las suites AES-GCM.

Este conjunto de cifrado utilizando el cifrado autenticados AES-GCM con algoritmo de datos asociados (AEAD) AEAD_AES_128_GCM y AEAD_AES_256_GCM. Tomando en consideración que cada uno de estos algoritmos AEAD está conformado por una etiqueta de autentificación de 128 bits con GCM. El "nonce" o número aleatorio utilizado una única vez, este tendrá 12 bytes de longitud y es parcialmente implícito. Partiendo de que el "nonce" se genera como parte del proceso de reconocimiento y es estático durante toda la sesión y la otra parte se transporta en cada paquete.
Para llegar a cabo la actualización se descarga un paquete que contiene IIS Crypto GUI.

Figura 15. Software NARTAC

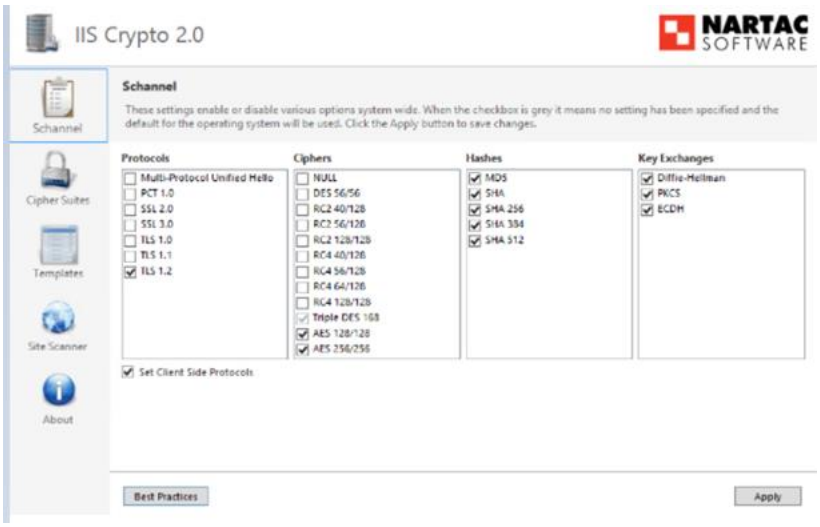


Fuente: Elaboración propia con base a pantallazo del software Nartac

Siendo esta una herramienta que tiene como fin permitir a los administradores habilitar o deshabilitar protocolos inseguros, suites de cifrado, hashes y mecanismos de intercambio de claves en Windows Server 2008, 2012, 2016 y 2019.

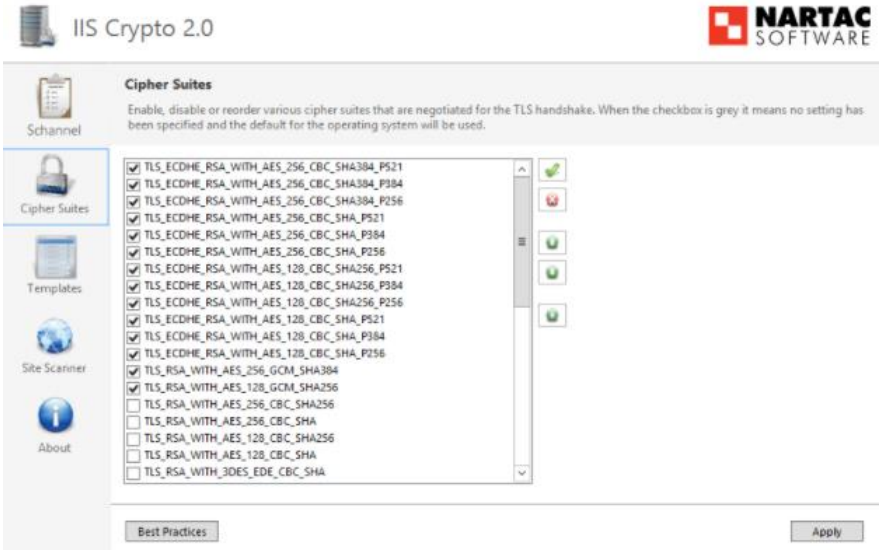
Una vez que se instala la aplicación se ingresa y esta nos permite de una manera ágil y sencilla modificar los protocolos, suites de cifrado y hashes que se requiera en la máquina.

Figura 15. Evidencia de configuración de cifrado adecuado



Fuente: Elaboración propia con base a pantallazo del software Nartac

Figura 16. Evidencia de configuración de cifrado adecuado 2



Fuente: Elaboración propia con base a pantallazo del software Nartac

En el momento que se ha finalizado los ajustes y la aplicación de ellos se reinicia el sistema para que se hagan efectivos los cambios.

Después del plan de mitigación de riesgos podemos evidenciar que las vulnerabilidades de alto impacto antes encontradas, no se hacen presentes después de realizar las configuraciones y actualizaciones necesarias en la red, por lo tanto, se mejora y se complementan los niveles de seguridad en la red empresarial.

Figura 17. Escaneo de red después de la mitigación de vulnerabilidades

Fuente: Elaboración propia con base a pantallazo del software Nessus

Como se puede evidenciar en la imagen anterior después de realizar las correcciones necesarias se detalla que las vulnerabilidades antes encontradas en la infraestructura de la red empresarial se encuentran mitigadas gracias a las actualizaciones y adecuaciones de los servicios SSL de los SUITES de encriptación, lo que mejora considerablemente la seguridad de los datos, ya que se manejaban datos como firmas digitales, cuentas bancarias, autorizaciones por entidades financieras.
Efectuadas las correcciones de vulnerabilidad se evidencia una mayor confiabilidad en el manejo de los datos, teniendo en cuenta que la empresa anteriormente era vulnerable a ataques cibernéticos tales como SWEET32, DDoS, MAN in the MIDDLE, PHISHING, entre otros.

6. CONCLUSIONES

De acuerdo con los objetivos planteados el estudio ha sido exitoso, ya que se mitigaron las vulnerabilidades encontradas en una red empresarial, después de un análisis profundo logramos evidenciar que había riesgos de alto impacto de los cuales no se tenía conocimiento. Gracias a las herramientas utilizadas y la información recolectada; se realizó un análisis exhaustivo para el estudio de los riesgos, lo cual nos llevó a generar un plan para la mitigación de riesgos y así evitar posibles irrupciones en la red empresarial.

Con este proyecto se dio solución a un problema que ha ido tomando gran relevancia en el día de hoy como es la ciberseguridad, buscando y analizando vulnerabilidades que resulten altamente peligrosas para la red empresarial.

En conclusión, se analizó la infraestructura de red empresarial correctamente con las herramientas, metodologías y conocimientos adquiridos en el diplomado de seguridad informática, evidenciando los diferentes tipos de vulnerabilidades de las cuales no se tenía idea por falta de conocimientos por parte de los empleados y el departamento de TI sobre los certificados SSL y sus cifrados de intensidad.

Gracias a las herramientas utilizadas y técnicas manejadas, las cuales facilitan el estudio de manera más profunda de la red empresarial, se logró un desglosamiento minucioso para así poder clasificar las vulnerabilidades de menor a mayor riesgo, para lograr una mitigación de cada una de ellas.
Mediante el estudio realizado a la infraestructura de red, se realizó un plan de mitigación ya que se debió actualizar o generar un nuevo certificado que pudiese contrarrestar los riesgos que presenta un sistema con un cifrado deficiente, para así evitar la pérdida de información o ingreso de personal no autorizado hacía datos confidenciales.

7. REFERENCIAS

Advisors. (s.f.). advisors. Recuperado de https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

Alevsk. (s.f.). Blog de Alevsk. Recuperado de https://www.alevsk.com/2010/07/ettercap-potente-herramienta-de-auditorias-lan/

Arguello, F. (13 de 10 de 2020). infoteknico. Recuperado de https://www.infoteknico.com/que-es-wireshark-y-como-se-utiliza/

ARTUNDUAGA, J. F. (2021). Diseño De Un Plan De Seguridad Informática Para Un Plan De Información. Neiva: Universidad Cooperativa De Colombia.

Avast Academy Team. (7 de 10 de 2016). Avast. Recuperado de https://www.avast.com/es-es/c-ddos#gref

Bartolín, J. A. (2008). Seguridad de la Información Redes, informática y sistemas de información. España.

Belcic, I. (22 de 09 de 2020). Avast. Recuperado de https://www.avast.com/es-es/c-sql-injection#gref

Belcic, I. (5 de 2 de 2020). Avast. Recuperado de https://www.avast.com/es-es/c-phishing#gref

Bembibre, V. (01 de 01 de 2009). Definición ABC. Obtenido de https://www.definicionabc.com/tecnologia/router.php

COLOMBIA, E. C. (2009). www.sic.gov.co. Recuperado de www.sic.gov.co: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Conpilar News. (13 de 04 de 2021). ConPILAR news. Recuperado de https://conpilar.es/que-es-md5/

DigiCert. (2021). Digicert. Recuperado de https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https

Huerta, A. V. (07 de 2002). Recuperado de https://www.rediris.es/cert/doc/unixsec/unixsec.pdf

ISOTools Excellence. (21 de 05 de 2015). SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Iformación. Obtenido de https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

KB.IWEB.COM. (25 de 04 de 2019). KB.IWEB.COM. Recuperado de https://kb.iweb.com/hc/es/articles/230268628-Vulnerabilidades-SSL-TLS-Ataques-POODLE-BEAST-SWEET32-y-la-muerte-de-SSLv3-Aviso-de-Seguridad-Open-SSL?mobile_site=true

Latto, N. (22 de 7 de 2020). Avast. Obtenido de https://www.avast.com/es-es/c-what-is-doxxing#gref

Malenkovich, S. (10 de 04 de 2013). Kaspersky daily. Recuperado de https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/

Malwarebytes. (s.f.). Malwarebytes. Obtenido de https://es.malwarebytes.com/malware/

MariadelaFuente. (29 de 04 de 2019). mariadelafuente. Recuperado de https://www.marindelafuente.com.ar/que-es-nmap-por-que-necesitas-este-mapeador-de-red/

MINISTERIO DE COMERCIO, I. Y. (15 de 01 de 2021). politica documentos electronicos mincit. Recuperado de https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.mincit.gov.co/servicio-ciudadano/transparencia-acceso-informacion/documentos/politica-documentos-electronicos-mincit-20210115.aspx&ved=2ahUKEwirg5Oa_Iz2AhWQRDABHScJD5AQFnoECBUQAQ&usg=AOvVaw2

Netlinux. (s.f.). netlinux. Recuperado de https://www.netlinux.cl/servicios-linux/servidor-de-respaldo

Ortiz, A. E. (05 de 03 de 2019). https://www.hostdime.com.pe. Recuperado de https://www.hostdime.com.pe: https://www.hostdime.com.pe/blog/acerca-puertos-tcp-udp-comparacion-similitudes-diferencias/#:~:text=Tanto%20TCP%20como%20UDP%20son,sobre%20el%20protocolo%20de%20Internet.&text=UDP%20es%20un%20protocolo%20sin,IP%20(TCP%20%2F%20IP).

Panda Security. (S.F.). Panda Security. Recuperado de https://www.pandasecurity.com/es/security-info/exploit/

Santos C., J. M., Correa P., R. S., Cárdenas Santa M., M., Diaz G., S., & Molano V., D. (18 de 10 de 2012). funcionpublica.gov.co. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.