EDP UNIVERSITY OF PUERTO RICO, INC.

RECINTO DE HATO REY

PROGRAMA DE MAESTRÍA EN SISTEMAS DE INFORMACIÓN

CON ESPECIALIDAD EN SEGURIDAD DE INFORMACIÓN E INVESTIGACIÓN DE FRAUDE

DAVID KENT, FUNDADOR DEL WEBSITE DE REDES DE PETRÓLEO Y GAS SE DECLARA CULPABLE DE UN CARGO DE FRAUDE INFORMÁTICO

Requisito Para La Maestría En Sistemas De Información

Con Especialidad En Seguridad De Información E Investigación De Fraude

MARZO, 2021

PREPARADO POR

CARMEN M. COLON COLON

Sirva la presente para certificar que el Proyecto de Investigación titulado:

DAVID KENT, FUNDADOR DEL WEBSITE DE REDES DE PETRÓLEO Y GAS SE DECLARA CULPABLE DE UN CARGO DE FRAUDE INFORMÁTICO

Preparado por

Carmen M. Colón Colón

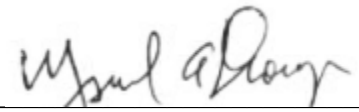
Ha sido aceptado como requisito parcial para el grado de

Maestría En Sistemas De Información

Con Especialidad En Seguridad De Información E Investigación De Fraude

Marzo, 2021

Aprobado por:



DR. MIGUEL A. DROUYN MARRERO

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN Y TRASFONDO

Introducción

En el ámbito de la seguridad de la información, la Autenticación, la Autorización y el Control de Acceso son las tres consideraciones más importantes que todo profesional de seguridad de sistemas necesita para dar siempre la máxima prioridad. Se debe implementar un sistema de autenticación riguroso si un profesional de sistemas espera establecer una infraestructura que sea inmune a los ataques cibernéticos. En el mundo criminalmente avanzado de hoy, no se puede confiar en la autenticación de un solo factor para evitar intrusiones no deseadas y eso hace que la presencia de un modelo de autenticación de múltiples factores sea una necesidad más que un lujo. La autorización de usuarios dentro de un sistema también es un proceso que debe implementarse rigurosamente. En esencia, la autorización implica la verificación realizada por un sistema para determinar si un usuario solicitante puede acceder para ver o editar un recurso o no.

David Kent, de Spring, Texas, EEUU, fue sentenciado a prisión en octubre del 2016 por hackear Rigzone.com, un website de la industria del petróleo y de gas que fundó y vendió al negocio de datos laborales DHI Group, luego creó un segundo website, Oilpro.com, con el cual pretendía robar datos de clientes para aumentar su valor. Una denuncia penal revela que el caso contra Kent se inició desde antes del 2014. Fue entonces cuando DHI Group Inc., que había comprado el website de Kent, Rigzone, se preocupó de que el sitio hubiera sido violado y le tendió una trampa al pirata informático que usaba dos cuentas de clientes falsas como cebo. Las autoridades afirman que Kent, que ahora dirige el website de empleo Oilpro, supuestamente hackeó Rigzone y robó información del currículum de más de 700,000 cuentas de clientes.

Descripción del Caso

- Número del caso - S1 16 Cr. 385 (DLC) U.S v. David Kent
- Partes en el caso
    - Acusado(s) - David W. Kent, Jr., CEO de Single Integrated Operations Portal, Inc.
    - Víctimas u otras personas o entidades involucradas - DHI GROUP, INC
- Investigadores - Diego Rodríguez, subdirector a cargo del FBI
- Abogados - Joon H. Kim
- Fiscales - Sidhardha Kamaraju, Fiscal federal adjunto y Andrew K. Chan, Fiscal federal adjunto
- Jueces - Hon. Denise L. Cote, Distrito Sur de Nueva York

Trasfondo

Según Kent (2021) David W. Kent es un arquitecto y desarrollador de software con sede en Texas que recientemente se desempeñó como presidente de Oilpro.com. Fundó la red profesional para la industria del petróleo y el gas en 2013 y la convirtió en una operación comercial exitosa con un equipo de 15 empleados responsables de ventas, desarrollo, operaciones y marketing. Antes de esto, David W. Kent se desempeñó durante 12 años como fundador y presidente de Rigzone.com. Durante este tiempo, diseñó y desarrolló soluciones de software de petróleo y gas, incluido su servicio de datos patentado RigLogix para rastrear todas las plataformas de perforación en alta mar del mundo.

Kent vendió Rigzone.com en 2011 por $51 millones. Había fundado la empresa mientras estaba en la Universidad Metodista del Sur, de la cual se graduó magna cum laude con una licenciatura

en sistemas de información gerencial y una especialización en economía. Estudiante becado en SMU, ganó el premio Anderson Consulting Best Senior Award y también fue miembro del equipo de tenis de la escuela. En un momento, estuvo clasificado entre los 100 mejores jugadores de Texas.

Al ser diagnosticado con cáncer, Kent lanzó Cancercorner.org para compartir artículos e investigaciones sobre la prevención y el tratamiento del cáncer. También es un piloto con licencia con calificaciones de vuelo por instrumentos y multimotor. Además de volar y jugar al tenis, participa activamente en el ministerio de asistencia alimentaria en el área de Houston.

Una denuncia criminal proporciona detalles interesantes sobre el trabajo del detective involucrado en descubrir pistas y al cerebro detrás del acceso en línea supuestamente no autorizado. La investigación expone la creación de un website de la industria del petróleo y el gas y la venta de este por $51 millones. Luego, la misma persona que creó ese primer website, crea otro similar al que había vendido y, finalmente, intenta venderlo a las mismas personas que le compraron el primero.

Descripción de Hechos

Según USA vs. Kent (2017), en el 2000, David Kent fundó un website que, en parte, ofrecía a los profesionales de la industria del petróleo y el gas la posibilidad de establecer contactos mediante la publicación de currículos y otra información personal y profesional. Después de crear una cuenta en el website, el usuario inicia sesión con un nombre de usuario y una contraseña. Kent

obtuvo ingresos de este website a través de la venta de publicidad y tarifas de reclutadores y empleadores que buscaban solicitantes de empleo.

En agosto de 2010, una empresa que cotiza en bolsa con sede en la ciudad de Nueva York le pagó a Kent $51 millones por el website. En el momento de la venta, la base de datos de miembros valía alrededor de $6 millones.

Kent se desempeñó como ejecutivo durante el primer año de transición de su ex website a nuevos propietarios. Luego renunció en septiembre de 2011 y fundó un nuevo negocio, Oilpro, otra empresa de redes en línea al servicio de los profesionales de la industria petrolera.

A partir de octubre de 2013, Kent presuntamente accedió a la base de datos de miembros de su antiguo website sin la autorización o permiso de los nuevos propietarios. Una vez que Kent obtuvo acceso a la base de datos del website, robó información, entre las que se encontraban las identidades y perfiles de unas 700,000 cuentas de clientes. Además de este allanamiento de morada digital, uno de los empleados de Oilpro de Kent parece haber pirateado la cuenta de Google Analytics del antiguo website y reenviado los datos a Kent.

Kent utilizó esos datos robados y envió invitaciones a todos los miembros de su antiguo website para unirse a Oilpro.com. En abril de 2014, Kent se puso en contacto con el director ejecutivo de la empresa que había comprado su antiguo website y le contó sobre cómo Oilpro había recibido una oferta de inversión no solicitada. Usando esa premisa, Kent supuestamente le explicó al CEO

que su misión original al establecer Oilpro era construir otro website que la compañía del CEO pudiera adquirir.

Después de más de un año de comunicaciones sobre la posible venta de Oilpro a la empresa que había adquirido el primer website, Kent y el director ejecutivo, director financiero y asesor general de la empresa adquirente realizaron una teleconferencia para discutir la propuesta de adquisición de Oilpro. Kent manifestó que Oilpro había aumentado su membresía a través de un marketing estándar supuestamente legal.

El 14 de abril de 2014, las cuentas de miembros ficticios que el primer website creó por sospechas de piratería recibieron un correo electrónico de un empleado de Oilpro solicitando una membresía. Al rastrear cómo el empleado de Oilpro obtuvo la información de contacto, se descubrió que el 17 de octubre de 2013, se enviaron alrededor de 100,000 solicitudes HTTP a la base de datos de miembros mediante el uso de lo que se identificó como un comando Get Resume, que fue diseñado para explotar un fragmento de código fuente exclusivo del primer website y conocido solo por algunas personas, incluido Kent. Esta fue solo la primera ronda de hacks identificada.

Acusaciones, Cargos y Penalidades

- Ley de Fraude y Abuso Informático (CFAA), 18 U.S.C. § 1030
- Ley de Acceso a Comunicaciones Electrónicas y De Alambres Almacenados (ECPA), 18 U.S.C. §§ 2510-2523

- Fue sentenciado a 5 años en prisión en octubre de 2017 por conspiración y obligado a pagar más de $3 millones en restitución.
- Un Caso Civil continúa demandando una condena máxima de 20 años en prisión por Fraude Electrónico y pagar $20 millones en restitución.

Definición de Términos

- Autenticación: es la verificación de las credenciales proporcionadas con las presentes en la base de datos (Vera-Cruz, C., 2020).
- Autorización: es el proceso mediante el cual un sistema determina si el usuario posee privilegios suficientes para acceder a los recursos solicitados o no (Vera-Cruz, C., 2020).
- Control de Acceso: es el proceso mediante el cual el acceso a esos recursos se restringe a un número seleccionado de usuarios (Vera-Cruz, C., 2020).

REVISION DE LITERATURA

Introducción

El siguiente informe presenta la investigación realizada sobre el caso de fraude cibernético cometido por David Kent, fundador de Oilpro. De igual manera, se discuten los fraudes involucrados, las leyes aplicables, dos ejemplos de casos relacionados y las herramientas de investigación forense utilizadas para la obtención de evidencia.

Fraudes Involucrados

Todos los artículos en referencia utilizados para el análisis del caso ofrecen un resumen de este. Uno de los artículos indica que en julio de 2017 Oilpro anunció que cerraba operaciones (Blum, 2017). El segundo menciona que, como parte de un acuerdo de culpabilidad, Kent acordó no apelar ninguna sentencia de 4 años o menos (Raymond, 2016). Por último, el tercer articulo explica como DHI se preocupó de que el website hubiera sido violado y le tendió una trampa a Kent usando dos cuentas de clientes falsas como cebo (Mangan, 2016).

En el artículo Hacking 101, Anton Gesmundo (Gesmundo, 2018) ofrece ideas sobre cómo es la mente de un hacker. Después de todo, el primer paso para una gran defensa es conocer la ofensiva del oponente. Un ataque a la información no siempre se lleva a cabo de la misma manera, lo que significa que los hackers siempre se vuelven creativos con sus enfoques. No importa cuán único sea el enfoque, todavía existe una metodología genérica para llevar a cabo un ataque:

1. Reconocimiento: obtener información sobre el objetivo y cómo ingresar al sistema de destino.

2. Explotación: obtener acceso al sistema o ingresar al sistema.
3. Escalada de privilegios: obtener más acceso, como privilegios de administrador o comandos de consola.
4. Dejar un oyente: para mantener el progreso del hackeo y continuar el exploit en otro momento.
5. Extracción de datos: el ataque real de tomar la información necesaria.
6. Cubrir pistas: borrar registros, archivos o comandos creados para evitar que el administrador del sistema los descubra.

En última instancia, la prevención de un intento de hackeo dependerá de cuán preparado esté el sistema para los dos primeros pasos.

El documento The Global Risks Report 2018 (Collins, 2018), explica que los riesgos de ciberseguridad también están creciendo, tanto en su prevalencia como en su potencial disruptivo. Los ataques contra empresas casi se han duplicado en cinco años, y los incidentes que alguna vez se hubieran considerado extraordinarios se están volviendo cada vez más comunes. El impacto financiero de las infracciones de ciberseguridad está aumentando, y algunos de los mayores costos en 2017 se relacionaron con los ataques de ransomware, que representaron el 64% de todos los correos electrónicos maliciosos. Ejemplos notables incluyeron el ataque WannaCry, que afectó a 300,000 computadoras en 150 países, y NotPetya, que causó pérdidas trimestrales de $300 millones para varias empresas afectadas. Otra tendencia creciente es el uso de ciberataques para atacar infraestructura crítica y sectores industriales estratégicos, lo que genera temores de que, en

el peor de los casos, los atacantes podrían desencadenar una falla en los sistemas que mantienen funcionando a las sociedades.

Leyes Aplicables

Las leyes aplicables son las siguientes:

- Ley de Fraude y Abuso Informático (CFAA), 18 U.S.C. § 1030: Prohíbe el acceso intencional a una computadora sin autorización o en exceso de autorización, aunque no define lo que significa “sin autorización”.
- Ley de Acceso a Comunicaciones Electrónicas y De Alambres Almacenados (ECPA), 18 U.S.C. §§ 2510-2523: Prohíbe la interceptación, uso, divulgación o procuración de cualquier otra persona, real o intentado, para interceptar o intentar interceptar cualquier comunicación por cable, oral o electrónica.
- Fue sentenciado a 5 años en prisión en octubre de 2017 por conspiración y obligado a pagar más de $3 millones en restitución.
- Un Caso Civil continúa demandando una condena máxima de 20 años en prisión por Fraude Electrónico y pagar $20 millones en restitución.

Casos Relacionados

Los casos relacionados al fraude cibernético cometido por David Kent son el de Matthew Keys y Aaron Swartz.

El 14 de marzo de 2013, Matthew Keys (United States v. Matthew Keys, 2016), un ex editor de redes sociales de Reuters fue acusado de múltiples cargos de violaciones de la CFAA por

supuestamente proporcionar a hackers nombres de usuario y contraseñas del website de Tribune Company a fines de 2010 después de que lo despidieran de su trabajo en Tribune. El gobierno alega que esta conducta fue parte de una conspiración para realizar cambios no autorizados en el website de Tribune y dañar sus computadoras. La acusación formal acusa tres violaciones criminales de la CFAA, incluida la conspiración para causar daño a una computadora protegida, la transmisión de un código malicioso y el intento de transmisión de un código malicioso.

Por otra parte, Aaron Swartz (United States v. Aaron Swartz, 2013), un programador de computadoras, empresario y activista fue acusado federalmente de múltiples cargos de fraude electrónico y violaciones de la CFAA, incluida la obtención ilegal de información de una computadora protegida y el daño imprudente de una computadora protegida. Los cargos se derivaron del supuesto esfuerzo de Swartz para descargar aproximadamente 4.8 millones de artículos de JSTOR, biblioteca digital sin fines de lucro, utilizando la red del MIT (Massachusetts Institute of Technology). Cualquiera en el campus del MIT podía acceder a su red y, como resultado, a JSTOR, pero los términos de servicio de JSTOR limitaban la cantidad de artículos que se podían descargar a la vez. Swartz escribió un código (script) que le indicaba a su computadora que descargara artículos de JSTOR continuamente y, cuando se detectó esta violación y se denegaron las solicitudes de su computadora, Swartz falsificó la dirección de su computadora para engañar a los servidores de JSTOR.

Herramientas de Investigación

La herramienta forense de investigación utilizada para la obtención de evidencia es la siguiente:

- Forensic Toolkit (FTK) (Dodt, C., 2019): Es una herramienta de software de investigaciones digitales citada por los tribunales creada para ayudar a los clientes a encontrar pruebas relevantes más rápido, aumentar drásticamente la velocidad del análisis y reducir los retrasos.

SIMULACIÓN (RECREACIÓN EXPERIMENTAL)

Una denuncia criminal proporciona detalles interesantes sobre el trabajo del detective involucrado en descubrir pistas y al cerebro detrás del acceso en línea supuestamente no autorizado. La investigación expone la creación de un website de la industria del petróleo y el gas y la venta de este por $51 millones. Luego, la misma persona que creó ese primer website, crea otro similar al que había vendido y, finalmente, intenta venderlo a las mismas personas que le compraron el primero.

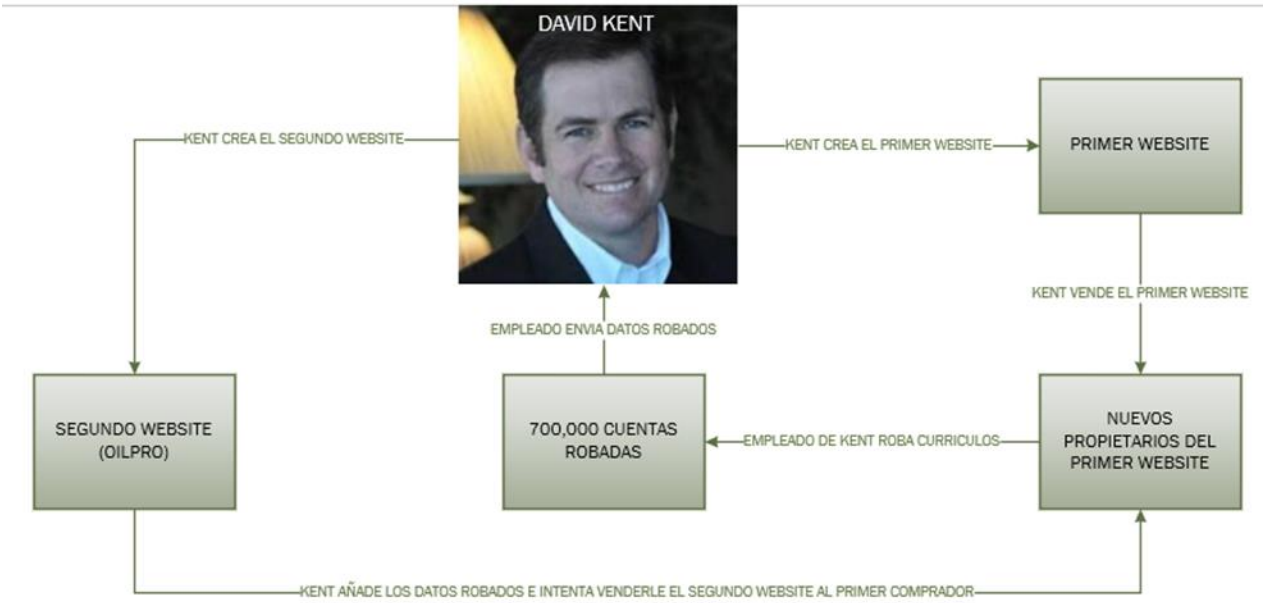


Figura 1.1: Diagrama de simulación del fraude.

A partir de octubre de 2013, Kent presuntamente accedió a la base de datos de miembros de su antiguo website sin la autorización o permiso de los nuevos propietarios. Una vez que Kent obtuvo acceso a la base de datos del website, robó información, entre las que se encontraban las

identidades y perfiles de unas 700,000 cuentas de clientes. Además de este allanamiento de morada digital, uno de los empleados de Oilpro de Kent parece haber pirateado la cuenta de Google Analytics del antiguo website y reenviado los datos a Kent.

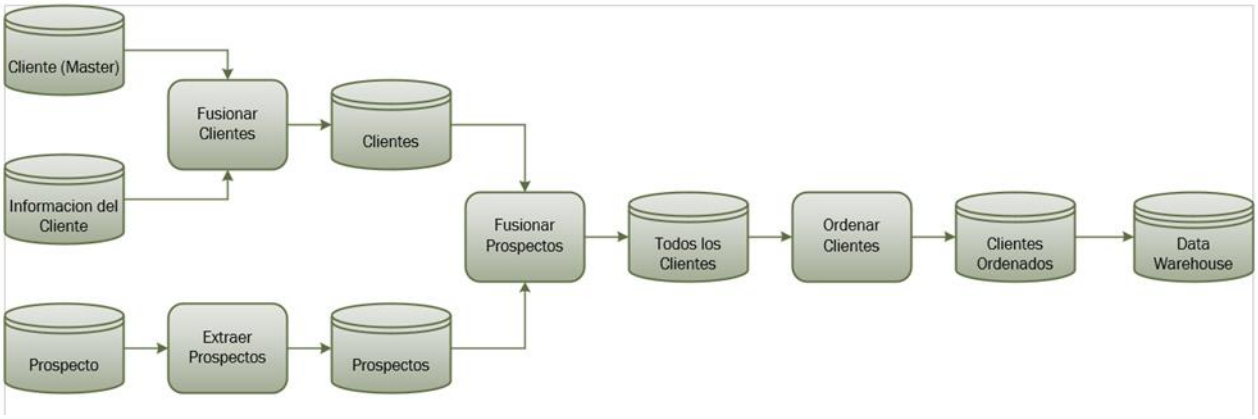


Figura 1.2: Acceso indebido a la Base de Datos.

Kent utilizó esos datos robados y envió invitaciones a todos los miembros de su antiguo website para unirse a Oilpro.com. En abril de 2014, Kent se puso en contacto con el director ejecutivo de la empresa que había comprado su antiguo website y le contó sobre cómo Oilpro había recibido una oferta de inversión no solicitada. Usando esa premisa, Kent supuestamente le explicó al CEO que su misión original al establecer Oilpro era construir otro website que la compañía del CEO pudiera adquirir.

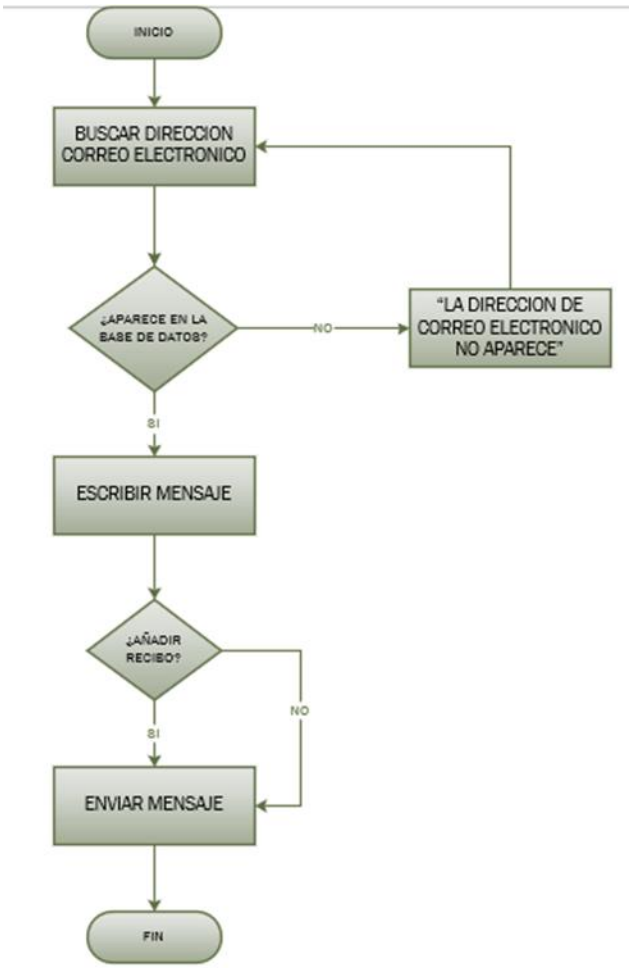


Figura 1.3: Correo electrónico de invitación a Oilpro.

El 14 de abril de 2014, las cuentas de miembros ficticios que el primer website creó por sospechas de piratería recibieron un correo electrónico de un empleado de Oilpro solicitando una membresía. Al rastrear cómo el empleado de Oilpro obtuvo la información de contacto, se descubrió que el 17 de octubre de 2013, se enviaron alrededor de 100,000 solicitudes HTTP a la base de datos de miembros mediante el uso de lo que se identificó como un comando Get Resume, que fue diseñado para explotar un fragmento de código fuente exclusivo del primer website y conocido solo por algunas personas, incluido Kent. Esta fue solo la primera ronda de hacks identificada.

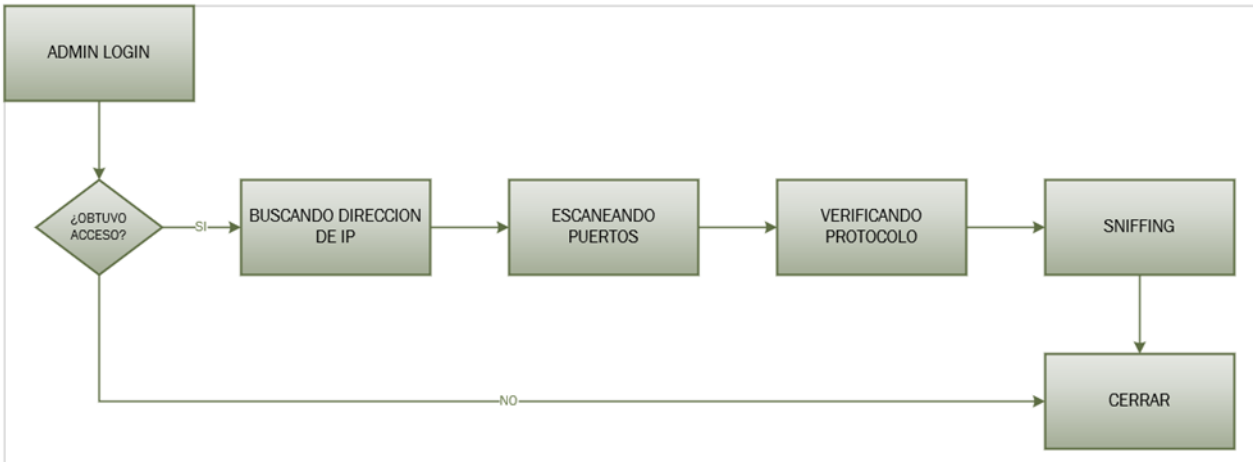


Figura 1.4: Acceso indebido al Servidor.

INFORME DEL CASO (PERITO)

Resumen Ejecutivo

El FBI es una agencia federal de investigación e inteligencia con jurisdicción en una amplia gama de delitos federales; asuntos de seguridad nacional como terrorismo y espionaje; intrusiones y delitos cibernéticos e informáticos; y actividades de inteligencia relacionadas con esas misiones.

El FBI en conjunto con la Oficina de Estafas y Seguridad y su subdirector, Diego Rodríguez, ha solicitado nuestros servicios para descubrir el posible fraude electrónico por parte de David Kent. El Sr. Kent es sospechoso de infiltrarse indebidamente al sistema de base de datos de la compañía DHI. De igual manera, se alega que el Sr. Kent tiene cómplices infiltrados en DHI los cuales en horas laborables copian información de usuarios usando el equipo de la compañía. El Sr. Rodríguez entiende que la imagen creada de un dispositivo USB para ser analizada podría contener evidencia inculpatoria vital para el arresto de David Kent y sus cómplices.

Objetivo

El FBI contrata los servicios de C3 Security con el objetivo de analizar y descubrir información electrónica en una imagen creada de un dispositivo USB, con el propósito de obtener posible material de evidencia que ayude a la Oficina de Estafas y Seguridad a acusar y lograr el arresto de David Kent.

Alcance Del Trabajo

El 27 de abril de 2020 Diego Rodríguez le hace entrega a Carmen M. Colón Colón (Investigadora Forense de C3 Security) de una imagen creada de un dispositivo USB y visto por la Oficina de Estafas y Seguridad como posible dispositivo contenedor de evidencia. Esto con el propósito de analizar el mismo ya que existe el interés de encontrar datos relevantes que sirvan como evidencia inculpatoria contra David Kent. C3 Security tiene la tarea de descubrir, recuperar y preservar cualquier evidencia relevante encontrada en la imagen creada de un dispositivo USB con el propósito de ser analizada y posteriormente ser presentada como evidencia por el Sr. Rodríguez. Siguiendo los estándares de la industria forense se comienza el proceso de análisis utilizando la siguiente tecnología:

- Forensic Toolkit (FTK)

La herramienta antes mencionada es considerada estándar de excelencia en la industria de la investigación forense y es altamente aceptada en procesos investigativos conducidos por el FBI, Interpol y múltiples agencias de ley y orden. Esto garantiza que el proceso investigativo realizado por C3 Security cumple o excede los requisitos establecidos por el Gobierno Federal para el procesamiento, preparación y entrega de evidencia a ser utilizada en cualquier proceso judicial. Dejando esto establecido C3 Security comienza con el proceso de adquisición y análisis de evidencia. C3 Security creará un informe de hallazgos y los notificará por medio escrito al Sr. Rodríguez para ser evaluados y tomar la acción legal correspondiente con relación a los acusados envueltos en los incidentes en cuestión.

Datos Del Caso

- Número de caso: 008
- Investigador: Carmen M. Colón Colón
- Cliente: Oficina de Estafas y Seguridad del FBI
- Representante del Cliente: Diego Rodríguez

Descripción De Los Dispositivos Utilizados

A continuación, se detallan los dispositivos utilizados durante el proceso investigativo:

- Desktop HP, modelo Pavilion 500 PC donde residen todas las herramientas y aplicaciones que serán utilizadas en este proceso.
- Ultra Block USB Write Blocker - Dispositivo USB que permite la adquisición de información de un disco sin crear la posibilidad de que se dañe accidentalmente el contenido de la unidad original de donde se extrae la data. Esto es logrado al bloquear cualquier comando de escritura al dispositivo analizado y convirtiéndolo en un device read-only.
- Imagen creada de un dispositivo USB - SanDisk, modelo Cruzer Spark USB 2.0 No. de Serie R-REM-WDT-SDCZ61. Entregado a C3 Security por el Sr. Rodríguez.

Resumen De Hallazgos

El proceso de Análisis Forense Digital envuelve la adquisición, preservación, análisis y presentación de evidencia digital. Este tipo de evidencia es frágil y el investigador podría, sin darse cuenta alterar o destruir la información contenida en algún dispositivo que está siendo objeto de análisis. Esto trae como consecuencia que esta evidencia sea declarada inadmisible ante un

tribunal. Para minimizar la posibilidad de que esto suceda C3 Security utiliza como referencia el Electronic Data Recovey Model (EDRM) para así obtener una evidencia correctamente preservada, integra y confiable, convirtiéndola así en evidencia electrónica defendible jurídicamente.

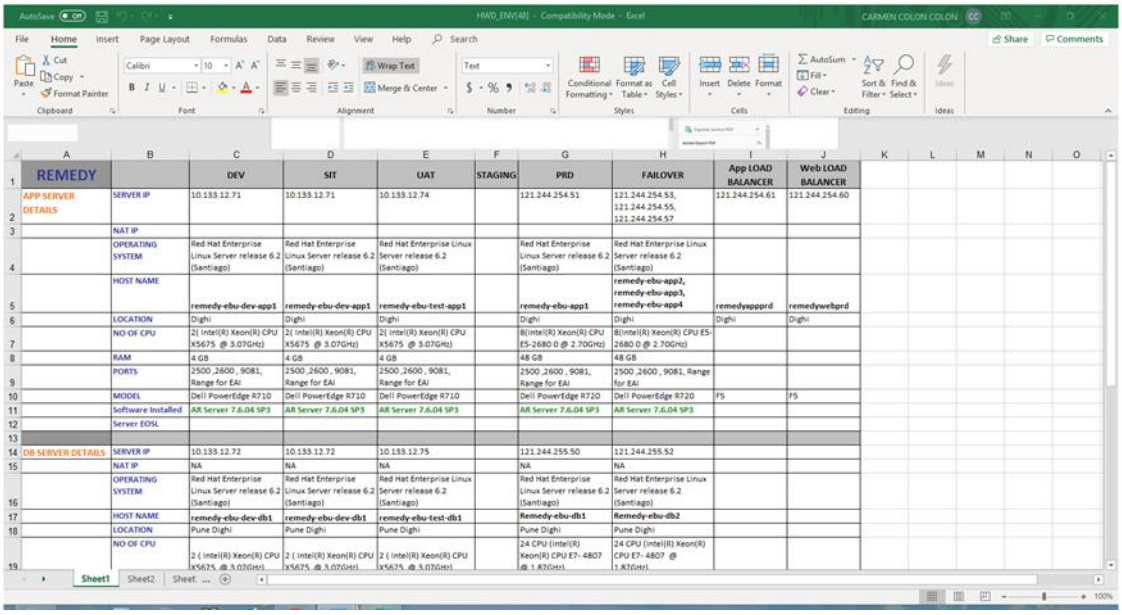
Luego de culminar el proceso de análisis del contenedor de evidencia (SanDisk, modelo Cruzer Spark USB 2.0 No. de Serie R-REM-WDT-SDCZ61) y por medio de la herramienta Forensic Toolkit (FTK) logramos descubrir múltiples archivos en los siguientes formatos:

- .xls
- .eml
- .jpg

Los archivos analizados se catalogan de dos formas:

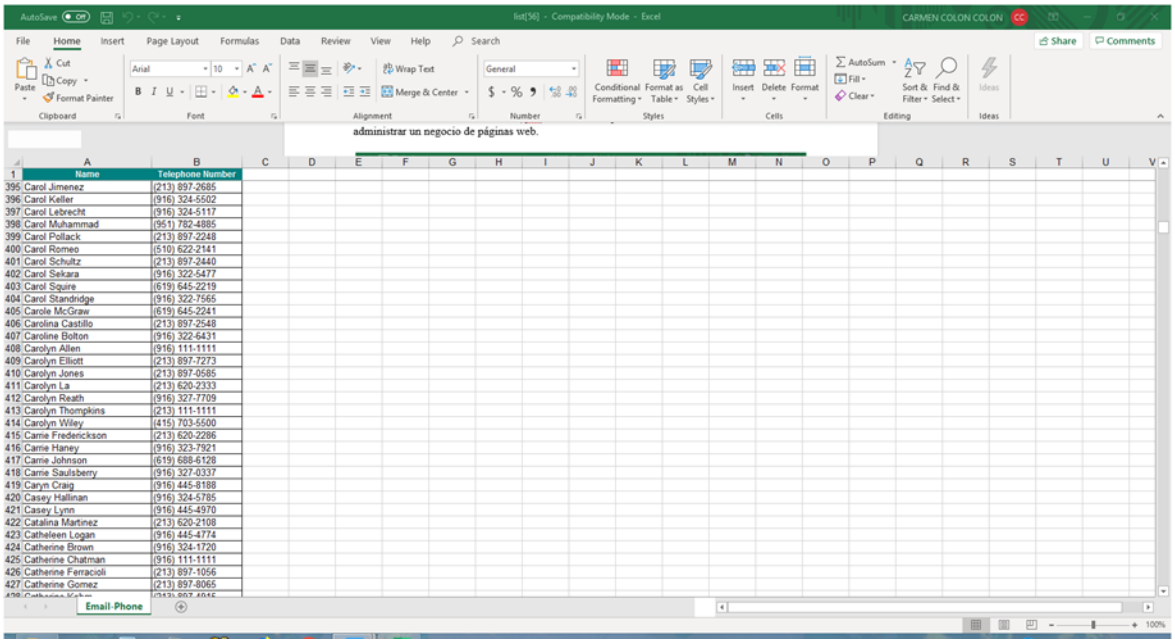
- Existentes: descubiertos a simple vista al observar el contenido de la imagen en FTK.
- Borrados: archivos descubiertos luego de analizar la imagen con la opción de recuperación de archivos borrados.

A continuación, se detallan los archivos encontrados que por la naturaleza de la información contenida se catalogan como evidencia inculpatoria con relación a los sospechosos en este caso:



REMEDY		DEV	SIT	UAT	STAGING	PRD	FAILOVER	App LOAD BALANCER	Web LOAD BALANCER
APP SERVER DETAILS	SERVER IP	10.133.12.71	10.133.12.71	10.133.12.74		121.244.254.51	121.244.254.53, 121.244.254.55, 121.244.254.57	121.244.254.61	121.244.254.60
	NAT IP								
	OPERATING SYSTEM	Red Hat Enterprise Linux Server release 6.2 (Santiago)	Red Hat Enterprise Linux Server release 6.2 (Santiago)	Red Hat Enterprise Linux Server release 6.2 (Santiago)		Red Hat Enterprise Linux Server release 6.2 (Santiago)	Red Hat Enterprise Linux Server release 6.2 (Santiago)		
	HOST NAME	remedy-ebu-dev-app1	remedy-ebu-dev-app1	remedy-ebu-test-app1		remedy-ebu-app1	remedy-ebu-app2, remedy-ebu-app3, remedy-ebu-app4	remedyappprd	remedywebprd
	LOCATION	Dighi	Dighi	Dighi		Dighi	Dighi	Dighi	Dighi
	NO OF CPU	2(Intel(R) Xeon(R) CPU X5675 @ 3.07GHz)	2(Intel(R) Xeon(R) CPU X5675 @ 3.07GHz)	2(Intel(R) Xeon(R) CPU X5675 @ 3.07GHz)		8(Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz)	8(Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz)		
	RAM	4 GB	4 GB	4 GB		48 GB	48 GB		
	PORTS	2500 ,2600 , 9081, Range for EAI	2500 ,2600 , 9081, Range for EAI	2500 ,2600 , 9081, Range for EAI		2500 ,2600 , 9081, Range for EAI	2500 ,2600 , 9081, Range for EAI		
	MODEL	Dell PowerEdge R710	Dell PowerEdge R710	Dell PowerEdge R710		Dell PowerEdge R720	Dell PowerEdge R720	F5	F5
	Software Installed	AR Server 7.6.04 SP3	AR Server 7.6.04 SP3	AR Server 7.6.04 SP3		AR Server 7.6.04 SP3	AR Server 7.6.04 SP3		
	Server EOSL								
OB SERVER DETAILS	SERVER IP	10.133.12.72	10.133.12.72	10.133.12.75		121.244.255.50	121.244.255.52		
	NAT IP	NA	NA	NA		NA	NA		
	OPERATING SYSTEM	Red Hat Enterprise Linux Server release 6.2 (Santiago)	Red Hat Enterprise Linux Server release 6.2 (Santiago)	Red Hat Enterprise Linux Server release 6.2 (Santiago)		Red Hat Enterprise Linux Server release 6.2 (Santiago)	Red Hat Enterprise Linux Server release 6.2 (Santiago)		
	HOST NAME	remedy-ebu-dev-db1	remedy-ebu-dev-db1	remedy-ebu-test-db1		Remedy-ebu-db1	Remedy-ebu-db2		
	LOCATION	Pune Dighi	Pune Dighi	Pune Dighi		Pune Dighi	Pune Dighi		
	NO OF CPU	2 (Intel(R) Xeon(R) CPU X5675 @ 3.07GHz)	2 (Intel(R) Xeon(R) CPU X5675 @ 3.07GHz)	2 (Intel(R) Xeon(R) CPU X5675 @ 3.07GHz)		24 CPU (Intel(R) Xeon(R) CPU E7- 4807 @ 1.87GHz)	24 CPU (Intel(R) Xeon(R) CPU E7- 4807 @ 1.87GHz)		

Figura 2.1 – existente – tabla de excel (.xls): Documento que muestra el inventario de equipos existentes en la red central de DHI.



administrar un negocio de páginas web.

Name	Telephone Number
Carol Jimenez	(213) 897-2685
Carol Keller	(916) 324-5602
Carol Lebrecht	(916) 324-5117
Carol Muhammad	(951) 782-4885
Carol Pollack	(213) 897-2248
Carol Romeo	(510) 622-2141
Carol Schultz	(213) 897-2440
Carol Sekara	(916) 322-5477
Carol Squire	(619) 645-2219
Carol Standridge	(916) 322-7565
Carole McGraw	(619) 645-2241
Carolina Castillo	(213) 897-2548
Caroline Bolton	(916) 322-6431
Carolyn Allen	(916) 111-1111
Carolyn Elliott	(213) 897-7273
Carolyn Jones	(213) 897-0585
Carolyn La	(213) 620-2333
Carolyn Reath	(916) 327-7709
Carolyn Thompkins	(213) 111-1111
Carolyn Wiley	(415) 703-5600
Carrie Frederickson	(213) 620-2286
Carrie Haney	(916) 323-7921
Carrie Johnson	(619) 688-6128
Carrie Saulsberry	(916) 327-0337
Caryn Craig	(916) 445-8188
Casey Hallinan	(916) 324-5785
Casey Lynn	(916) 445-4970
Catalina Martinez	(213) 620-2108
Catheleen Logan	(916) 445-4774
Catherine Brown	(916) 324-1720
Catherine Chatman	(916) 111-1111
Catherine Ferracioli	(213) 897-1056
Catherine Gomez	(213) 897-8065

Figura 2.2 – existente – tabla de excel (.xls) – Documento que muestra el nombre y el número telefónico de 3,070 clientes.

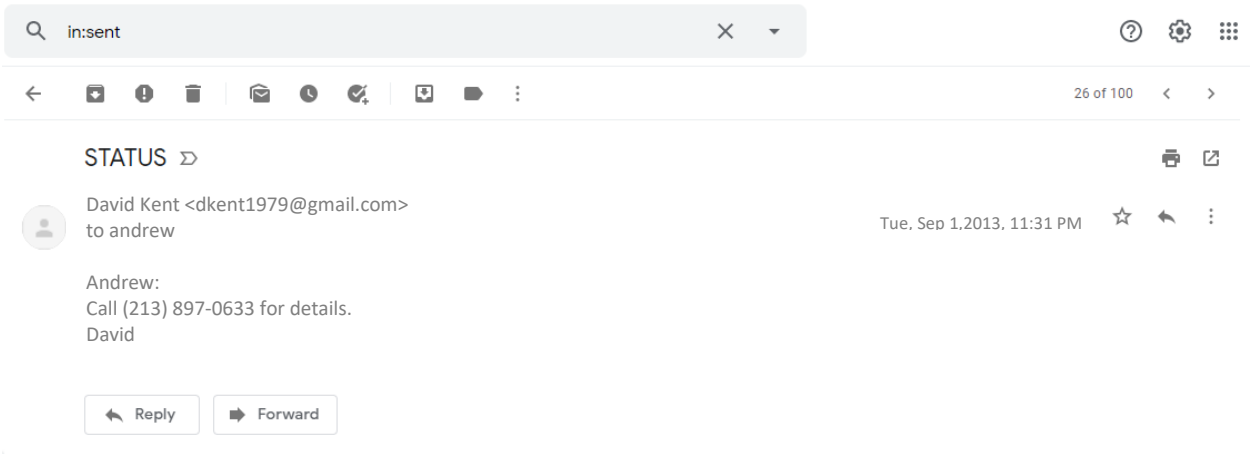


Figura 2.3 – existente – correo electrónico (.eml): Correo electrónico que muestra una conversación entre Andrew y David.

Figura 2.4 – existente – foto (.jpg): Foto que muestra cómo hacer un reset al password de administrador.

A través de las pantallas enumeradas anteriormente se puede ver en detalle evidencia que prueba que David Kent es sospechoso de infiltrarse indebidamente al sistema de base de datos de la compañía DHI. De igual manera, sus cómplices infiltrados en DHI los cuales en horas laborables copian información de usuarios usando el equipo de la compañía.

NOTA: Para ver más detalles sobre el proceso de extracción del contenido del dispositivo y los archivos recuperados a través de FTK, haga referencia a la sección de procedimientos de este reporte.

Cadena De Custodia

Al comenzar nuestro proceso debemos asegurarnos de establecer una cadena de custodia de evidencia íntegra. La cadena de custodia se ocupa de registrar el proceso de adquisición, análisis y control de toda evidencia. En el siguiente documento se detalla la cadena de custodia seguida por C3 Security.

Detalle de la Cadena de Custodia:

Primer Evento:

- Descripción del evento: Evidencia recogida en la Oficina del subdirector del FBI. Evidencia entregada por el Sr. Rodríguez y recogida por la Sra. Colón, investigadora de C3 Security. La evidencia consiste en un SanDisk, modelo Cruzer Spark USB 2.0 No. de Serie R-REM-WDT-SDCZ61.
- Evento verificado por: Carmen M. Colón Colón y Diego Rodríguez.
- Número de evidencia: E-008-2020-04-27

- Fecha de comienzo: abril 27, 2020 – 9:01AM
- Fecha de terminación: abril 27, 2020 – 11:04PM
- Lugar de origen: Oficina del subdirector del FBI
- Destino: Laboratorio Forense – C3 Security

Segundo Evento:

- Descripción del evento: Creación de número de caso y asignación de evidencia al mismo.
- Evento verificado por: Carmen M. Colón Colón
- Número de evidencia: Evidencia # E-008-2020-04-27, Asignada al caso # 008
- Fecha de comienzo: abril 27, 2020 – 12:13PM
- Fecha de terminación: abril 27, 2020 – 12:32PM
- Lugar de origen: Laboratorio Forense – C3 Security
- Destino: Laboratorio Forense – C3 Security.

Tercer Evento:

- Descripción del evento: Proceso de adquisición y análisis de evidencia. Refiérase a la sección de procedimientos en este reporte para detalles específicos del proceso.
- Evento verificado por: Diego Rodríguez.
- Número de evidencia: Evidencia # E-008-2020-04-27, Asignada al caso # 008
- Fecha de comienzo: abril 28, 2020 – 8:00AM
- Fecha de terminación: abril 29, 2020 – 1:02PM
- Lugar de origen: Laboratorio Forense – C3 Security
- Destino: Laboratorio Forense – C3 Security

Cuarto Evento:

- Descripción del evento: Entrega de informe de análisis forense al Sr. Rodríguez para su evaluación. El informe fue entregado directamente al Sr. Rodríguez por la investigadora a cargo de la evidencia, Carmen M. Colón Colón.
- Evento verificado por: Carmen M. Colón Colón y Diego Rodríguez
- Número de evidencia: Reporte referente a la Evidencia # E-008-2020-04-27, Asignada al caso # 008
- Fecha de comienzo: abril 30, 2020 – 9:17AM
- Fecha de terminación: abril 30, 2020 – 10:58AM
- Lugar de origen: Laboratorio Forense – C3 Security
- Destino: Oficina del subdirector del FBI

Quinto Evento:

- Descripción del evento: Devolución de la evidencia original entregada por el Sr. Rodríguez a Carmen M. Colón Colón. La evidencia fue entregada directamente al Sr. Rodríguez por la investigadora a cargo de la evidencia, Carmen M. Colón Colón.
- Evento verificado por: Carmen M. Colón Colón y Diego Rodríguez
- Número de evidencia: Evidencia # E-008-2020-04-27, Asignada al caso # 008
- Fecha de comienzo: abril 30, 2020 – 11:01AM
- Fecha de terminación: abril 30, 2020 – 11:38AM
- Lugar de origen: Laboratorio Forense – C3 Security
- Destino: Oficina del subdirector del FBI

Procedimientos

A continuación, se describen los procedimientos empleados durante el proceso de descubrimiento, adquisición, recuperación y preservación de la evidencia.

1. Procedimiento: creación del caso
    - Herramienta: FTK Forensic Toolkit 1.81
    - Fecha de comienzo: abril 27, 2020 – 12:13PM
    - Fecha de terminación: abril 27, 2020 – 12:32PM
2. Procedimiento: preparación de imagen
    - Captura de la imagen a ser utilizada
    - Herramienta: FTK Forensic Toolkit 1.81
    - Fecha de comienzo: abril 28, 2020 – 8:00AM
    - Fecha de terminación: abril 28, 2020 – 8:29AM
3. Procedimiento: análisis de la imagen
    - En este punto se procesará la imagen para obtener posible evidencia inculpatoria y probar la hipótesis del subdirector del FBI. Se buscarán documentos existentes y borrados (recuperación de estos).
    - Herramienta: FTK Forensic Toolkit 1.81
    - Fecha de comienzo: abril 28, 2020 – 8:34AM
    - Fecha de terminación: abril 29, 2020 – 1:02PM

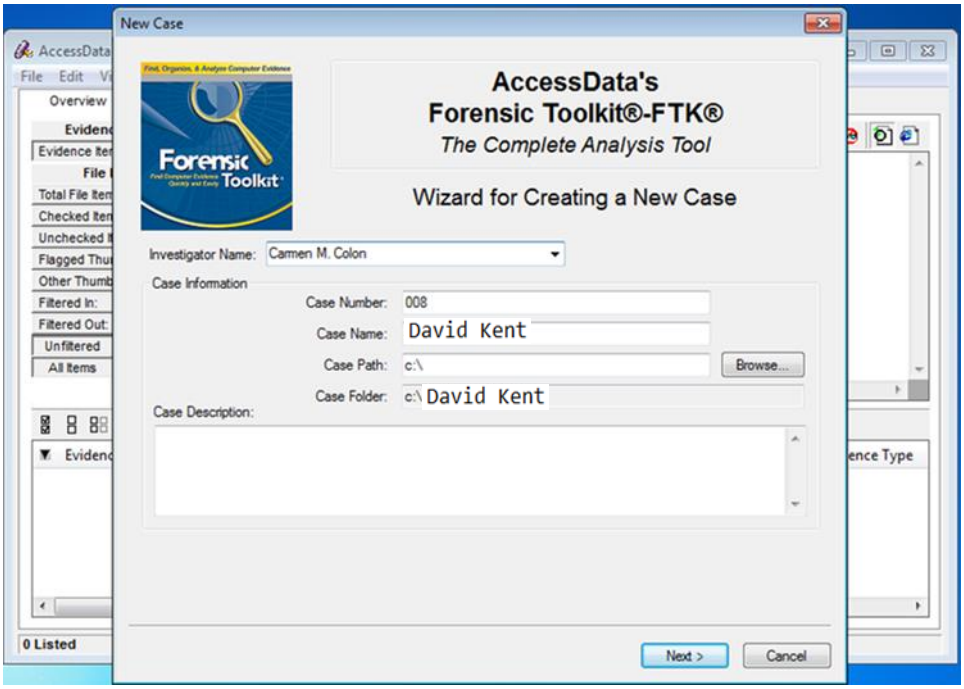


Figura 2.5: Se prepara el caso en FTK Forensic Toolkit 1.81 con toda la información para identificar el mismo.

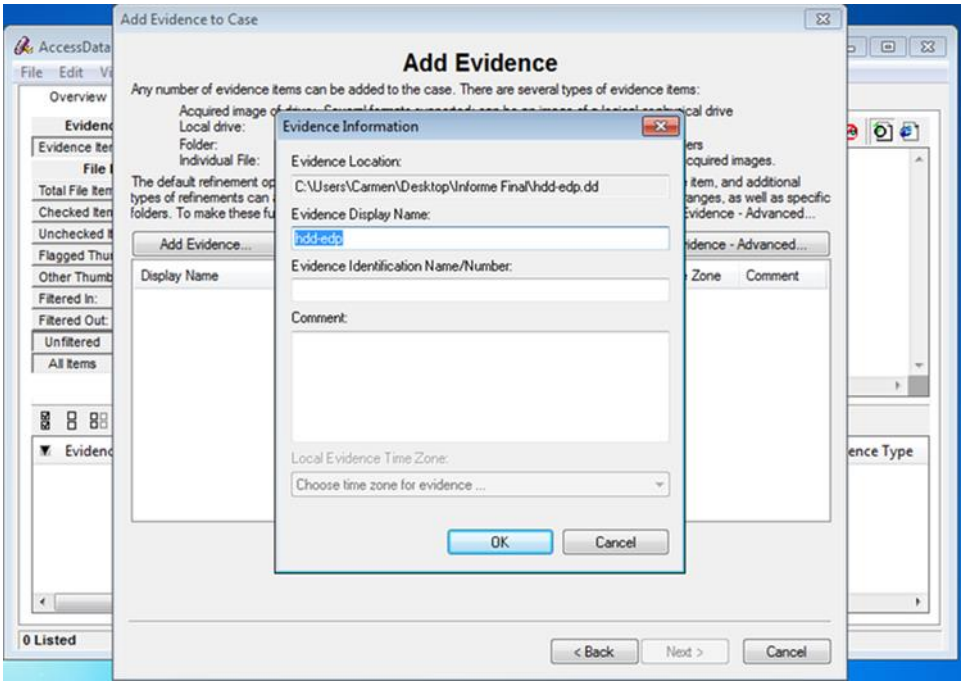


Figura 2.6: Se añade la evidencia a analizar.

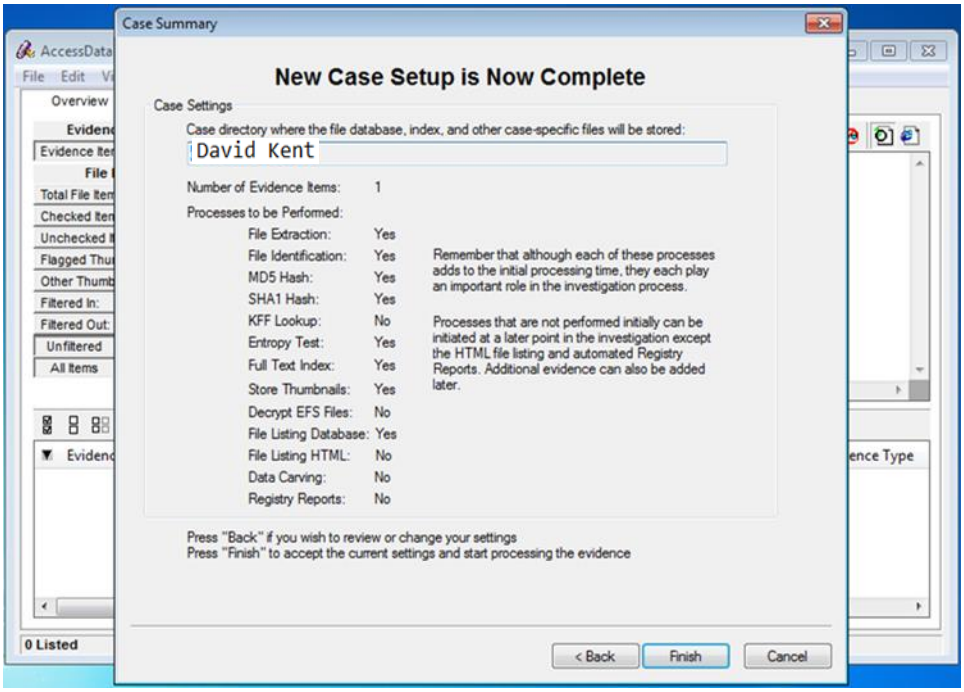


Figura 2.7: Configuración del nuevo caso completado.

Una vez se crea el nuevo caso se verifican los archivos encontrados.

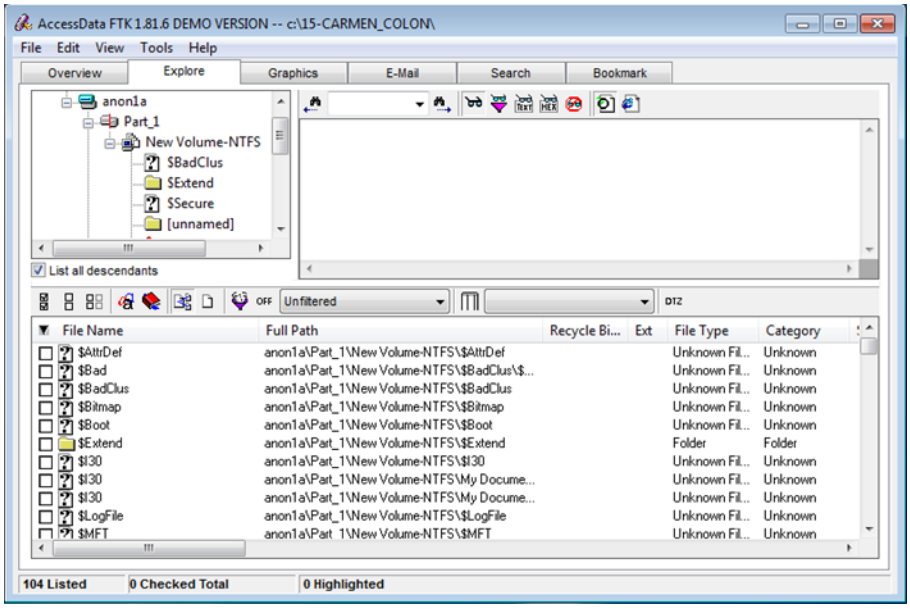


Figura 2.8: Se listaron 104 archivos.

Ya que, verificando archivo por archivo no es una manera eficiente de encontrar evidencia relevante, se procede a usar la búsqueda por palabra clave utilizando Notepad.

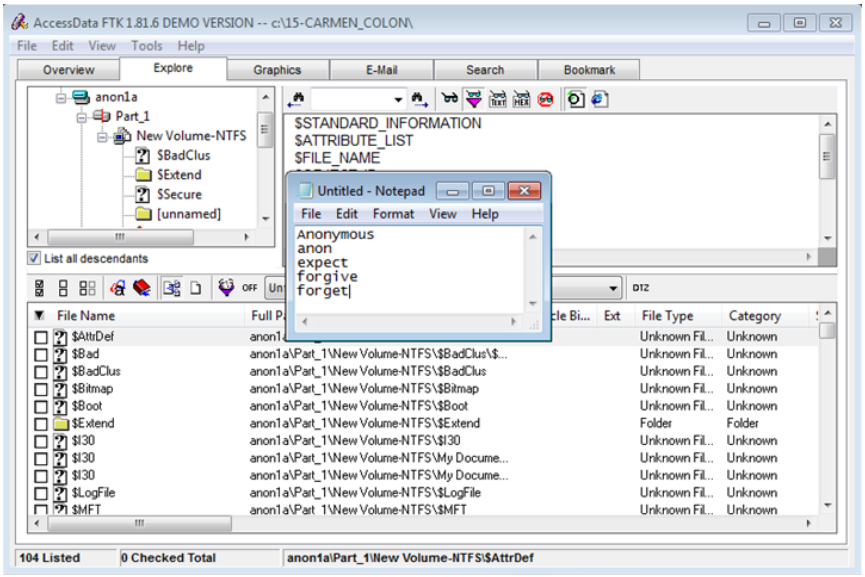


Figura 2.9: Se crearon palabras clave en Notepad y se grabaron en el Desktop.

Se accedió al tab de Search y se escogió la opción de Import para comenzar la búsqueda por palabras clave que se guardaron en Notepad.

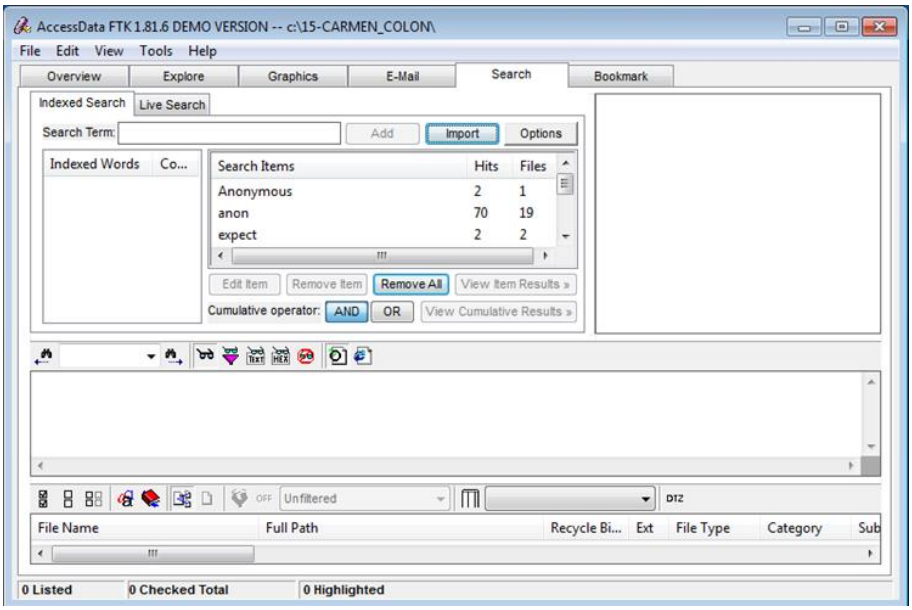


Figura 2.10: Búsqueda por palabras clave. Se encontraron cinco resultados.

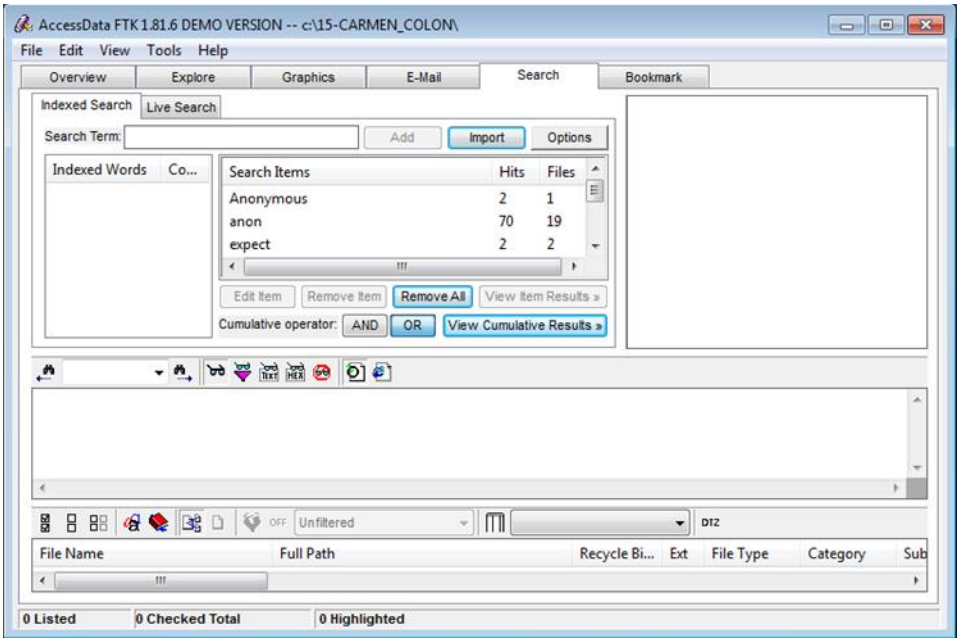


Figura 2.11: Se escogió la opción OR, luego la opción View Cumulative Results.

Se encontraron 81 resultados en 22 archivos.

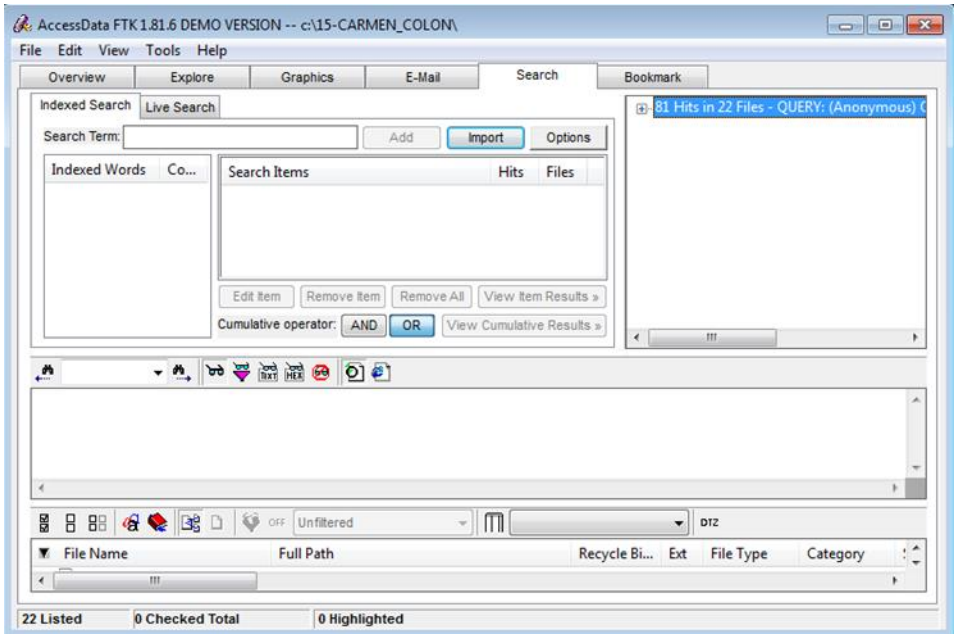


Figura 2.12: Resultados finales.

Se procedió a examinar los Hits.

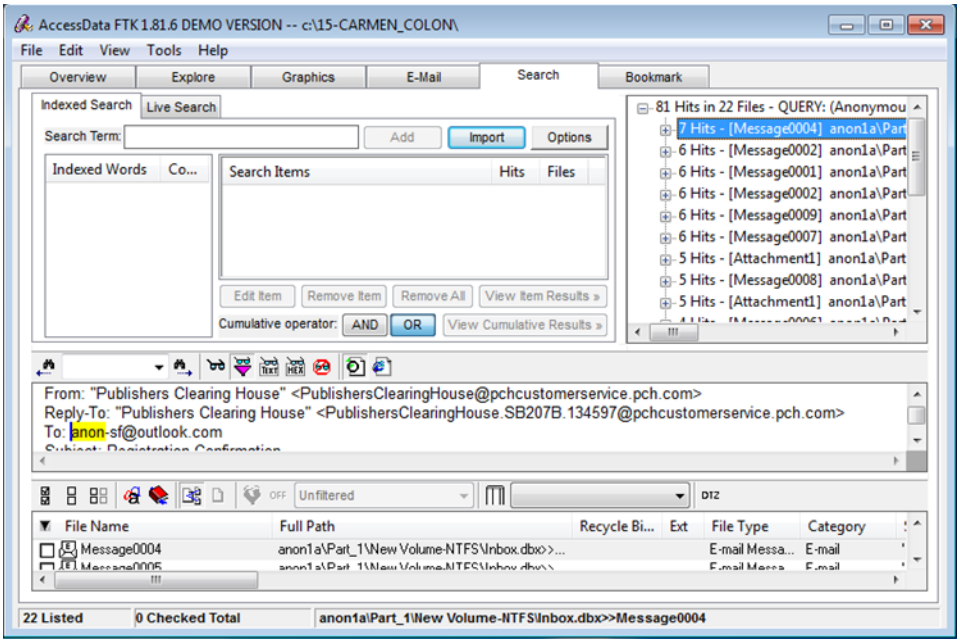


Figura 2.13: Hits, Previews y Files.

Ya que no se encontró evidencia importante se procede a verificar en el tab de Graphics.

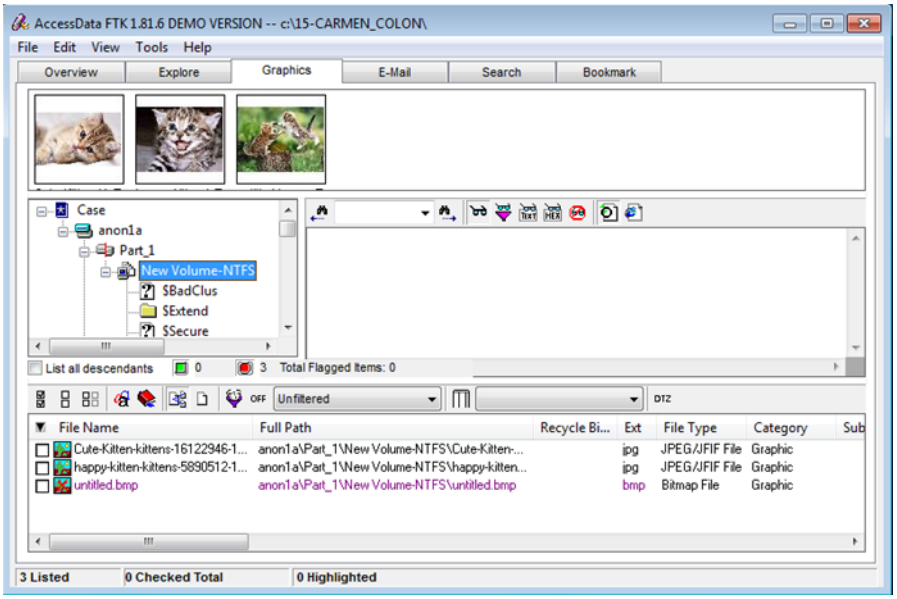


Figura 2.14: Vista de thumbnails.

Examinando se encontró un website incriminatorio.

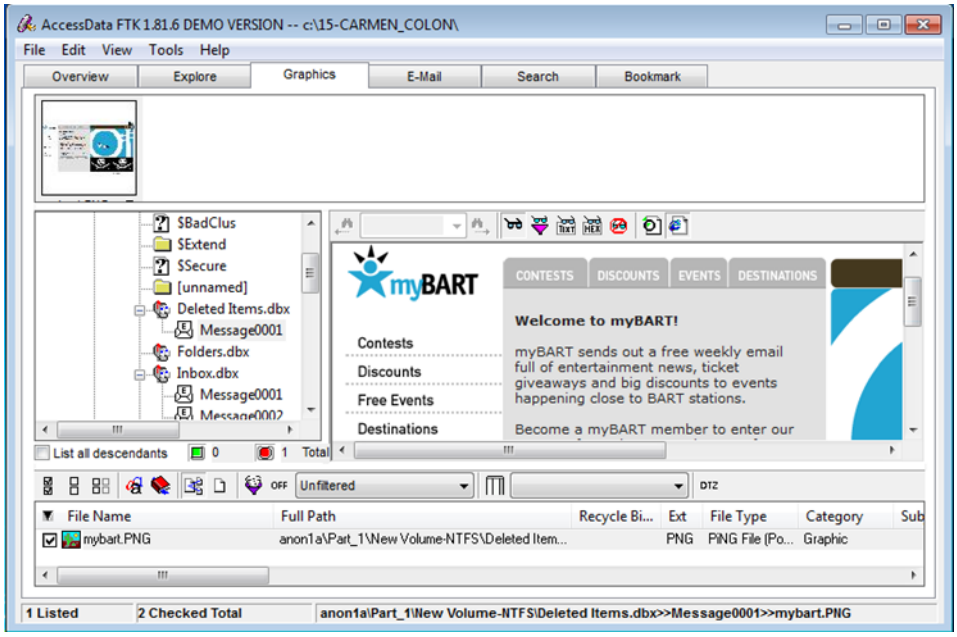


Figura 2.15: Website incriminatorio.

Ya con la evidencia incriminatoria se procede a crear un reporte.

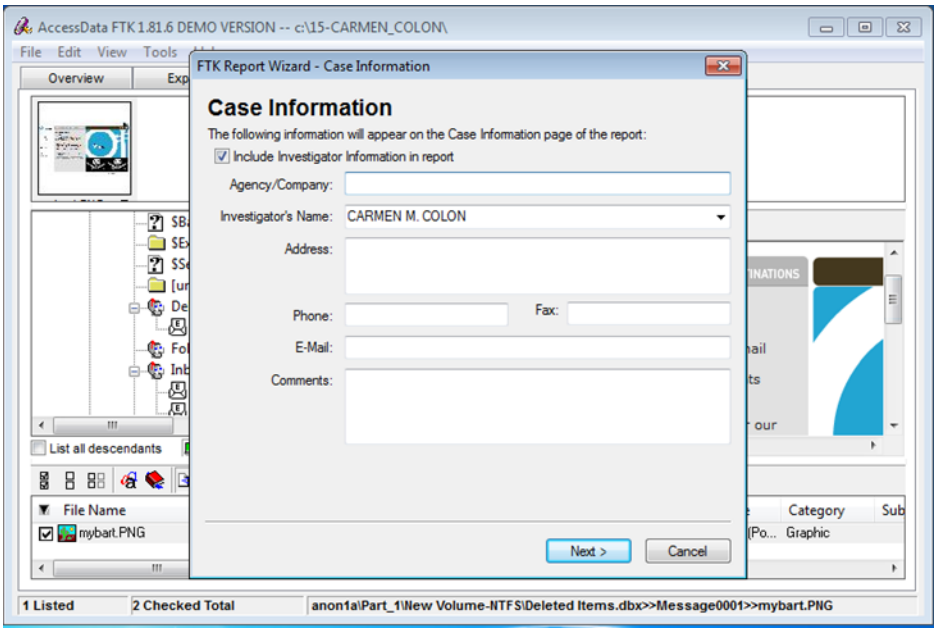


Figura 2.16: Creando un reporte.

Reporte

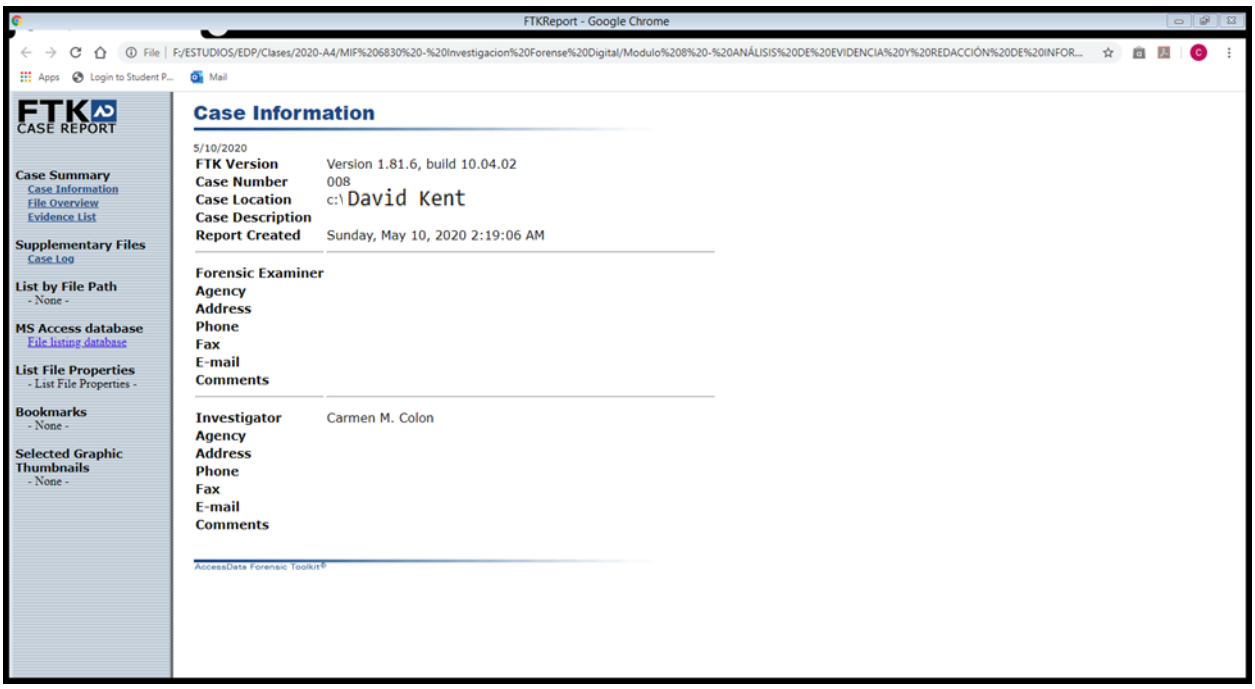


Figura 2.17: Información general.

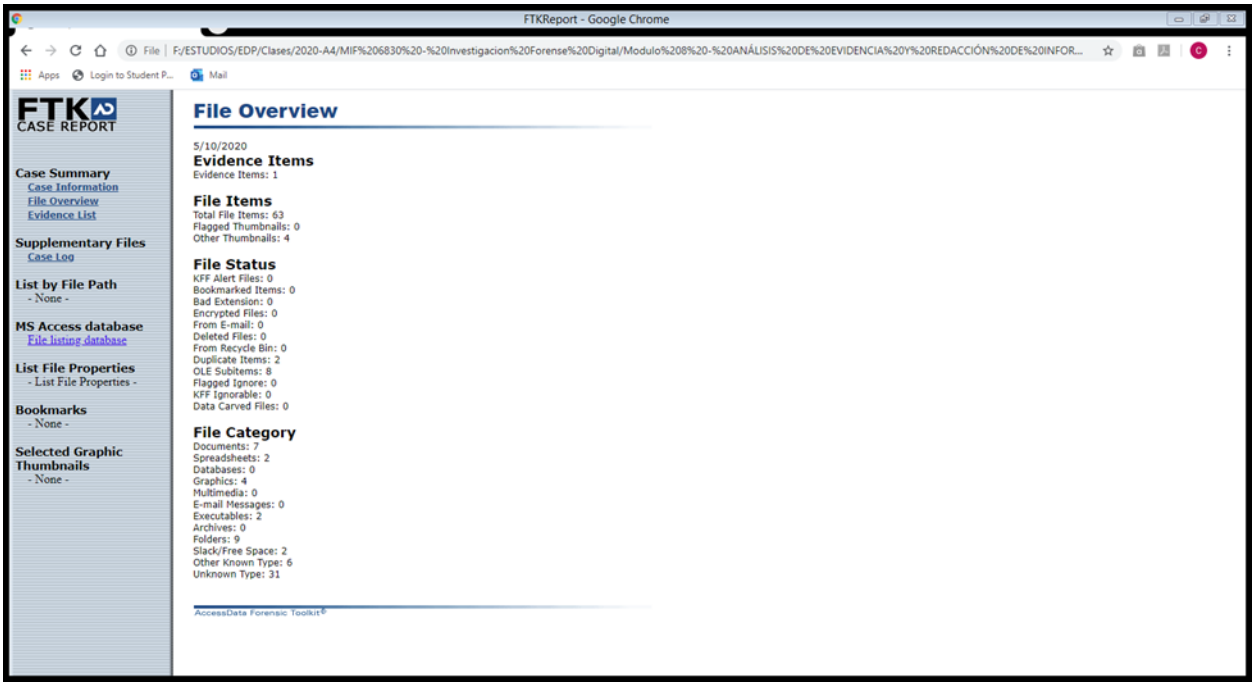


Figura 2.18: Resumen de hallazgos.

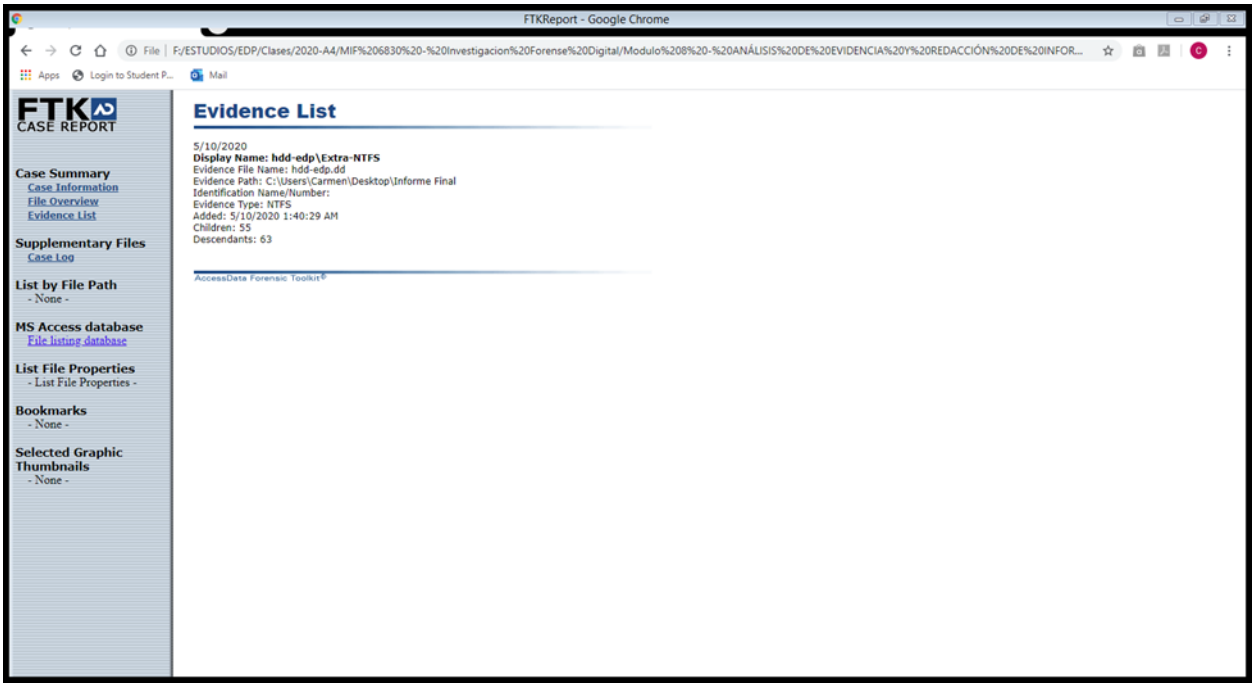


Figura 2.19: Descripción general de la evidencia.

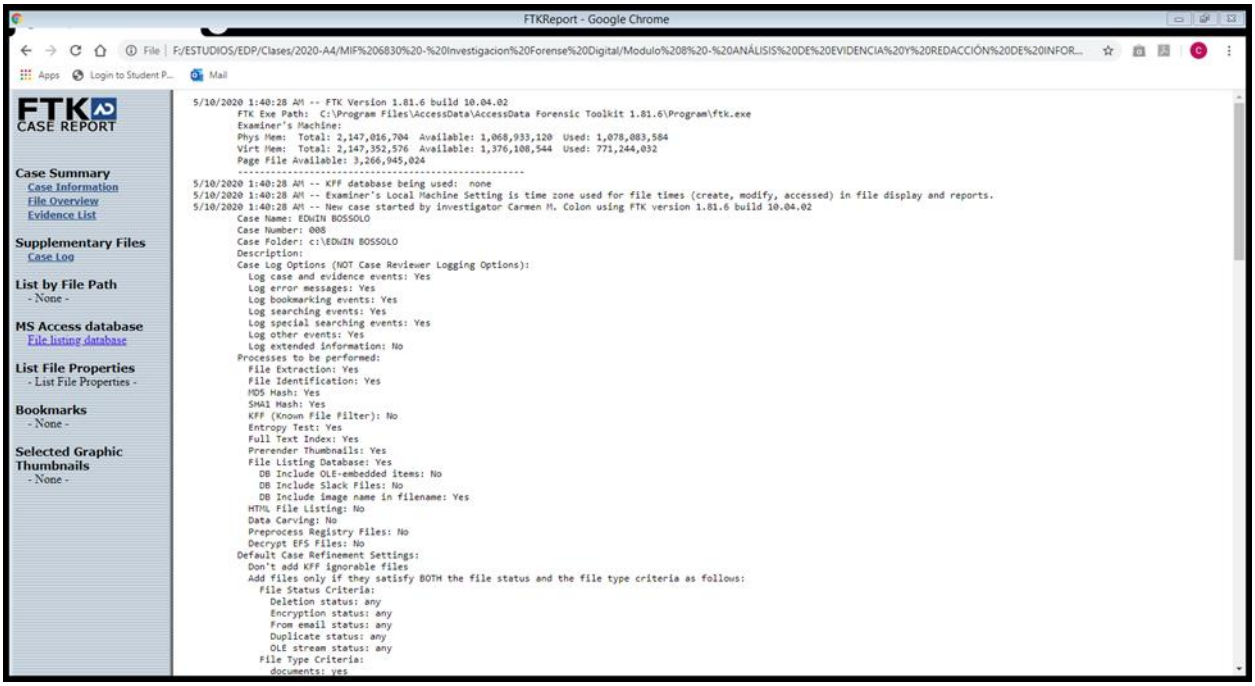


Figura 2.20: Log del proceso investigativo.

Conclusión

Luego de evaluar la evidencia encontrada en el dispositivo podemos concluir que parte del contenido de este indica claramente que David Kent es sospechoso de infiltrarse indebidamente al sistema de base de datos de la compañía DHI. De igual manera, sus cómplices infiltrados en DHI los cuales en horas laborables copian información de usuarios usando el equipo de la compañía. Además, se encontró que Kent tenía en su posesión información confidencial de la compañía. Esto se concluyó así debido a la existencia de listas de equipo e inventarios de distribución de servidores y sus respectivas funciones además de información personal de sus clientes. Está establecido que el dispositivo no fue alterado por nadie al momento de la entrega. La cadena de custodia claramente establece que C3 Security recogió el dispositivo de la oficina del subdirector del FBI bajo la supervisión del Sr. Rodríguez. Es por eso por lo que concluimos que toda la evidencia aquí expuesta cumple con todos los estándares de integridad y confiabilidad para ser utilizada en cualquier proceso legal. Además, certificamos que todos los procesos utilizados para la obtención de dicha evidencia cumplen o exceden los parámetros establecidos por el gobierno federal y las prácticas estándares de la industria forense digital.

DISCUSIÓN DEL CASO

David Kent, de 41 años, fue acusado de robar datos de más de 500,000 currículums de usuarios de Rigzone.com, que había vendido a DHI por $51 millones en 2010, para aumentar la membresía de su nuevo website Oilpro.com. Kent luego intentó vender Oilpro, creado en 2013, a DHI al tergiversar que el nuevo website aumentó su membresía a 500,000 a través de métodos de marketing estándar. Kent lanzó Rigzone en 2000 el cual permite a los miembros crear perfiles y cargar currículums. Cuando el website se vendió a DHI en 2010, su base de datos de miembros valía $6 millones. Desde el principio, Kent se propuso construir un nuevo website que DHI estaría interesado en adquirir. Para enero de 2016, la base de datos de su nueva empresa había aumentado a 500,000 miembros. La base de datos de Rigzone fue hackeada dos veces en 2014 y 2015, lo que provocó que se solicitara a los miembros que se unieran a Oilpro.

Realmente no hubo daños y la compañía no incurrió en ningún costo más allá de usar empleados asalariados para parchear códigos que tenían problemas conocidos desde 2010, cuando DHI, entonces llamado Dice Holdings, compró Rigzone de Kent por $51 millones.

AUDITORÍA Y PREVENCIÓN

Introducción

Como repositorio principal de la información más valiosa de la organización, la base de datos es quizás el segmento más sensible del panorama de IT. Muchas organizaciones están aprendiendo que los activos de las bases de datos son vulnerables tanto a los externos a través de aplicaciones web internos como a empleados que aprovechan privilegios más directos. Los registros de clientes, informes financieros y datos de clientes están en riesgo. Además, el cumplimiento de requisitos reglamentarios como Sarbanes-Oxley (SOX), el Payment Card Industry Data Security Standard (PCI DSS) y otros requieren que las organizaciones realicen evaluaciones de seguridad de la base de datos. El propósito de este trabajo es ayudar a las organizaciones a dar el primer paso hacia la protección de sus bases de datos mediante la evaluación de las mejores prácticas de seguridad y evitar el fraude electrónico como el del caso de estudio de David Kent.

Microsoft SQL Server

Microsoft SQL Server es un sistema de administración de bases de datos relacionales (RDBMS) que admite una amplia variedad de procesamiento de transacciones, inteligencia empresarial y aplicaciones de análisis en entornos corporativos de IT. MS SQL Server es una de las tres tecnologías de bases de datos líderes en el mercado como Oracle Database y IBM DB2.

Análisis SWOT

El análisis SWOT se utiliza para la planificación estratégica la cual puede ser utilizada por los administradores de MS SQL Server para realizar un análisis situacional de la organización. Es una

técnica práctica para analizar las Fortalezas (S), Debilidades (W), Oportunidades (O) y Amenazas (T) a las que se enfrenta MS SQL Server en su entorno empresarial actual. Su propósito principal es identificar las estrategias que una organización puede utilizar para aprovechar y proteger las fortalezas, erradicar sus debilidades, explotar oportunidades externas y contrarrestar las amenazas.

FORTALEZAS / STRENGTHS	DEBILIDADES / WEAKNESSES
Excelente rendimiento en nuevos mercados. Trayectoria exitosa de integración de firmas de cortesía a través de fusiones y adquisiciones. Red de distribución sólida. Buenos rendimientos de los gastos de capital. Alto nivel de satisfacción del cliente. Trayectoria exitosa en el desarrollo de nuevos productos. Cartera de marcas sólida. Fuerte comunidad de distribuidores.	La comercialización de los productos dejó mucho que desear. El inventario de días es alto en comparación con los competidores, lo que hace que la empresa recate más capital para invertir en el canal. La inversión en Investigación y Desarrollo está por debajo de los actores de más rápido crecimiento en la industria. No es muy bueno en la previsión de la demanda de productos que conduce a una mayor tasa de oportunidades perdidas en comparación con sus competidores. Un éxito limitado fuera del negocio principal. Hay lagunas en la gama de productos vendidas por la empresa. La compañía no ha sido capaz de hacer frente a los desafíos presentes por los nuevos participantes en el segmento y ha perdido una pequeña cuota de mercado en las categorías de nicho.
OPORTUNIDADES / OPPORTUNITIES	**AMENAZAS / THREATS**
Nuevos clientes del canal en línea. Disminución del costo de transporte debido a los precios de envío más bajos. Las nuevas tendencias en el comportamiento del consumidor pueden abrir un nuevo mercado. La nueva tecnología ofrece la oportunidad de practicar la estrategia de precios diferenciados en el nuevo mercado. Apertura de nuevos mercados debido a un acuerdo gubernamental. Nuevas políticas medioambientales. La nueva política fiscal puede afectar significativamente la forma de hacer negocios y puede abrir nuevas oportunidades para que los actores establecidos aumenten su rentabilidad. El desarrollo del mercado conducirá a la dilución de la ventaja de la competencia y permitirá a MS SQL Server aumentar su competitividad en comparación con los demás competidores.	Cambiar el comportamiento de compra de los consumidores del canal en línea podría ser una amenaza para el modelo de cadena de suministro impulsado por la infraestructura física existente. El aumento del nivel salarial, especialmente los movimientos como los $15 la hora, y el aumento de los precios en China pueden llevar a una fuerte presión sobre su rentabilidad. El aumento de la tendencia hacia el aislacionismo en la economía estadounidense puede conducir a una reacción similar de otro gobierno, lo que puede afectar negativamente a las ventas internacionales. Competencia intensa. El aumento de la materia prima puede suponer una amenaza para su rentabilidad. No hay suministro regular de productos innovadores. Las nuevas regulaciones medioambientales en virtud del Acuerdo de París (2016) podrían ser una amenaza para ciertas categorías de productos existentes. La demanda de los productos altamente rentables es de naturaleza estacional y cualquier evento improbable durante la temporada alta puede afectar la rentabilidad de la empresa a corto y medio plazo.

Figura 3.1: Análisis SWOT.

Flujo de Procesamiento (Workflow)

En la Figura 2 se describen las etapas que se utilizan normalmente para procesar y ejecutar una instrucción SQL. En algunos casos, MS SQL Server puede ejecutar estas etapas en un orden ligeramente diferente. Por ejemplo, la etapa DEFINE podría producirse justo antes de la fase FETCH, dependiendo de cómo haya escrito el código.

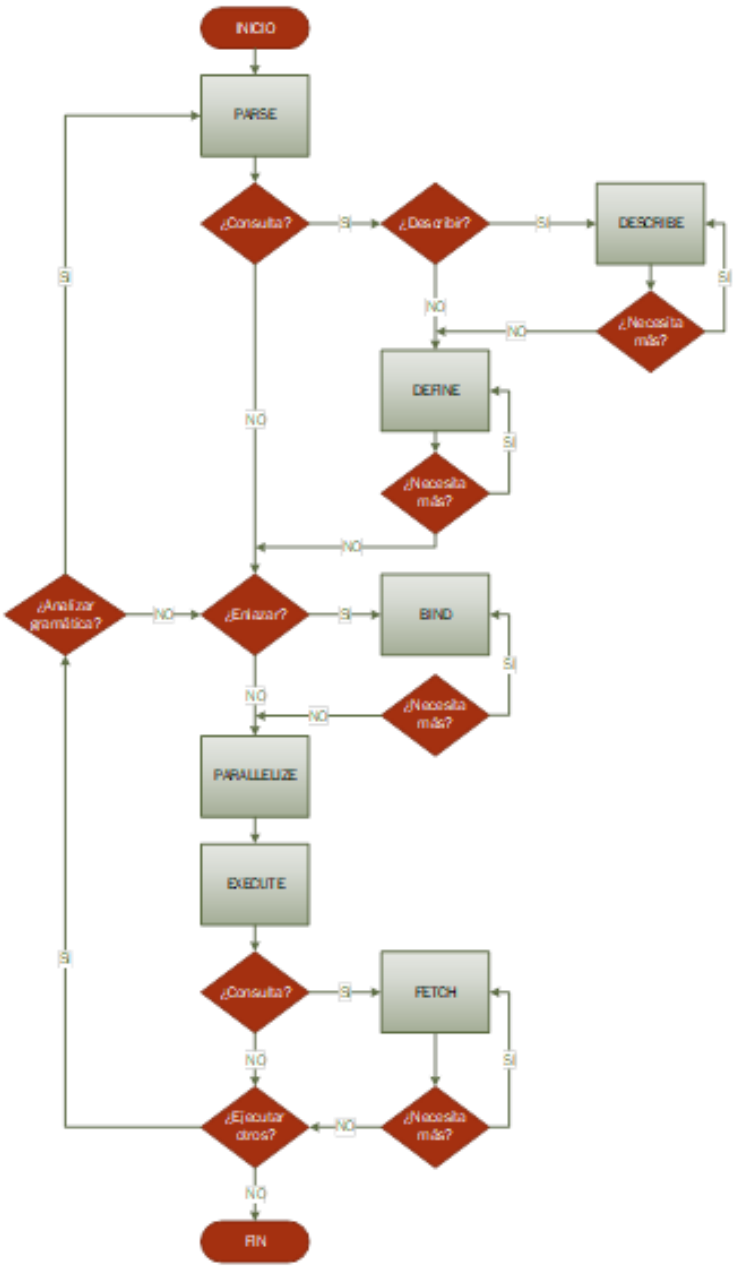


Figura 3.2: Las etapas en el procesamiento de una declaración SQL.

Objetivo, Alcance y Criterio de la Auditoría

La evaluación de la seguridad de los datos es un proceso que mide el riesgo de los datos en un momento determinado. El primer elemento de riesgo se mide evaluando la susceptibilidad de una base de datos a una serie de vulnerabilidades conocidas y escenarios de ataque. Cada

vulnerabilidad identificada se clasifica por gravedad, bajo, medio, alto, crítico, etc. Finalmente, se genera un informe que resume los resultados. Un resumen de evaluación es una recomendación del riesgo general que la administración puede utilizar para priorizar los pasos necesarios para mejorar la seguridad de la base de datos; esto les dice a los gerentes de seguridad y administradores de bases de datos qué necesita su atención primero.

Evaluación de Seguridad de MS SQL Server

El diseño fundamental de un proceso de evaluación de seguridad de base de datos incluye los siguientes atributos:

- Impacto en los Sistemas de Producción: Muchos procesos de evaluación intentan identificar vulnerabilidades imitando las actividades de un atacante. Por ejemplo, una evaluación puede intentar aprovechar una vulnerabilidad de desbordamiento de búfer conocida o utilizar la fuerza bruta para obtener credenciales de acceso válidas. Estas técnicas de explotación son comunes entre las herramientas automatizadas de evaluación de redes y servidores web, especialmente las herramientas de código abierto como Nikto, Nessus y Whisker. El problema con estas metodologías es que pueden causar tiempo de inactividad o daño la base de datos si cualquier exploit es exitoso. Una simulación de desbordamiento de búfer, por ejemplo, puede bloquear una base de datos. Cualquier posibilidad de tiempo de inactividad o daño es obviamente inaceptable en entornos de producción. Este hecho hace que los mecanismos de explotación sean apropiados solo para las pruebas de laboratorio. Por otro lado, los resultados de las pruebas de laboratorio no son aplicables a las bases de datos de producción. Las vulnerabilidades encontradas, o lo que es más importante, las que no se encuentran en el laboratorio pueden o no existir en la

producción. La solución de evaluación de seguridad de la base de datos debe funcionar sin utilizar exploits reales. Las bases de datos de producción no se pueden poner en riesgo.

- Precisión: Muchas evaluaciones no profundizan lo suficiente en la información disponible de la base de datos para validar el estado de una vulnerabilidad determinada. Considere la vulnerabilidad de desbordamiento de búfer intf xp_spr en MS SQL Server (BID1204). Este es un procedimiento almacenado extendido que puede ser explotado por un atacante para bloquear el servidor u obtener privilegios administrativos. Hay dos enfoques para la evaluación con respecto a esta vulnerabilidad que conducen a resultados inexactos. Los enfoques orientados a la explotación intentan enviar datos a xp_sprintf a pesar del riesgo. Dependiendo de la respuesta al exploit, informan si el servidor es vulnerable o no. Sin embargo, la precisión de este enfoque depende de si la cuenta de usuario utilizada por la herramienta de evaluación tiene privilegios EXECUTE sobre xp_sprintf. Es posible que un usuario PUBLIC no tenga privilegios para esta cuenta. Por lo tanto, se produce un error en un exploit de una cuenta PUBLIC y la evaluación notifica un resultado no vulnerable. Sin embargo, una aplicación web puede tener privilegios para xp_sprintf hacer que el servidor de base de datos sea bastante vulnerable, a pesar del resultado original no vulnerable. Otros enfoques de evaluación simplemente comprueban la versión del software para evaluar la vulnerabilidad. En este caso, las versiones 6.5 SP4 y anteriores de SQL Server sufren de esta vulnerabilidad. Esta evaluación de solo versión concluye que un servidor con la versión 6.5 SP1 es vulnerable. Sin embargo, este enfoque omite si el procedimiento almacenado realmente existe en el servidor. Si se quitada el procedimiento almacenado, como se recomienda, el resultado de la evaluación no debe ser vulnerable.

- Eficiencia: La evaluación de la seguridad de la base de datos debe hacer más que proporcionar una lista de vulnerabilidades plana. Tal documento por sí solo no es procesable. Los administradores podrían intentar corregir secuencialmente cada vulnerabilidad del documento, pero tal esfuerzo sería extremadamente ineficiente. Algunas vulnerabilidades requieren atención inmediata, mientras que otras pueden esperar o incluso ser ignoradas. Un proceso de evaluación más eficiente prioriza cada vulnerabilidad de acuerdo con el riesgo. Con un análisis de riesgos priorizado, un administrador de seguridad o un administrador de base de datos puede desarrollar un plan eficaz para la corrección. Otro problema con las vulnerabilidades del documento es que los riesgos no pueden ser evaluados y priorizados por la administración. Los administradores de bases de datos, los administradores de seguridad y los auditores internos necesitan informes de evaluación que comuniquen la postura de seguridad de la base de datos a nivel ejecutivo. Entre otros usos, estos informes se utilizan para justificar los presupuestos de seguridad, informar sobre los resultados de un nuevo proceso de seguridad y medir el cumplimiento normativo. Por lo tanto, las soluciones de evaluación de bases de datos deben integrar capacidades de generación de informes que traduzcan los datos de capacidad de vulnerabilidad en análisis de riesgos a nivel ejecutivo.
- Amplitud de Análisis: La evaluación de la seguridad de los datos de prácticas recomendadas debe incluir una variedad de pruebas que aborden cada una de las siguientes áreas:
    - Vulnerabilidades conocidas - Las bases de datos de vulnerabilidades públicas (Bugtrac, NVD, etc.) rastrean miles de vulnerabilidades de software conocidas, incluidas las que existen dentro de las bases de datos y sus sistemas operativos

subyacentes. La evaluación de la seguridad de la base de datos debe evaluar la susceptibilidad a todas esas vulnerabilidades conocidas que son relevantes para el software de base de datos de destino y el sistema operativo subyacente.

- Configuración del sistema - La seguridad de la base de datos es muy sensible a los problemas de configuración del sistema, muchos de los cuales están cubiertos por las prácticas recomendadas. Cientos de elementos de configuración deben evaluarse en función del tipo y el uso previsto de la base de datos. Un ejemplo simple es la frecuencia de cambio de contraseña. Las prácticas recomendadas recomiendan que las contraseñas de recuento de AC de usuario cambien con frecuencia. La evaluación de la base de datos debe permitir al administrador configurar una política de frecuencia de cambio y comparar automáticamente esa política con el periodo de todas las contraseñas reales. La solución de evaluación puede enumerar en todas las cuentas con contraseñas que infringen la directiva para ayudar a priorizar la amenaza y corregir el problema. Una buena prueba de evaluación comprueba si el administrador ha utilizado mecanismos de base de datos integrados para aplicar correctamente la política para la contraseña.
- Gestión de privilegios - También se debe evaluar la medida en que se administran los privilegios de base de datos. En general, los propietarios de bases de datos deben adherirse a una directiva de privilegios mínimos. Las prácticas recomendadas exigen que los privilegios de usuario se concedan a las cuentas solo a través de roles. Los privilegios concedidos directamente pueden producir derechos de acceso excesivos cuando los usuarios cambian de posición dentro de la organización. Las subvenciones directas también implican un proceso de autorización

indocumentado, una barrera común para el cumplimiento de leyes reguladoras como Sarbanes-Oxley. Por lo tanto, la evaluación debe examinar el diccionario de datos para los registros en los que el concesionario es una cuenta y no un rol. Las cuentas que coincidan con esta condición pueden aparecer junto con los privilegios concedidos directamente para ayudar a medir la amenaza y ayudar a solucionar el problema.

- Objetos externos - Ciertos objetos que son externos a la base de datos se pueden aprovechar, si no se configuran correctamente, para atacar una base de datos. Estos objetos externos son principalmente objetos del sistema operativo como archivos, servicios, claves del registro, etc. Por ejemplo, IBM DB2 incluye un archivo ejecutable denominado db2job que se puede explotar, de forma predeterminada, para permitir a los usuarios locales ejecutar código con privilegios administrativos. Susceptibilidad a esta vulnerabilidad se determina mediante la comprobación de los permisos del sistema operativo en el archivo db2job.
- Cumplimiento normativo - La evaluación de la base de datos debe prestar especial atención a los requisitos de seguridad que son específicamente relevantes para el cumplimiento normativo. Por ejemplo, SOX requiere el seguimiento de todas las nuevas cuentas de usuario dentro de las bases de datos que almacenan información de informes financieros. Por lo tanto, la evaluación debe comprobar el diccionario de datos para las cuentas cuya fecha de creación se encuentra dentro de un período de tiempo configurable. Las cuentas nuevas pueden aparecer en los informes de resultados de la evaluación.

Hallazgos

El número de ID de Bugtrac 2041 (BID 2041) identifica una vulnerabilidad de Microsoft SQL Server 2000/Data Engine en la que un procedimiento almacenado extendido es susceptible a un desbordamiento de búfer que puede bloquear el sistema o habilitar la ejecución de código arbitrario, es decir, un gusano. Para probar esta vulnerabilidad sin enviar realmente datos a la entrada buffer en cuestión, la evaluación de seguridad puede aplicar el siguiente proceso.

- Prueba de vulnerabilidad: Compruebe la versión del software con respecto a los que se sabe que son vulnerables. Microsoft ha publicado un parche para esta vulnerabilidad.
    - Si se ha aplicado el parche, entonces el servidor no es vulnerable.
    - Si se encuentra que la versión coincide con las versiones vulnerables conocidas, compruebe la existencia del xp_printstatements del procedimiento almacenado. Las prácticas recomendadas de seguridad de la base de datos recomiendan la eliminación de todos los procedimientos almacenados extendidos innecesarios.
        - Si se ha quitado xp_printstatements, la base de datos no es vulnerable.
        - Si existe xp_printstatements, la base de datos es vulnerable.
- Priorizar por riesgo: Debe extraer la lista de usuarios que tienen privilegios EXECUTE en el xp_printstatements del procedimiento almacenado.
    - Si se conceden privilegios a un gran número de usuarios o PUBLIC, es decir, a todos, entonces el riesgo asociado con esta vulnerabilidad es relativamente alto.
    - Por otro lado, si los privilegios se conceden solamente a SA (administradores del sistema), entonces el riesgo asociado con esta vulnerabilidad es bajo.

Recomendaciones Para La Prevención Del Fraude

Cuentas Compartidas

El uso compartido de una sola cuenta de base de datos por muchos usuarios infringe el requisito de seguridad fundamental para la responsabilidad del usuario. No hay manera de vincular definitivamente a un solo usuario a un evento potencialmente malintencionado cada vez que se comparten cuentas de usuario. Por lo tanto, prácticamente todas las prácticas recomendadas de control de seguridad de IT (COBIT, etc.) hace hincapié en la necesidad de prevenir y/o detectar el uso compartido de cuentas. Como resultado, este problema es otro obstáculo común para el cumplimiento de regulaciones como Sarbanes-Oxley. Desafortunadamente, una evaluación puntual de la información de la cuenta de base de datos no revela cuentas compartidas. La detección de cuentas compartidas requiere supervisión del comportamiento para realizar un seguimiento continuo de las sesiones de base de datos e identificar las cuentas que usan las sesiones simultáneas de diferentes direcciones de IP.

Establecer Políticas y Controles

Las políticas de la base de datos permiten a los administradores definir reglas que especifican un comportamiento aceptable, un comportamiento inaceptable y transacciones reguladas específicamente. Las políticas son muy granulares con atributos que se extienden a columnas específicas, operaciones SQL, captura de respuesta de consulta, restricciones de hora del día, IP de origen, nombres de host de origen, sistema operativo de origen y mucho más.

Supervisar y Hacer Cumplir

La base de datos puede configurarse de forma flexible para supervisar y aplicar políticas. Los datos de auditoría son muy granulares que permiten una evaluación forense exhaustiva. El almacenamiento de datos de auditoría aprovecha una arquitectura distribuida que se escala entre los centros de datos más grandes mientras mantiene una vista unificada. El archivado de auditoría admite la programación automatizada, la compresión, el cifrado y una firma digital. Las infracciones de seguridad pueden desencadenar acciones de respuesta que van desde simples registros de eventos, hasta alertas en tiempo real y bloqueo de usuarios. Por último, la correlación avanzada de eventos permite la detección precisa de los ataques más sofisticados.

Conclusión

La evaluación de la seguridad de la base de datos es un primer paso importante en una buena estrategia general de seguridad de la base de datos. Los cuatro criterios de diseño de prácticas recomendadas deben incluir el impacto en los sistemas de productos, la precisión, la eficiencia y la amplitud de las pruebas. La herramienta gratuita de evaluación de vulnerabilidades Scuba by Imperva Database aborda cada uno de estos criterios, al tiempo que supera las barreras presupuestarias, de recursos y de experiencia. Más allá de un primer paso exploratorio ofrecido por Scuba y hacia una infraestructura de base de datos más segura, una organización debe implementar conjuntamente una solución completa del ciclo de vida de la seguridad de la base de datos, tal como lo ofrece la seguridad de la base de datos Imperva SecureSphere y los productos de gateway de supervisión. Los productos Imperva SecureSphere proporcionan un ciclo de vida de seguridad de base de datos completo que no solo ofrece evaluación en toda la organización,

sino que también integra capacidades granulares de definición, supervisión, aplicación y medición de políticas.

CONCLUSION

Para concluir, vender su empresa por una suma exorbitante no fue suficiente. Lanzar un competidor unos años después no fue suficiente. Robar 700,000 cuentas de la empresa que le dio ese dinero no fue suficiente. No, Kent tuvo que vender otro website de trabajo de energía a la empresa que compró el primero. Pudo haber sido avaricia o estupidez; aún no se sabe. En la página de Oilpro en 2014, Kent fue descrito como "un desarrollador de software apasionado y emprendedor adicto a soñar con nuevas ideas, programar y trabajar con talento A +". Supongo que tendrá mucho tiempo para soñar con algunas de esas ideas luego de pagar su condena y comenzar desde cero a buscar trabajo ya que dudo que alguien vuelva a confiar en el por mucho tiempo. Por otra parte, en una demanda civil, DHI exige $20 millones en daños. Eso es a pesar de que la corporación no pudo documentar ni un centavo en pérdidas. A estas alturas, aún no se sabe sobre por qué los gerenciales que están en DHI están exigiendo una cantidad tan exorbitante. Para las personas que entienden cómo funciona el mundo a menudo, podría percibirse como una simple codicia. Kent confesó su crimen y ha pagado una indemnización. Cualquier otro castigo representa una inclinación de la justicia contra las personas que admiten algún delito. Pero DHI sigue actuando por codicia. La codicia no es buena. A nivel mundial, esa mentalidad está socavando el capitalismo de marca. Debería preocupar a los inversores que, a través de su demanda civil, DHI podría estar planteando dudas sobre su propia gerencia corporativa.

REFERENCIAS

Berris, P. (2020). Congressional Research Service. Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress. Recuperado de https://fas.org/sgp/crs/misc/R46536.pdf

Blum, J. (2017). Chron. Oilpro shutting down months after founder pleaded guilty to theft. Recuperado de https://www.chron.com/business/energy/article/Oilpro-shutting-down-months-after-founder-plead-11721198.php

Casetext. (2013). Casetext. United States v. Swartz. Recuperado de https://casetext.com/case/united-states-v-swartz-4

Claburn, T. (2017). The Register. An oil industry hacker facing jail, a $20m damages bill, and claims of counter-hacking. Recuperado de https://www.theregister.com/2017/10/14/david_kent_oilpro_latest/

Cole, J. & Thompson II, R. (2015). Congressional Research Service. Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA). Recuperado de https://fas.org/sgp/crs/misc/R44036.pdf

Collins, A. (2018). World Economic Forum. The Global Risks Report 2018. Recuperado de http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Department of Justice. (2016). United States Department of Justice. Former Fox40 Web Producer Sentenced to Prison for Attack on Media Sites. Recuperado de https://www.justice.gov/usao-edca/pr/former-fox40-web-producer-sentenced-prison-attack-media-sites

Department of Justice. (2017). United States Department of Justice. Oilpro.Com Founder

Sentenced To Prison For Hacking Into Competitor's Computer System. Recuperado de https://www.justice.gov/usao-sdny/pr/oilprocom-founder-sentenced-prison-hacking-competitor-s-computer-system

Dodt, C. (2019). Infosec. Computer Forensics: FTK Forensic Toolkit Overview [Updated 2019]. Recuperado de https://resources.infosecinstitute.com/topic/computer-forensics-ftk-forensic-toolkit-overview/

Gesmundo, A. (2018). Hacking 101. [Entrada de blog]. Recuperado de https://www.globalsign.com/en/blog/hacking-101

Kent, D. (2021). Blogger. David W. Kent on Blogger. Recuperado de https://davidwkent.blogspot.com/

Mangan, D. (2016). CNBC. How a jobs site may have snared alleged 'hacker' founder. Recuperado de https://www.cnbc.com/2016/03/31/how-a-jobs-site-may-have-snared-alleged-hacker-founder.html

Microsoft. Prueba SQL Server on-premises o en el cloud. Recuperado de https://www.microsoft.com/es-es/sql-server/sql-server-downloads

Parada, M. (2019). Open Webinars. Que es SQL Server. Recuperado de https://openwebinars.net/blog/que-es-sql-server/

Peterson, A. (2014). The Washington Post. The law used to prosecute Aaron Swartz remains unchanged a year after his death. Recuperado de https://www.washingtonpost.com/news/the-switch/wp/2014/01/11/the-law-used-to-prosecute-aaron-swartz-remains-unchanged-a-year-after-his-death/

Raymond, N. (2016). Reuters. Oil industry networking site creator pleads guilty in U.S. hacking case. Recuperado de https://www.reuters.com/article/us-oilpro-crime-idUSKBN1482L5

Vera-Cruz, C. (2020). TechTarget. La importancia del control de acceso y cómo mejorarlo. Recuperado de https://searchdatacenter.techtarget.com/es/cronica/La-importancia-del-control-de-acceso-y-como-mejorarlo

Zetter, K. (2016). Wired. Matthew Keys Sentenced to Two Years for Aiding Anonymous. Recuperado de https://www.wired.com/2016/04/journalist-matthew-keys-sentenced-two-years-aiding-anonymous/