UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Pentest a empresa de sector automotriz

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Aldebarán Dejadir Díaz Yáñez

ASESOR DE INFORME

M.C. Alejandro Velázquez Mena

Ciudad Universitaria, Cd. Mx., 2019

INTRODUCCIÓN

En este informe se abordarán las diferentes problemáticas que se tenían presentes en la empresa las cuales dieron lugar a mi contratación. Hablaré principalmente del proyecto por el cual fui contratado: “Pentest a empresa de sector automotriz” así como otros proyectos internos que realicé los cuales permitieron incrementar y reforzar la seguridad y la prevención de ataques y fugas de la información.

Se abordará de manera específica cada técnica utilizada en la remediación de las vulnerabilidades encontradas en las pruebas de penetración. Por otra parte, hablaré acerca de mis actividades diarias, de la atención a incidentes de seguridad y de las metodologías utilizadas para la correcta remediación de vulnerabilidades, prevención de riesgos, amenazas e infecciones que pudiera significar la pérdida de información sensible, costos adicionales a la compañía, así como tiempo invertido en recuperar información y reparar activos.

Detallaré las diferentes herramientas, técnicas empleadas y propuestas para mejorar la seguridad de la información, prevenir ataques, corrección de huecos de seguridad, así como la capacitación a grupos de riesgo específicos y la manera en la que trabajo con Aguascalientes, Toluca, Morelos y mi contraparte en Estados Unidos para reforzar la seguridad de la Compañía.

OBJETIVO

La meta de esta prueba de hackeo ético es determinar las áreas vulnerables a un ataque real, y conocer la capacidad de detección y respuesta al mismo, los objetivos son:

1. Verificación de los controles perimetrales de la red.

2. Comprobación de la seguridad en la configuración de la infraestructura de TI (equipos y sistemas)

3. Obtener reporte ejecutivo, informe técnico y recomendaciones de hallazgos y solución.

4. Identificar y recomendar medidas de seguridad para la infraestructura de TI y los datos de la empresa.

DESCRIPCIÓN DE LA EMPRESA

El área de TI dentro de la empresa es una de las más grandes al tener más de 60 empleados. TI está subdividida en dos: BA (Business Application) y BI (Business Intelligence). Cada área reporta a un subdirector diferente quienes a su vez reportan al director general de TI; él a su vez reporta a Dirección General, Finanzas y Estados Unidos.

Seguridad de la Información le reporta al subdirector de infraestructura y al equipo de Seguridad la Información de Estados Unidos y su vez al CISO.

En el siguiente organigrama podemos apreciar lo descrito anteriormente:

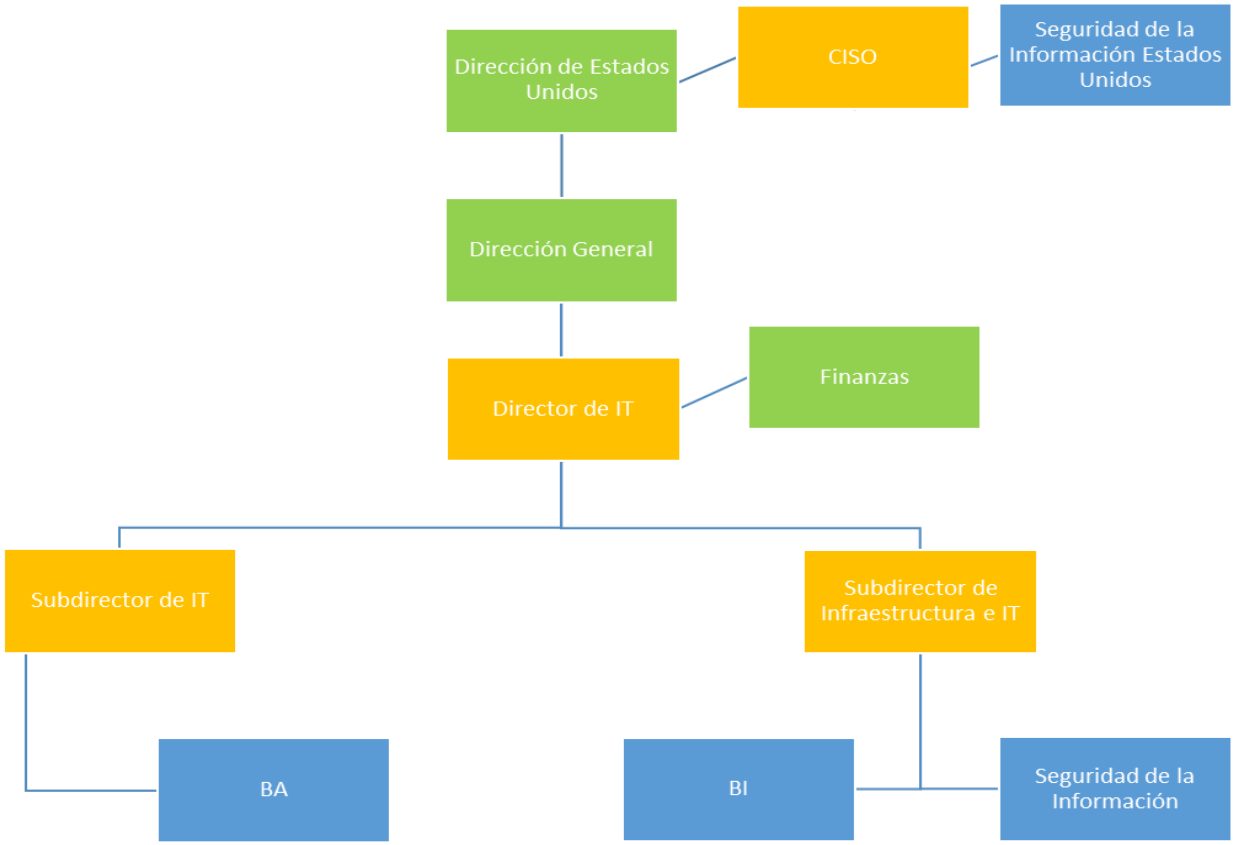


Figura 1. Organización de la empresa

CAPITULO 1: DESCRIPCIÓN DE PROYECTOS ADICIONALES Y ACTIVIDADES DIARIAS

Analista de Seguridad de la Información. Enero 2017 – Actual

1.1 Análisis de vulnerabilidades

Administración, detección y corrección de vulnerabilidades: Identificación de los activos sensibles, así como creación y gestión de grupos críticos, aplicación de parches y escalamiento a áreas críticas.

1.2 Creación de laboratorio para simular red corporativa

(AD, servers 2008 y 2012, clientes Win7/W10, Firewall, switch) para realizar pruebas de implementación de herramientas y políticas de seguridad

1.3 Blindaje de equipos Windows server y desktop

Para detección de movimiento lateral y disminución de riesgo en ataques a infraestructura Windows.

- Restricción de dispositivos de almacenamiento externos a solo lectura o bloqueo total e instalación vía Windows GPO.
- Control de documentos con Macros a para evitar impacto.

1.4 Instalación de Carbon Black

Propuse la adquisición de Carbon Black, la cual es una herramienta que aumenta considerablemente el nivel de protección de las computadoras al impedir que se ejecuten programas maliciosos, que los usuarios instalen cosas indebidas y permitirnos tener visibilidad de todos estos eventos y lograr identificar al paciente cero en caso de alguna infección o ataque lo cual nos permite actuar de una manera mucho más eficiente. En enero, la empresa adquirió ésta herramienta y he estado coordinando al equipo de servidores, de endpoints (equipos de usuarios finales) y al proveedor para poder hacer la implementación a nivel nacional a un total de 8,050 equipos entre endpoints y servidores. Actualmente, ya estamos a la mitad de la fase de pruebas y en Julio comenzaremos con la distribución del agente a nivel nacional.

Basándome en los 3 pilares de protección de la información: confidencialidad, disponibilidad e integridad, ésta implementación permitirá que los esfuerzos dedicados hoy en día en la detección de virus, programas maliciosos así como el tiempo y dinero invertido en la reparación de los equipos afectados por estas amenazas se vean reducidos lo que conlleva a un aumento de la productividad al no tener que dejar varios días al empleado sin su equipo el cual es su herramienta principal de trabajo, prevención a pérdida de información y el robo de la misma así como un ahorro significativo para la compañía.

1.5 Certificación de usuarios privilegiados

Esta actividad consiste en solicitar las listas de usuarios con acceso a las aplicaciones JSOX a los administradores de cada una de esas aplicaciones. Se deben filtrar las listas de tal forma que sólo se mantengan aquellos usuarios privilegiados, es decir, aquellos que tienen permiso de acceso, escritura y que pueden eliminar algún objeto sobre el aplicativo.

Una vez identificados, se envían estos listados a los gerentes responsables de cada uno de los usuarios identificados; ellos deben certificar y justificar que el usuario o los usuarios identificados siguen requiriendo el acceso a la plataforma.

Posteriormente, es revisar cada una de estos listados para validar aquellos usuarios que ya no requieren el acceso, cambió el propietario de la cuenta o que fueron baja de la compañía, pero el objeto (la cuenta), sigue en el aplicativo, aunque de forma inactiva.

Ya que fueron identificados, el procedimiento para darlos de baja del aplicativo es:

- Levantar un ticket a la mesa de ayuda solicitando la baja y asignación del ticket al administrador de la aplicación correspondiente.
- Dar seguimiento con el administrador que la baja se realice en un lapso no mayor a 2 días.
- Solicitar evidencia al administrador del antes y después de la eliminación de la cuenta o del cambio de propietario.
- Una vez validada la evidencia, se solicita al administrador cierre el ticket.

Finalmente, el conjunto de correos, listados, bajas y evidencias de las mismas son enviadas al subdirector de TI, quien se encargará de validar cada una de las respuestas de los gerentes, comprobar que todos los aplicativos JSOX fueron incluidos y que las bajas solicitadas por los gerentes fueron ejecutadas de manera correcta, que la evidencia compartida esté completa y que se haya cerrado el ticket generado. Una vez concluido este proceso, el subdirector envía sus comentarios o aprobación para terminar el proceso de certificación de usuarios privilegiados.

1.6 Concientización de seguridad

Como parte de la tarea de incrementar la seguridad de la compañía, es importante educar al usuario para que pueda llevar las mejores prácticas de seguridad tanto en la oficina como en su vida personal.

Derivado de esto, comenzamos a realizar la instalación de un aditamento a Outlook, el cual permite reportar cualquier correo sospechoso directamente a la cuenta destinada para este fin y que posteriormente sea analizada por nosotros y Estados Unidos en caso de requerir algún tipo de atención delicada o ser severidad 1, que es cuando el riesgo de impacto es muy alto para la compañía.

De manera adicional, en conjunto con Estados Unidos, creamos campañas de phishing. Es decir, redactamos correos maliciosos dirigidos a cada uno de los empleados de la compañía, con la intención que aprendan a identificar este tipo de amenazas, reconozcan entre un correo de phishing, un correo de spam y lo reporten automáticamente mediante la herramienta previamente mencionada o en su defecto lo envíen directamente al correo destinado para este fin y posteriormente eliminen el correo de su Bandeja de Entrada y cualquier otra subcarpeta.

Si el usuario llegara a caer en alguno de estos correos creados por nosotros, al final de cada uno, existe una infografía la cual primero le indica que es un ejercicio controlado por la compañía y posteriormente le explica qué es phishing y ayuda a identificar los elementos que normalmente se presentan en un correo malicioso, así como los pasos a seguir en caso de ser víctima de esta clase de amenazas.

De manera adicional a estos ejercicios, se envía de manera mensual un boletín el cual da información al usuario respecto a las últimas noticias de seguridad en el mundo, como hackeos, fugas de información entre otros. También le da al usuario consejos y mejores prácticas para su vida diaria, como ejemplo, es cómo estar seguros cuando realizar una compra en línea, cómo almacenar contraseñas y como crearlas de manera que sean seguras y difíciles de hackear. Damos consejos respecto al tema de la confidencialidad y de cómo deben ser prudentes de a quién y cómo entregan su información, como las llamadas de vishing o extorsión. Finalmente incluye un correo especial donde pueden enviar sus dudas, comentarios o incluso solicitar ayuda en caso de haber sido víctimas de este tipo de amenazas.

Finalmente, y en coordinación con Estados Unidos, se creó un curso de Seguridad en Línea para todos los usuarios que utilicen la red corporativa de tal forma que se les enseñen más conceptos, mejores prácticas de seguridad, así como reforzar el aprendizaje para la identificación de amenazas como correos sospechosos, riesgos de realizar descargas en sitios sospechosos, compras en línea y cómo actuar si has sido víctima de estas amenazas.

Responsabilidades diarias:

1.7 Detección de equipos comprometidos

Realizar la detección de equipos comprometidos o infectados, es algo vital para la compañía ya que esto permite controlar la amenaza y evitar su propagación al resto de los equipos.

Para realizar esta tarea, tenemos un sistema en el cual nos es reportado de manera automática cualquier tráfico sospechoso, intento de ataque con su respectiva IP y qué tipo de ataque intentó realizar. Adicionalmente, recibimos un reporte de nuestra consola con los últimos equipos infectados, si fueron remediados por el antivirus o es necesaria atención especial en algún equipo. El equipo de Estados Unidos también nos reporta actividad sospechosa en la red. Hacemos uso también de nuestro correlacionador de eventos para detectar tráfico sospechoso y detectar intentos de hackeo a la compañía.

Mi responsabilidad recae en estar al pendiente de estas alertas y reportes para contener la amenaza, dar seguimiento al proceso de remediación el cual va desde desinfectar el equipo hasta re clonarlo, durante este tiempo, se analiza el contenido de la computadora en busca de cualquier archivo residual dejado por el virus o malware, se le corren antivirus y otras herramientas para asegurar que, al regresar la información a la computadora recién clonada, esta no vuelva a infectarse.

La importancia de lograr contener estas infecciones es evitar la propagación del virus o malware y evitar la pérdida de información valiosa para la compañía y el usuario ya que en caso de que el equipo presente un segundo reporte de infección o de tráfico sospechoso, se procede al formateo total del equipo, sin posibilidad a respaldos, dando como resultado la pérdida de toda la información.

1.8 Atención y respuesta a tickets de seguridad

Como parte de las infecciones previamente mencionadas, aparte del seguimiento con el personal de la mesa de ayuda, le doy seguimiento en el sistema de tickets de Seguridad de la Información, donde se van registrando el status de cada remediación.

De manera adicional, también aquí se reportan los correos sospechosos enviados por los usuarios para poder analizarlos y darle seguimiento puntual con el usuario para indicarle los siguientes pasos, asegurarnos que no haya abierto el correo, dado click en links, abierto archivos adjuntos o proporcionado datos personales que pudieran comprometerlo a él y la compañía.

Frecuentemente son reportados falsos positivos, es decir, aquellos tickets generados de correos que no son maliciosos, que simplemente son spam o que son reportados por error. Por lo que realizar el análisis e identificación de cada correo reportado es fundamental para evitar perder tiempo en seguimientos a esta clase de reportes.

Una vez concluido el análisis, identificación y seguimiento en caso necesario, se cierran los tickets generando un histórico de todos los incidentes reportados para futuras referencias y auditorías.

1.9 Atención a casos de Compliance, Auditoría e investigaciones confidenciales

De manera continua recibimos reportes y requerimientos de Estados Unidos y México de diferentes áreas de Compliance, Auditoría, Legal y Recursos Humanos, solicitando la obtención de evidencia de algún usuario debido a alguna investigación confidencial, temas de incumplimiento, conflictos de intereses, conflictos legales o fuga de información a la competencia.

De mi lado, es realizar un respaldo de la información del usuario ya sea total o parcial dependiendo el requerimiento, dar seguimiento con las áreas involucradas, monitorear la actividad del usuario y en caso necesario, decomisar su equipo para las investigaciones y tareas necesarias.

Una vez concluidas las investigaciones correspondientes se determina si el usuario saldrá de la compañía o si es posible regresarle su equipo y continuar con sus actividades.

1.10 Escaneos de seguridad y coordinación de aplicación de parches de seguridad

Como parte de mis actividades diarias se encuentra realizar escaneos de seguridad a diferentes aplicativos y equipos y coordinar la aplicación de parches de seguridad.

Para realizar estos escaneos utilizo diferentes herramientas de seguridad, tales como: Nessus, Nikto, Nmap, Metasploit, The Mole, SQL Map, entre otras. La finalidad de estos escaneos de seguridad es encontrar aquellas vulnerabilidades que pudieran permitir a un atacante comprometer la red y robar información sensible o confidencial de la empresa.

El proceso toma aproximadamente de dos a tres días dependiendo el impacto del aplicativo o servidor, ubicación y ambiente, ya que puede ser un servidor de desarrollo o productivo en donde si es el primer caso, no hay problema el tiempo en que se realice el escaneo, sin embargo, si es productivo, el escaneo debe coordinarse con el equipo de infraestructura, así como con el administrador del servidor o aplicativo.

Una vez concluidos los escaneos, analizo los resultados comparándolos e identificando la criticidad de cada vulnerabilidad, así como la manera de remediarla. Posteriormente, realizo un reporte con todos los hallazgos, el cual es presentado al equipo de infraestructura y en ocasiones al dueño del aplicativo para poder coordinar la aplicación de parches, cambios de configuración y actualizaciones necesarias para remediar las vulnerabilidades.

El proceso de remediación de vulnerabilidades toma aproximadamente mes y medio, debido a un "período de freeze" en el cual, no podemos realizar ningún cambio sobre ningún ambiente productivo. En este lapso, se aprovechan las ventanas para analizar el impacto que podrían ocasionar algunos parches o actualizaciones a los aplicativos que residen en los servidores y si es o no viable la remediación sugerida, en caso de tener un impacto alto la aplicación del parche, se procede a encontrar una contramedida o en su defecto documentar el por qué no se puede actualizar dejando establecido que se buscará a futuro la actualización completa del framework o el aplicativo para que soporte el último nivel de parcheo necesario.

El seguimiento a todo este proceso lo coordino mediante juntas semanales de la siguiente manera:

- Primera junta: se presentan hallazgos a infraestructura.
- Segunda junta: infraestructura presenta plan de trabajo y fecha compromiso para remediación de todas las vulnerabilidades.
- Juntas posteriores: se presenta el avance de remediaciones de acuerdo al plan de trabajo, así como aclaración de dudas, problemas, contramedidas adicionales hasta llegar al objetivo final que es la remediación total de los hallazgos.

Debido al tamaño de la compañía y la cantidad de ambientes y aplicativos, es necesario segmentar estas pruebas de tal forma que no se junten las remediaciones de todos los ambientes en un solo periodo.

1.11 Revisión de nuevos proyectos de seguridad

Por políticas de la compañía, todos los nuevos proyectos, aplicativos, adquisición de software, actualización sobre aplicativos existentes o nuevas integraciones a aplicativos, deben ser revisadas por Seguridad de la Información.

Cada equipo de trabajo está obligado a pasar por diferentes etapas durante el desarrollo de su proyecto llamadas "Gates", las cuales van desde el Gate 0 hasta el Gate 6. Dentro de estas etapas, la primera y tercera etapa están relacionadas 100% con seguridad.

En la etapa cero, deben definir cómo funcionará su aplicativo, qué medidas y prácticas de seguridad utilizará, cómo protegerá los datos, cómo serán las comunicaciones, así como la infraestructura necesaria para la realización del proyecto, en otras palabras, una descripción general de la funcionalidad del proyecto y los requerimientos de software, hardware.

Posteriormente en la tercera etapa, deben realizar un diagrama de arquitectura de red donde se expresen las comunicaciones, infraestructura a utilizar (nueva y ya existente), protocolos, puertos, aplicativos con los que tendrá interconexiones y que se vea claramente que el aplicativo funciona en tres capas o en caso necesario en dos capas, en cuyo caso se busca una excepción a la política global. Adicionalmente, deben llenar un documento de Controles y Contramedidas de Seguridad de la Información, donde deberán detallar de qué manera funciona el aplicativo en cuanto a:

- Autenticación
- Autorización
- Inserción y validación de datos
- Administración de configuraciones, cambios y acceso
- Manejo, almacenamiento y protección de datos sensibles
- Administración de sesiones y acceso
- Métodos criptográficos
- Protección contra manipulación de parámetros del aplicativo
- Manejo de excepciones

- Administración, manejo y generación de logs y procesos auditables

Una vez que tienen completa la información anteriormente mencionada, se realiza una junta de revisión que consiste en:

- Entender la funcionalidad del aplicativo o necesidad del cambio, actualización o integración.

- Revisar el diagrama de arquitectura de red de tal forma que siga las políticas de seguridad de la compañía, utilice comunicaciones seguras, cifradas y que la información se mantenga siempre protegida, así como que la comunicación entre la infraestructura involucrada sea correcta y pase por los equipos de seguridad correctos (firewalls, proxy, IDS, IPS, balanceadores).

- Revisar el documento de controles y contramedidas para que lo que expresen en el diagrama concuerde con la documentación, así como que las medidas de seguridad que no se pueden expresar gráficamente, sino en este documento sean correctas de tal forma que el nivel de seguridad del aplicativo sea del más alto nivel.

Una vez hecha la revisión anterior, el equipo realizará las correcciones pertinentes y se tendrá una segunda junta para comprobar que todo sea correcto. Si es aprobado, entonces toda ésta documentación es presentada al equipo de Seguridad de Estados Unidos, quienes dan sus recomendaciones y aprueban el desarrollo del proyecto y el equipo puede continuar su desarrollo, ya bajo las medidas de seguridad establecidas y aprobadas hasta llegar al Gate 6 o liberación a producción del aplicativo, cambio o actualización.

Previo a realizar la liberación, se realiza un escaneo de seguridad a los servidores utilizados por el aplicativo y se realiza todo el proceso de remediación detallado en el apartado anterior para asegurar que el aplicativo resida en un ambiente totalmente seguro.

Es importante mencionar que no todos los proyectos, cambio o actualizaciones se presentan a Estados Unidos, sólo aquellos que tienen un alto impacto para la compañía o que en su defecto tienen conexión hacia internet o que presentan algún servicio tercerizado.

1.12 Análisis y aprobaciones a solicitudes de apertura de sitios o nuevo software

De acuerdo a los procesos internos, cada vez que un usuario requiere acceso a una página web o la instalación de algún software, debe levantar un ticket con la mesa de ayuda quien me contacta para que analice el requerimiento y de mi aprobación.

De acuerdo al requerimiento se llevan diferentes procesos y análisis de seguridad que a continuación detallo:

Si es para la aprobación de una página web:

- Analizo la página web con un Sandbox, que tiene la compañía el cual simula las conexiones y comportamiento de la página web y da un resultado de riesgo de apertura el cual va de 0 a 10 siendo:
    - 1 a 4, posible la apertura del sitio ya que no presenta riesgo crítico.
    - 5 a 6, requiere un análisis más profundo de la página web para aprobar la apertura.
    - 7 a 10, imposible la apertura del sitio ya que presenta conexiones sospechosas, descarga malware al equipo o son páginas que se encuentran reportadas y están en algún blacklist.

Adicionalmente, se valida la justificación del usuario por la que solicita el acceso al sitio y finalmente se aprueba o rechaza el requerimiento con la debida justificación de por qué no se otorga el acceso.

En muchas otras ocasiones, se requiere el acceso a una página web o IP en específico, en estos casos, el usuario debe levantar un ticket con la mesa de ayuda solicitando una IP estática para su equipo y el de los usuarios que requieren el acceso, posteriormente nos debe enviar un formato de firewall con su requerimiento, ya que en estos casos el permiso no va sobre el proxy sino sobre el firewall para permitir la comunicación.

Dentro de este formato de firewall, debe incluir:

- Datos del solicitante
- Justificación
- Tipo de regla (permanente o temporal)
- IP(s) origen (IP estática solicitada previamente)
- IP(s) destino

- Puerto(s)
- Tipo de comunicación (unidireccional o bidireccional)

Se analiza el requerimiento con base en su justificación, origen, destino y si el puerto o protocolo utilizado es seguro impidiendo el robo de información o que ponga en riesgo la integridad de la compañía.

Posteriormente es enviada la aprobación, correcciones o rechazo con su debida justificación. Una vez corregido y aprobado el formato, entonces el usuario levanta su ticket con la mesa de ayuda enviando el formato firmado y aprobado para que posteriormente el cambio sea aplicado por el equipo de Telecomunicaciones.

Si es para la instalación de nuevo software:

- Busco las características del software y me baso en detalles como:
    - Fabricante
    - Última versión liberada
    - Tipo de soporte
    - Impacto al CPU del equipo y la red
    - Medios de descarga
    - Funcionamiento del software
    - Si es Open Source o se planea adquirir la licencia

- Busco las vulnerabilidades reportadas para el software requerido las cuales vienen reportadas de acuerdo al sistema de CVE donde:
    - 1 a 4, no presenta un riesgo alto la instalación del aplicativo.
    - 5 a 6, requiere un análisis mayor de la vulnerabilidad reportada.
    - 7 a 10, son vulnerabilidades críticas que ponen en alto riesgo la integridad y seguridad del equipo que ponen en riesgo a la compañía.

Después del análisis anterior, se envía la aprobación o rechazo al usuario con la debida justificación en caso de no proceder su requerimiento.

CAPITULO 2: PENTEST A EMPRESA DE SECTOR AUTOMOTRIZ

En este capítulo abordaré mi proyecto principal explicando con detenimiento cada uno de los procesos llevados a cabo, los ambientes evaluados, las metodologías utilizadas, los hallazgos, impactos y actividades adicionales que se fueron llevando a la par con la finalidad de obtener mejores resultados para estas pruebas de intrusión.

2.1 Antecedentes

Las primeras pruebas de penetración se realizaron en agosto de 2016 donde se percataron que la compañía era vulnerable a muchas amenazas que podrían afectar gravemente la producción. Por lo que, en enero de 2017, fecha en la que ingresé a la empresa, mi proyecto inicial fue documentar y estructurar la información generada durante la ejecución de pruebas de hackeo a los activos digitales de la empresa dónde se almacena información crítica (clientes y financiera).

Lo anterior, con el fin de localizar las áreas que sean focos rojos ante fugas de información e incumplimiento a las leyes mexicanas de datos y políticas de la empresa.

Un problema adicional, era la poca visibilidad en la red y la falta de detección oportuna de ataques o amenazas a la compañía; por lo que era necesario ganar visibilidad en la red mediante la implementación de procesos y herramientas de seguridad, coordinar diferentes áreas de sistemas en las diferentes localidades de la República Mexicana.

Las pruebas de penetración siempre son realizadas por un tercero y las remediaciones a las vulnerabilidades reportadas son hechas por mí. Como parte de nuestro proceso de verificación de controles de seguridad e incrementar la seguridad de nuestros sistemas e infraestructura de TI, se lanza el RFP para el inicio de las pruebas de intrusión o pentesting.

En total participan entre 3 y 5 proveedores diferentes, a cada uno de ellos se les hace llegar un documento con nuestros requerimientos y, a su vez, ellos nos entregan sus propuestas. Posteriormente, nosotros elegimos al ganador con base en su experiencia, conocimientos técnicos, propuesta, valor agregado al ejercicio y costo.

2.2 REQUERIMIENTOS DEL NEGOCIO

Se invita a los proveedores a realizar su propuesta económica y técnica para la ejecución de las pruebas de intrusión a la plataforma web y activos de La Compañía en donde destacan los siguientes:

- DMZ
- Red Interna
- Prueba de Ingeniería Social
- Prueba de Intrusión a la imagen del SO utilizado por la Compañía

2.3 META DEL PROYECTO

La meta de esta prueba es determinar las áreas vulnerables ante un ataque real, así como conocer la capacidad de detección y respuesta al mismo. Los objetivos son:

1. Verificación de los controles perimetrales de la red.

2. Obtener reporte ejecutivo, informe técnico incluyendo descripción del ataque realizado, recomendaciones sobre los hallazgos y solución de estos.

3. Identificar y recomendar medidas de seguridad para la infraestructura de TI y los datos de la Compañía.

2.4 ALCANCE DEL TRABAJO

La prueba deberá ser realizada bajo el enfoque *Gray Box*, el cual corresponde a la perspectiva interna y externa donde se proveerá información limitada de la infraestructura de la red administrativa y mediante técnicas de hacking externo e interno se obtendrá información necesaria para proseguir con el ataque. Se busca una prueba de seguridad cercana a un escenario de ataque real bajo la perspectiva tradicional de los ataques generados desde internet e internos y que afectan a los componentes expuestos hacia la red. Además, se deberá realizar la búsqueda y explotación de formas de acceso a la red interna o privada. El tiempo de ejecución de las pruebas será por un mes como máximo.

Los alcances son los siguientes:

DMZ

- Comprobar el nivel de exposición de información privada de La Compañía en Internet: Redes sociales, servicios de compartición de archivos (Dropbox, Drive, Mega, PasteBin, etcétera) y sitios de acceso público.
- Comprobar el nivel de seguridad de los sitios web principales de La Compañía, además de subdominios. Hablando de 87 sitios en total.
- Identificar, analizar y comprobar el nivel de seguridad de los controles perimetrales de la red mediante la explotación (acordada previamente) de los huecos de seguridad encontrados.

Red Interna

- Comprobar el nivel de seguridad de la red corporativa (264 servidores) ante un eventual ataque de empleados, visitantes o cualquier persona que tenga acceso a un segmento de red y pueda burlar los controles de seguridad para lograr acceder a información sensible.

Ingeniería Social

- Alcance limitado a ingeniería social con el objetivo de comprobar las medidas de seguridad ante intentos de robo de credenciales de cuentas institucionales en redes sociales y sitio web corporativo.

Pruebas de Seguridad a imagen del SO

- Comprobar el nivel de seguridad de la imagen del sistema operativo utilizada, con el objetivo de encontrar huecos de seguridad, así como obtener recomendaciones para un hardenizado mayor.

Pentesting exitoso

Se considerará como tal al lograr acceso a: Pantallas de sistemas, evidencia digital (base de datos), credenciales de cualquier cuenta, acceso a niveles administrativos del sistema, depósito de un archivo en el sistema de archivos, creación de cuenta en el DA (Directorio Activo) u obtención de cuenta de administración de privilegios altos, prueba de concepto de compromiso de la integridad de la información y hallazgo de información sensible.

2.5 ESTÁNDARES Y AMBIENTE TÉCNICO

Vulnerabilidades a evaluar

Se esperan como pruebas mínimas más no exclusivas durante la ejecución del proyecto:

- Reconocimiento de la red (escaneo y enumeración)
- Identificación de vulnerabilidades en la red
- Explotación de vulnerabilidades (previamente acordado)
- Escalamiento de privilegios
- Footprinting
- Ingeniería social
- Client side attack
- SQL Injection en sitios web
- LDAP Injection.
- Ataques de fuerza bruta
- Password & Hashing cracking.
- SSL MiTM
- Vulnerabilidad que pudiera resultar en DoS
- Enumeración de usuarios
- Web, OWASP top 10 (sobre aplicaciones qué deberíamos considerar)
- Auditoría de firewalls
- Y los que el proveedor pueda ofrecer previa validación con La Compañía.

2.6 Logística de trabajo

Durante la realización del proyecto el intercambio de información relativa al pentest (hallazgos, imprevistos, dudas) vía email con el líder de proyecto de La Compañía deberá ser utilizando algún algoritmo de cifrado como SHA256, SHA512, AES256 o utilizando PGP.

Trabajo desde las instalaciones de La Compañía

- Consultor en sitio (corporativo en DF)
- Podrá ser utilizado el equipo de cómputo del proveedor, el mismo deberá contar con los siguientes controles de seguridad:
    - Cifrado del disco duro / sistema de archivos.

Al finalizar las pruebas y después de haber entregado los reportes de resultados (ejecutivo y técnico) toda información deberá ser borrada de la computadora del proveedor por personal de La Compañía.

Manejo de evidencia:
Para el tratamiento de la evidencia generada durante el proyecto se deberá definir un esquema de almacenamiento seguro en conjunto con La Compañía.

2.7 Metodología de trabajo:

- Las pruebas de intrusión deberán ejecutarse conforme a los lineamientos establecidos por organismos reconocidos como EC-COUNCIL u OSSTM, debidamente validado por el Líder del Proyecto de La Compañía en las actas de seguimiento y deberán ser debidamente planeadas, donde el proveedor deberá describir con claridad y con el detalle necesario la metodología que seguirá para la ejecución de las pruebas.

- En caso de hallazgo crítico o de alto impacto, éste deberá ser reportado de manera inmediata a La Compañía como parte de los llamados hallazgos tempranos.

- Se deberá asignar un líder de proyecto, el cual será responsable de la comunicación con La Compañía acerca de las tareas y necesidades particulares del proyecto.

- Se realizarán reuniones semanales con el líder de proyecto para mostrar avances de los hallazgos hasta el momento.

- Las pruebas se deberán realizar con absoluto cuidado para no tener caídas o fallas de servidores, ciclos inactivos y otros problemas causados de manera inadvertida por las actividades.

- El líder técnico deberá previamente determinar los requisitos para ejecutar la prueba en un ambiente controlado.

- Por ningún motivo se autoriza al pentester a divulgar información de La Compañía obtenida como resultado de este ejercicio o por la ejecución del mismo.

- El líder técnico del pentest deberá mantener informado al líder del proyecto de La Compañía sobre el estado y avance de las pruebas.

- En caso de aparición de algún resultado destructivo o de interrupción o que se considere riesgoso y atente contra las premisas de seguridad, la prueba deberá ser interrumpida en forma inmediata, informando la novedad al Gerente del equipo de trabajo para la ejecución de las tareas de recuperación requeridas.

- Toda explotación de vulnerabilidades deberá ser previa aprobación por escrito del líder del proyecto de La Compañía y una vez que los objetivos principales han sido evaluados y seleccionados previamente con el fin de determinar el impacto que esta actividad tendría para La Compañía, garantizando las premisas de seguridad establecidas en estos términos de referencia.

  Por cada ciclo de prueba realizada se deberá entregar un informe ejecutivo que contenga como mínimo los siguientes elementos:

  - Descripción del trabajo realizado.
  - Resumen de las actividades realizadas.
  - Descripción del informe final entregado.
  - Descripción de principales hallazgos.
  - Conclusiones.
  - Recomendaciones.

Herramientas

Listar las posibles herramientas a utilizar por el equipo de pentest durante la prueba: Software de código abierto, o licencias comerciales con las que cuente el proveedor; se debe especificar qué herramientas se planean usar por cada fase.

2.8 DOCUMENTOS ENTREGABLES DEL PROYECTO

Lista de entregables:

El proveedor deberá entregar tanto en medio digital como impreso y en idioma español e inglés, lo siguiente:

1. Resumen ejecutivo:
    a. Objetivos de la evaluación, impacto de los hallazgos clave, recomendaciones de mitigación y facilidad de concretar el ataque.
    b. Acta de las actividades de seguimiento que realizó el proveedor y La Compañía durante la ejecución del objeto del contrato preparada y coordinada por el gerente del equipo de trabajo por parte del líder técnico del proveedor.
    c. Detalle de la definición de la clasificación del nivel de riesgos acordados para el proceso de evaluación de las vulnerabilidades, que se acordó con LA ENTIDAD.

2. Informe técnico:
    a. Tabla con listado de los hallazgos: Detalle de las vulnerabilidades descubiertas y/o explotadas, pruebas de concepto, implicaciones de los hallazgos y nivel de riesgo por probabilidad e impacto.
    b. Ruta de explotación (dónde inició el ataque y qué camino se siguió para llegar al objetivo).
    c. Evidencia de los hallazgos (pantallas, copias de la información, etcétera).
    d. Lista de los dispositivos comprometidos, y de los archivos copiados en cada uno de ellos (indicar rutas absolutas).

3. Informe de remediación:
    a. El informe deberá incluir un resumen con los hallazgos y las recomendaciones de remediación o mitigación por hallazgo.
    b. Podrá incluir recomendaciones de seguridad en base a la arquitectura de TI y seguridad de La Compañía.

4. Finalización

    a. Realizar una presentación de los resultados y un informe de nuevos tipos de pruebas que pueden ser aplicados a la infraestructura de La Compañía, que se recomiendan como resultado de cada escenario de pruebas realizado.

Los reportes deberán ser generados de en formato PDF firmados digitalmente y protegidos para su envío utilizando un método seguro (AES de 256 bits o PGP).

De manera adicional, para nosotros poder evaluar la propuesta y a los proveedores de una mejor manera solicitamos la siguiente información para poder tomar la mejor decisión de acuerdo a nuestras necesidades:

2.9 DESCRIPCIÓN DEL PROVEEDOR

- **Calificaciones del proveedor**

    - Información de la empresa y los participantes:
        - Empresa.
        - Tamaño de la compañía.
        - Ubicación física.
        - Participación en proyectos anteriores similares.
        - Años de experiencia.
        - Participación en conferencias de seguridad y publicaciones.
        - Referencias.

- **Descripción del equipo técnico que será asignado al proyecto. Se solicita lo siguiente:**

    - Designación del líder técnico. El líder técnico deberá contar con la mayor cantidad de certificaciones de Seguridad de la Información donde destaquen las siguientes:

        - Certified Network Defender
        - OPSEC Homeland Security
        - Certified Ethical Hacking
        - GIAC Penetration Tester

- Se requieren al menos dos consultores de Seguridad TI que formen parte del equipo asignado para la ejecución de las pruebas y quiénes deberán contar con al menos dos de las siguientes certificaciones de Seguridad de la Información:

  - Certified Network Defender
  - OPSEC Homeland Security
  - Certified Ethical Hacker
  - Certified Security Analyst
  - GIAC Penetration Tester
  - GIAC Certified Intrusion Analyst
  - Certified Hacking Forensic Investigator

- Proporcionar una muestra de un informe ejecutivo y técnico.

2.10 FORMATO DE PROPUESTA REQUERIDO

A continuación, se describe el formato requerido, orden y contenido para efectos de la propuesta.

Carta de cobertura de la propuesta: Debe incluir el nombre de la empresa, y datos generales de la misma, así como la persona que actuará como contacto para entrega y revisión de la propuesta misma.

Índice

1.0 Sumario ejecutivo

2.0 Visión del proyecto

2.1 Objetivos del proyecto y metas
2.2 Visión de entregables
2.3 Visión Lógica
2.4 Expectativas de eficiencia

3.0 Administración del Proyecto

3.1 Administración de la Información del Proyecto
3.2 Apreciación para la Calidad del proyecto
3.3 Estrategia de Comunicación con el Cliente
3.4 Estrategia de transferencia del conocimiento al equipo del proyecto
3.5 Estrategia para capacitación de usuarios

4.0 Organización del Proyecto

- 4.1 Estructura organizacional del Proyecto
- 4.2 Administración del proyecto y estructura de control
- 4.3 Resumen del Staff clave del proyecto

5.0 Estimación del Proyecto, Eventos claves y Plan de trabajo

- 5.1 Estimación del proyecto basado en Entregables
- 5.2 Eventos Claves externos al proyecto propuesto
- 5.3 Nivel de actividad del plan de trabajo del proyecto
- 5.4 Plan de Pagos asociado a Entregables del proyecto

6.0 Costos del Proyecto

7.0 Perfil del Proveedor

- 7.1 Antecedentes del Proveedor
- 7.2 Antecedentes del proveedor en proyectos de soporte
- 7.3 Antecedentes del proveedor en proyectos Automotrices
- 7.4 Antecedentes del proveedor en proyectos Financieros

8.0 Referencias y Recursos del Proveedor

- 8.1 Referencias de Proyectos de soporte
- 8.2 Referencias en proyectos Automotrices
- 8.3 Referencias en proyectos Financieros

9.0 Garantías

10.0 Precondiciones de la Propuesta

11.0 Cobertura de Seguros y Fianzas

12.0 Excepciones

13.0 Propuestas alternativas

14.0 Información adicional

2.11 Definición del problema y contexto de la participación profesional

Como se ha mencionado anteriormente, la falta de visibilidad en la red y la falta de un inventario actualizado de los servidores con información detallada de su ambiente, localidad y sistema operativo era clave para el proyecto de Pentest el cual comenzaría en febrero, por lo que durante enero en conjunto con el proceso de adaptación y entendimiento de la red, comencé a coordinar las áreas de sistemas encargadas de: servidores, infraestructura, endpoints y telecomunicaciones para obtener la información necesaria para las pruebas.

Comencé por el equipo de infraestructura y telecomunicaciones para comprender la estructura de la red, ubicación de dispositivos de capa 2 y 3 así como el alcance y asignación de los diferentes segmentos en LAN y DMZ. Para lo anterior, solicité un diagrama actualizado con la segmentación incluida. Esto era necesario para poder determinar los accesos y alcance de las pruebas de Pentest ya que no todos los segmentos son alcanzables desde donde estaría el proveedor.

Una vez comprendido lo anterior, me dirigí con el equipo de servidores en Aguascalientes para pedir un inventario de todos los servidores con la información mencionada anteriormente tanto en el ambiente de producción como en el de desarrollo. Al tener este inventario me percaté que muchos equipos tenían un sistema operativo obsoleto por el que seguramente cualquier atacante podría tener éxito o en este caso el proveedor que realizaría las pruebas de penetración.

Por otra parte, comencé con la identificación de los objetivos clave en la red, esto quiere decir aquellos activos que tienen un alto impacto en producción, así como aquellos equipos que probablemente su administración no fuera óptima o estuvieran desactualizados con el fin de escalar privilegios a través de ellos.

Al mismo tiempo, me dirigí con la dirección de endpoints para solicitar un inventario de los equipos con sus respectivas IP y asignaciones a cada empleado que incluyera: nombre de usuario, nombre de equipo asignado, localidad y modelo del equipo. Esto no sólo fue útil para el ejercicio de pentest sino también para las pruebas de ingeniería social ya que de esta manera se pudo realizar con mayor precisión y control.

Cabe mencionar que este primer período de pruebas únicamente estaba enfocado a LAN y equipos productivos. Posteriormente para el segundo semestre del año, se harían pruebas para DMZ y todas las aplicaciones en ella. El objetivo era detectar vulnerabilidades críticas que podrían permitir a los atacantes acceder y comprometer la información, su disponibilidad, integridad y confidencialidad. La prueba simuló ataques desde el perímetro interno y dirigido a los segmentos de red interna.

Las pruebas de Pentest comenzaron formalmente el lunes 13 de febrero de 2017. Para lograr identificar cualquier activo que pudiera ser vulnerable se realizó un escaneo pasivo a la red con la finalidad de identificar éstas vulnerabilidades en cada equipo para su futura explotación. Una vez concluido el escaneo,

se procedió a priorizar las vulnerabilidades de acuerdo al impacto que podría ocasionar al activo afectado de acuerdo al estándar CVE, esto permitiría a los pentesters poder explotar alguna vulnerabilidad que les permitiera comprometer el equipo y a partir de ahí escalar privilegios (ganar permisos de administrador), realizar movimiento lateral (utilizar las credenciales encontradas para comprometer más equipos en la red) y finalmente recopilar aquella información crítica o confidencial que pudiera representar un hallazgo importante para posteriormente dar las mejores recomendaciones de seguridad y resguardo de la información.

Durante las pruebas de penetración, se pudieron percatar de muchas vulnerabilidades que les permitieron comprometer la red en tan solo un día. Todo hallazgo o vulnerabilidad crítica nos era reportada, esto con la finalidad de remediar aquellas que representaran un riesgo crítico para la compañía, la información de la empresa y clientes o un posible ataque de denegación de servicio entre otros.

Las pruebas duraron dos semanas durante las cuales se obtuvo acceso a mucha información gracias a la cantidad de equipos vulnerables. Los pentesters lograron entrar a la red, tomar muestras de información encontrada, tener permisos de administrador al grado de poder crear una cuenta dentro del Directorio Activo de la compañía como un Domain Admin y a partir de ahí tener acceso a todos los activos. Lograron comprometer cámaras de seguridad de las plantas, demostrando lo fácil que sería poder manipular las grabaciones de las mismas, acceso a sitios con credenciales por default e inyecciones de código entre muchas otras.

Posterior a estas dos semanas, se realizó un ejercicio de ingeniería social. Ingeniería social es aquella práctica de infiltración a la organización mediante algún archivo o correo malicioso o incluso accediendo físicamente a la compañía con el fin de obtener información privilegiada y obtener algún beneficio a cambio. Para esta prueba, todo fue controlado y con la finalidad de demostrar a la compañía lo fácil que es comprometer la información de un usuario y de esta manera incrementar el conocimiento de seguridad de los usuarios para que aprendan a identificar y reportar archivos o correos maliciosos que pudieran dañar y comprometer la información de la compañía, actividad sospechosa en su equipo como lentitud, apagados repentinos, cifrado o borrado de archivos entre otros.

En esa ocasión, para las pruebas de ingeniería social se optó por tres formas distintas:

- Correo de phishing acerca de un evento reciente
- Correo de phishing de una cuenta por pagar falsa
- USB Drop Attack

El correo de phishing acerca de un evento reciente de la compañía, trataba de un supuesto resumen del evento, algunas imágenes y un link que, de acuerdo al correo, este te llevaba a un sitio web donde podías observar las imágenes del evento, entre otras cosas. Sin embargo, este ejecutaba el payload oculto en el archivo, estableciendo una comunicación entre el equipo de la víctima y el del pentester.

Los elementos para identificar que se trataba de un correo malicioso eran:

- Dirección del remitente diferente, es decir: los comunicados son enviados por una cuenta interna dedicada a estos fines, sin embargo, este correo había sido enviado por una cuenta totalmente distinta y con un dominio externo.
- El nombre de la compañía estaba mal escrito.
- Si posicionabas el cursor sobre el link a abrir, la URL a la que enviaba no era nada relacionada con la compañía.

El correo de la cuenta por pagar, era un poco más complicado de identificar ya que se trataba de un correo supuestamente de una institución gubernamental reclamando el pago de derechos e impuestos o de un club para adultos que de igual forma reclamaba un pago. Adjunto venía un archivo de Word con los detalles de la supuesta deuda, el detalle aquí es que, para ver los conceptos a pagar, tenías que deshabilitar el modo seguro de Word. En el momento que el usuario lo deshabilitaba, el payload era ejecutado estableciendo la comunicación previamente mencionada.

En este caso los elementos eran:

- Si no debías nada a la institución o nunca habías ido a ese club, no tenías por qué abrir el correo.
- El remitente no era ni siquiera relacionado con el contenido del correo.
- Si dudas de la procedencia del correo, no descargues archivos adjuntos y si ya lo hiciste no lo abras y menos deshabilites el modo seguro de Word.

Finalmente, USB Drop Attack, es un ejercicio en el cual se tiran USB por la compañía con el objetivo que un usuario la encuentre y la conecte al equipo. Previamente, se graban archivos con nombres que pudieran tentar al usuario a abrir las carpetas y archivos incluidos. Sin embargo, en el momento que el usuario abre el archivo incluido, se ejecuta el payload, se establece la comunicación previamente mencionada, comprometiendo a la computadora.

Esta comunicación permitió al pentester, comprometer el equipo completamente, es decir tener control total del mismo. Entre otras cosas, el pentester era capaz de realizar lo siguiente de manera remota:

- Tomar capturas de pantalla
- Grabar audios
- Activar la webcam y tomar fotos o videos
- Activar un Keylogger y robar credenciales de acceso o información bancaria
- Copiar archivos
- Ejecutar cualquier comando o abrir cualquier archivo

- Programar tareas en el equipo para, por ejemplo, apagar o encender la computadora

Las pruebas fueron dirigidas especialmente al área de marketing ya que son ellos los que reciben información de muchas fuentes diferentes, desde proveedores hasta correos de parte de clientes de la compañía.

En total, lograron comprometer los equipos de cinco usuarios distintos, de uno de ellos, se lograron obtener las credenciales de todas sus redes sociales, accesos a cuentas bancarias y correos. De todos los usuarios se obtuvieron capturas de pantalla de lo que realizaban en ese momento en el equipo, se activó también la webcam obteniendo una foto del usuario y se grabó la presentación de un nuevo proyecto sólo por unos segundos para demostrar el alcance de la prueba.

Se tuvo una junta con cada uno de los usuarios comprometidos para informarles que habían sido víctimas de estas pruebas de ingeniería social, cómo es que había sido posible hackearlos y la información que se obtuvo de cada uno de ellos. En los casos en los que se comprometieron cuentas personales, se les mostró una imagen con las cuentas comprometidas, se les hizo la petición que cambiaran todas sus contraseñas y se les indicó que su información sólo era a fin de las pruebas realizadas por la compañía y estas contraseñas nunca fueron utilizadas para otros fines y toda evidencia fue borrada enfrente del usuario.

Los resultados de estas pruebas fueron presentados al director y subdirectores de sistemas y presidente de la compañía. Se les mostraron las diferentes y diversas vulnerabilidades halladas, el impacto que podrían tener, así como el plan de trabajo para las remediaciones de las mismas.

De tal forma que, posterior a haber presentado los resultados, procedimos con las remediaciones. Este proceso tomó alrededor de dos meses ya que el primer paso fue contactar al administrador del servidor, aplicación o equipo afectado para notificarles de las vulnerabilidades encontradas, después, preparar un reporte por administrador o dueño de aplicativo donde se incluyera toda la información relacionada con las vulnerabilidades que afectaran sus equipos, ese incluía CVE asociado, criticidad, host, nombre, descripción y solución para remediar las vulnerabilidades halladas.
Sin embargo, debido a que ciertos aplicativos son muy críticos, o su desarrollo o ambiente son muy delicados, teníamos que medir el impacto que podrían causar al negocio las remediaciones sugeridas y en caso de no poder aplicar el parche o configuración necesaria, buscar una contramedida que nos protegiera contra la vulnerabilidad. Después de este proceso de reconocimiento y entendimiento, se corrigieron las 23 vulnerabilidades encontradas.

Entre el término de estas pruebas y el comienzo de las siguientes, ocurrió un evento de seguridad global. Se dieron a conocer un grupo de hackers conocidos como: The Shadow Brokers, quienes afirmaban haber robado herramientas forenses y de seguridad de la CIA y la NSA que permitirían explotar vulnerabilidades de día cero. El viernes 12 de Mayo del 2017, se registró el mayor ataque cibernético de la historia a nivel global gracias a un ransomware llamado WannaCry.

Un ransomware es un programa que secuestra la información de tu computadora, es decir, la cifra y posteriormente pide un pago a cambio de la llave para descifrar tu información, siendo muy riesgoso pagar ya que nada garantiza que te vayan a entregar la llave de cifrado o que tus archivos ya hayan sido eliminados.

Este ciberataque avanzó aceleradamente, en un lapso de tan sólo 12 horas ya se había propagado a 100 países logrando comprometer información gubernamental de los diferentes países, empresas y equipos personales. En ese mismo lapso de tiempo, logró recaudar 360,000 USD de todos aquellos usuarios que pagaron esperando recuperar su información.

¿Por qué tuvo un impacto tan alto? Debido a una herramienta liberada por el grupo de hackers previamente mencionado que explotaba una vulnerabilidad de día cero sobre un protocolo de comunicación llamado SMB sobre el puerto 445. Esta vulnerabilidad permitía al atacante obtener una sesión remota del equipo y controlarlo, sin embargo, este ransomware también tenía características de un gusano es decir que se propagaba por la red velozmente, en otras palabras, al entrar a tu equipo ejecutaba 3 archivos maliciosos: el primero cifraba tu información, el segundo te daba la pantalla de error y advertencia y el tercero comenzaba a buscar los equipos en red con el puerto 445 abierto y sin el parche de Microsoft para comprometer el equipo. A pesar de que Microsoft había liberado un parche de seguridad para remediar esa vulnerabilidad con un mes de anticipación pocas empresas y gobiernos lo aplicaron permitiendo que este ransomware comprometiera sus equipos.

En la empresa, tenemos un proceso de parcheo el cual se realiza de forma mensual para servidores y endpoints, sin embargo, para el momento que comenzó la propagación de este malware se había aplicado el parche al 80% de equipos. De un total de 8,000 equipos se lograron parchar 6400 equipos, el resto, eran vulnerables. Este ataque comenzó en Asia, posteriormente afectó a Europa alrededor del mediodía hora de México. A las 6 p.m., nos fue reportado el primer equipo infectado en el área financiera de la compañía, área a la cual estaban programadas para junio las siguientes pruebas de penetración. El primer equipo infectado fue el de un usuario que recibió un mal sospechoso, lo abrió y descargó el archivo permitiendo al ransomware entrar al equipo.

El problema radicó en que toda la información previamente mencionada relacionada con la vulnerabilidad y el ransomware, no estuvo disponible hasta casi después de las primeras 12 horas del ataque por lo que el proceso de reconocimiento y remediación fue literalmente a contra reloj. Como lo mencioné anteriormente, este malware era distribuido por la red velozmente por lo que al tener el primer equipo infectado era sólo cuestión de tiempo para que comenzara a propagarse. Y así fue, en tal sólo dos horas ya teníamos 20 equipos infectados.

El plan de acción fue el siguiente:

1) Coordinarnos con el equipo de servidores y endpoints de Aguascalientes, Toluca y Cuernavaca.
2) Coordinarnos con el equipo de Estados Unidos y con el de Europa, específicamente Reino Unido quienes nos reportaron que la planta de Renault en Francia había tenido una afectación tan grande que tuvieron que parar actividades y cerrar la planta.
3) Desconectar de la red lo equipos infectados para contener la infección.
4) A la par de los pasos anteriores, investigar acerca del ransomware para saber cómo operaba e identificar alguna remediación y técnica de mitigación.
5) Una vez identificado el funcionamiento del ransomware, logramos entender su comportamiento y encontrar el parche para aplicarlo a los equipos que hicieran falta.
6) Escanear repetidamente la red con diferentes herramientas para asegurar la aplicación del parche al 100 por ciento.

Logramos contener la infección satisfactoriamente al tener sólo 100 equipos infectados a nivel nacional de un total de 8,000 es decir sólo el 1.25% de infección total. Posterior a este proceso, me decidí a investigar más acerca de la vulnerabilidad aprovechada por este ransomware y me percaté que la misma herramienta liberada por The Shadow Brokers, servía para escanear la red y encontrar si había equipos vulnerables, infectados o con el puerto 445 habilitado, así que propuse el siguiente plan de acción el cual fue aprobado inmediatamente:

1) Utilizar la herramienta liberada por el grupo de hackers para escanear todos los segmentos de red.
2) Utilizar NMAP para escanear la red en busca de equipos con el puerto 445 habilitado.
3) Utilizar Nessus para comprobar que no faltara el parche de seguridad a ningún equipo.
4) Cruzar los resultados de los tres puntos anteriores y entregar el reporte con la remediación adecuada, es decir: aplicar el parche y desactivar el puerto 445 de ser posible.

Este evento nos ayudó a mejorar y reforzar el procedimiento de aplicación de parches de seguridad de tal forma que un mes después no tuvimos un solo equipo infectado cuando The Shadow Brokers liberó otra herramienta similar y se creó un nuevo malware llamado Not Petya, el cual aprovechaba la misma vulnerabilidad de WannaCry, entraba a los equipos, pero con la intención de robar las credenciales de administrador y realizar movimiento lateral y de esta manera comprometer todos los equipos de la organización.

Una vez concluidas las acciones para la remediación de equipos infectados, se realizaron las pruebas de penetración al brazo financiero de la compañía, pero con casi un mes de atraso debido al incidente de seguridad ocurrido.

Siguiendo la misma metodología de identificación de activos, alcances de red y distribución entre las localidades de los equipos, se obtuvieron muchas más vulnerabilidades que las encontradas en el primer ejercicio, hablando de un total de 800 vulnerabilidades.

Debido a la cantidad de vulnerabilidades halladas y la criticidad de las mismas, coordiné de manera inmediata al equipo de la financiera y servidores para identificar en cuáles equipos podríamos aplicar de manera inmediata los parches necesarios, en cuáles se iba a requerir un análisis y precaución mayor por el impacto que podría ocasionar la aplicación de algún parche o cambio en configuraciones.

Este proceso de remediación se tomó casi 3 meses debido a la cantidad de las vulnerabilidades, procesos internos de freeze, así como poder programar ventanas de tiempo para aquellos casos en los que era necesario un reinicio o interrumpir algún servicio.

Se lograron remediar un total de 795 vulnerabilidades, el resto no fue posible debido a la incompatibilidad de algunas aplicaciones en cuanto al framework, protocolos de comunicación necesarios para su operación o requerimientos de software para su funcionamiento adecuado, cabe mencionar que las vulnerabilidades que no fueron remediadas, no presentan un riesgo alto ni crítico para la compañía.

2.12 METODOLOGÍA UTILIZADA

En el área en la cual me desempeño es muy importante tener presente y emplear las siguientes metodologías para la detección de vulnerabilidades, ataques, remediación y recopilación de evidencia mediante técnicas forenses:

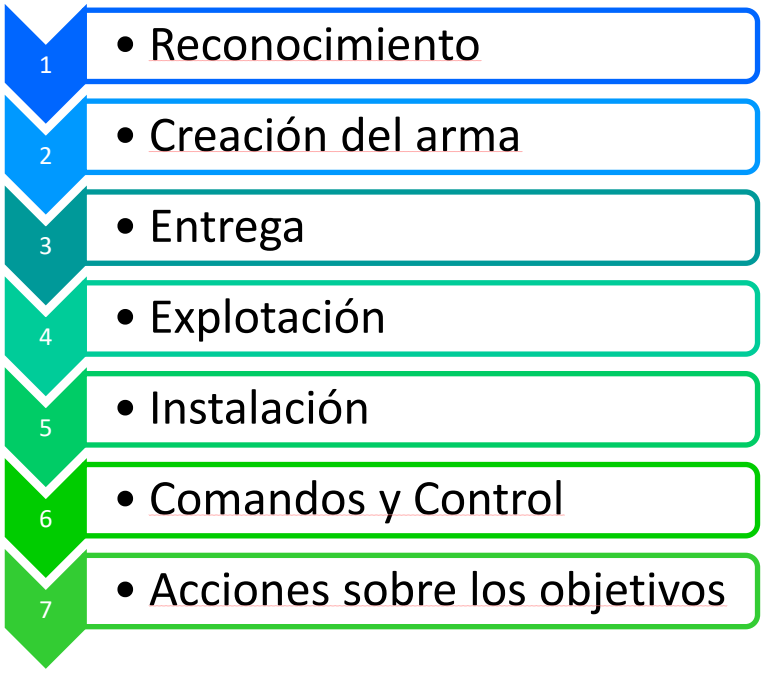


Figura2. Cyber Kill Chain

Fases de una intrusión (Cyber Kill Chain)

- **Reconocimiento:** Recopilación de información como correos, información en internet, correos de phishing, etc.

- **Creación del arma:** Crear un programa o utilizar alguno ya existente para comprometer la máquina y poder tener acceso a la organización cuando sea necesario.

- **Entrega:** Transmitir el código previamente mencionado al objetivo mediante correo, usb e incluso de manera directa si es que se tiene acceso físico al mismo.

- **Explotación:** Aprovechar alguna vulnerabilidad en el sistema operativo o software instalado para ejecutar algún exploit o el programa previamente creado.

- **Instalación:** El software malicioso se asegura de poder ejecutarse de forma permanente en el equipo infectado.

- **Comandos & Control:** Asegurarse que el programa malicioso tenga conexión con la computadora del hacker, proporcionando al atacante control remoto.

- **Acciones sobre los objetivos:** El atacante cumple su objetivo principal por el cual atacó a ese equipo u organización, puede ser robo de información, espiar, informar de las vulnerabilidades a la organización e incluso sólo por medir sus capacidades de hackeo.

Arquitectura de 2 capas:

La arquitectura tradicional de cliente/servidor también es conocida como arquitectura de dos capas. Ésta requiere una interfaz de usuario que se instala y se ejecuta en una PC o estación de trabajo y envía solicitudes a un servidor para ejecutar distintas operaciones.

Se dice que es de dos capas ya que cuenta con dos niveles en su estructura:

Nivel de Aplicación: Es la capa que se encarga de la interacción con el usuario, muestra el sistema al usuario, le presenta información y la obtiene también del usuario. También es conocida como interfaz gráfica y debe tener la característica de ser amigable, es decir, entendible y fácil de usar para el usuario.

Nivel de Base de Datos: Este nivel es la capa en donde se almacena toda la información ingresada en el sistema por el usuario o administradores y que puede ser depositada de manera permanente o temporal (debido a una eventual depuración).

Como características de esta arquitectura tenemos:

- Protocolos asimétricos
- Intercambios basados en mensajes
- Recursos compartidos

Arquitectura de 3 capas:

Esta arquitectura define cómo organizar los componentes de una capa y que éstos sólo puedan hacer referencia a componentes en capas inmediatamente inferiores. Esto permite identificar qué recursos podemos reutilizar en el desarrollo de las aplicaciones y utilización de hardware.

Se dice que es de tres capas ya que cuenta con tres niveles en su estructura:

Nivel de Aplicación: Es la capa que se encarga de la interacción con el usuario, muestra el sistema al usuario, le presenta información y la obtiene también del usuario. También es conocida como interfaz gráfica y debe tener la característica de ser amigable, es decir, entendible y fácil de usar para el usuario. Ésta capa se comunica únicamente con la capa intermedia o de servicios.

Nivel de Servicios: Es en esta capa donde residen las funciones que se ejecutan en las otras dos capas, se reciben las peticiones del usuario, se procesa la información y se envían las respuestas al proceso en cuestión. Se denomina capa de servicios porque es aquí donde se establecen todas las reglas y configuraciones que deben cumplirse. Esta capa se comunica con la capa de aplicación para recibir las solicitudes y presentar resultados y con la capa de base de datos para solicitar al gestor el almacenamiento y recuperación de datos.

Nivel de Base de Datos: Ésta capa es la encargada de almacenar los datos del sistema y de los usuarios. Su función es almacenar y devolver los datos a la capa de aplicación. Está conformada por uno o varios gestores de bases de datos que pueden estar localizadas en uno o muchos servidores.

Esta arquitectura se utiliza para sistemas complejos que requieren de grandes cantidades de procesamiento de información así como para incrementar el nivel de seguridad e integridad de los datos ya que al tener los servicios separados en tres capas diferentes, permite que si un servidor presenta alguna afectación, el impacto al negocio y aplicación no sea tan grande y sea más económico reparar la falla. En caso de una ataque cibernético hace mucho más sencillo localizar el patrón por el que atacaron el sistema y al estar la información resguardad en la capa más baja (base de datos), es mucho más complicado que un atacante logre entrar hasta ese nivel ya que por lo general entre capas existen firewalls y detectores de intrusos para identificar y bloquear el tráfico sospechoso y cualquier otro intento de ataque.

Por otra parte, es importante tener presentes los puertos más comunes de comunicación tanto TCP como UDP:

- 21 FTP
- 22 SFTP
- 23 Telnet
- 25 SMTP
- 53 DNS
- 80 HTTP
- 88 Kerberos
- 194 IRC
- 389 LDAP
- 443 HTTPS
- 445 SMB
- 636 LDAPS
- 1433 SQL
- 1521 Oracle
- 3389 RDP

CAPITULO 3: RESULTADOS

Como parte de mi trabajo en la compañía y con base en los proyectos realizados se lograron los siguientes resultados:

Pentest:

Antes	Durante	Actualmente
Vulnerabilidades internas: **47**	Vulnerabilidades internas: **15**	Restantes: **0**
Vulnerabilidades en manufactura: **No contemplado en el alcance de pruebas**	Vulnerabilidades en manufactura : **8**	Vulnerabilidades en manufactura: **0**
Segmentación adecuada de la red	Aplicación de parches de seguridad al término del mes	Aplicación de parches de seguridad previo al término del mes y un escaneo para comprobar aplicación al 100%

Figura 3. Resultados Pentest a empresa en LAN y ambientes

Posteriormente, en el segundo semestre del año se hicieron las mismas pruebas para los activos en el brazo financiero y DMZ obteniendo los siguientes resultados:

Antes	Actualmente
Vulnerabilidades: **800**	Restantes: **5**
Vulnerabilidades en aplicaciones**: 16**	Restantes: **0**

Figura 4. Vulnerabilidades Pentest en DMZ y financiera

Las vulnerabilidades de ambas pruebas hacen referencia a errores de configuración, malas prácticas de segmentación y de controles de acceso.

Vulnerabilidades detectadas en servidores

Mediante los análisis realizados con Nessus dirigidos a servidores obtuve los siguientes resultados.

Servidores en LAN y DMZ en brazo financiero:

Vulnerabilidades	Cantidad
Críticas	6
Altas	488
Medias	132
Bajas	9
Total	635

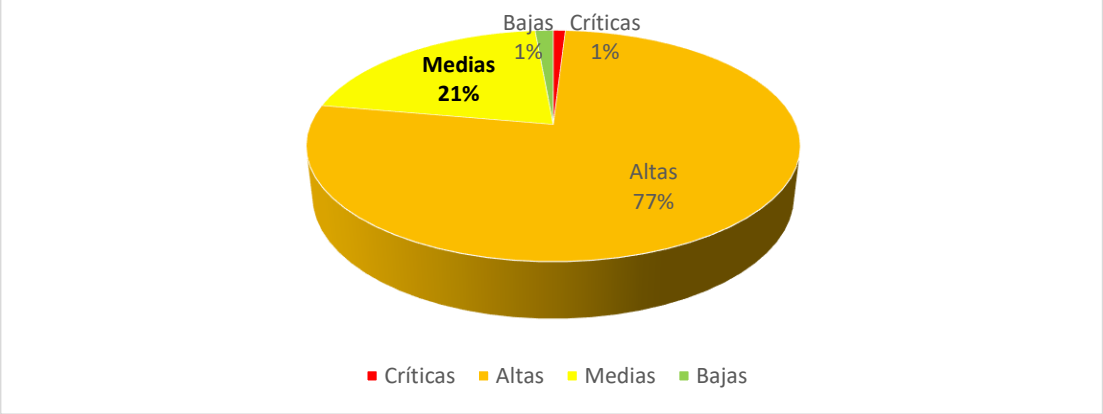


Figura 5. Vulnerabilidades en servidores

Éstas vulnerabilidades, son derivadas de software desactualizado y la falta de aplicación de parches de seguridad.

Para su remediación se creó un plan de trabajo a un mes y medio para remediar el 78% de las vulnerabilidades (críticas y altas) y otro mes para remediar el otro 22% (medias y bajas).

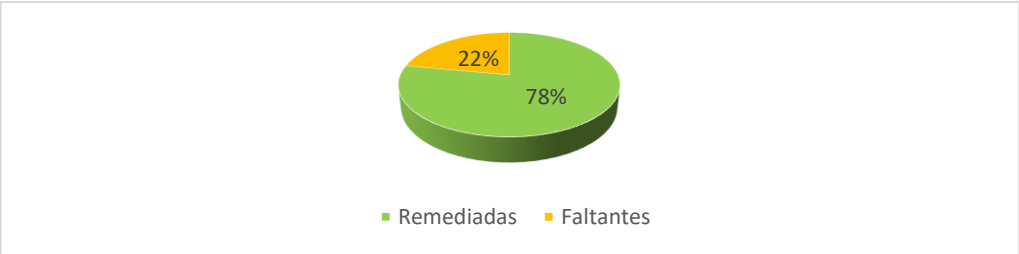


Figura 6. Progreso actual de remediaciones

Servidores en LAN y DMZ:

Ambiente	Criticidad	Cantidad
Producción	Críticas	47
	Altas	191
	Medias	637
	Bajas	103
	Total	**978**

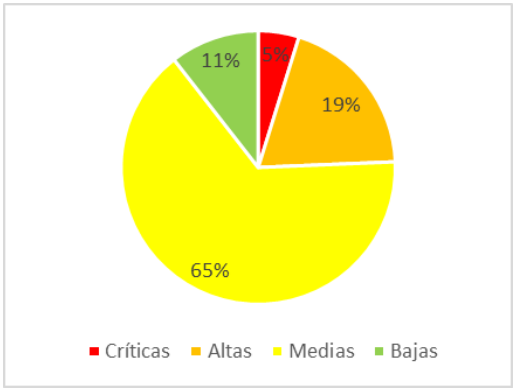


Figura 7. Producción

Ambiente	Criticidad	Cantidad
Desarrollo	Críticas	28
	Altas	104
	Medias	54
	Bajas	2
	Total	**188**

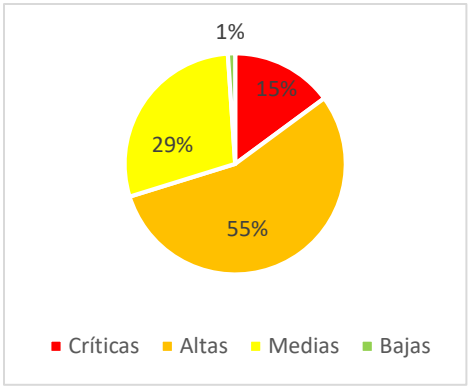


Figura 8. Desarrollo

Equipos Escaneados	
Producción	158
Desarrollo	34

Figura 9. Resultados sobre vulnerabilidades en LAN y DMZ a servidores de la empresa

Éstas vulnerabilidades, son derivadas de igual forma por software desactualizado y la falta de aplicación de parches de seguridad. Para su remediación se creó un plan de trabajo a un mes para remediar en su totalidad las vulnerabilidades.

Figura 10. Progreso actual de remediaciones

Carbon Black:

Actualmente seguimos en proceso de pruebas para evitar impactar en la producción y que el cambio no sea afecte a los 8,000 usuarios.

El progreso actual es el siguiente:

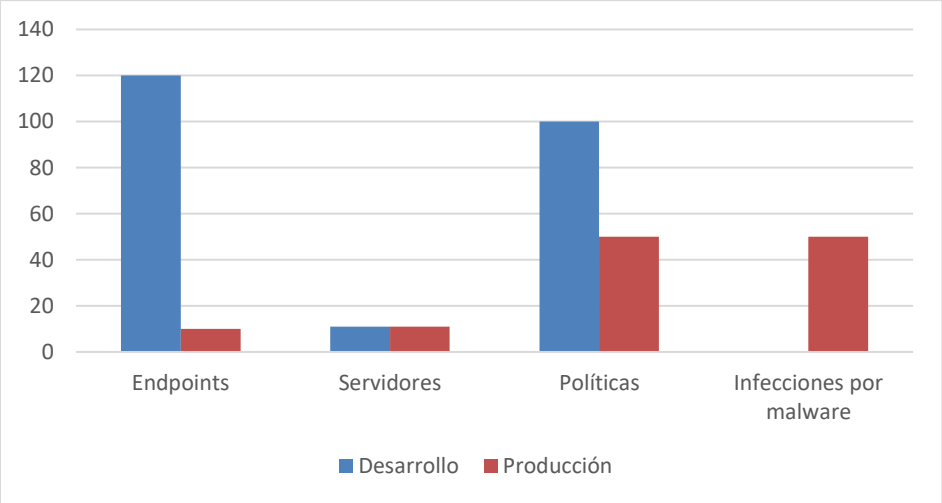


Figura 11. Progreso actual de implementación de Carbon Black

La creación de las políticas de restricción para Carbon Black están directamente relacionadas con las políticas de la compañía de software autorizado, así como las mejores prácticas de seguridad ya que no sólo bloquea la ejecución o instalación de software no autorizado, sino que también, bloquea la ejecución de archivos maliciosos, por lo que, es necesario definir qué archivos están permitidos y cuáles no dependiendo de las características que presentan los malware.

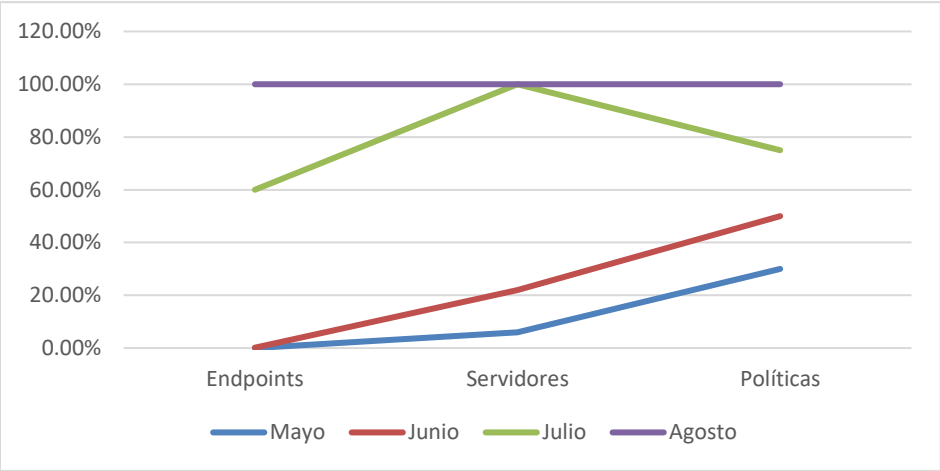


Figura 12. Proyección de aplicación a endpoints y servidores, así como de políticas de bloqueo

CONCLUSIONES

Como consecuencia de lo expuesto en el informe, gracias a mi incorporación a la compañía, los análisis y ejercicios realizados logré robustecer la seguridad en la organización, incrementar la visibilidad de los eventos de seguridad, prevenir infecciones e incrementar el nivel de cultura organizacional de seguridad de la información.

Aunado a esto, gracias a las nuevas medidas de seguridad y el monitoreo realizado, logré disminuir la cantidad de equipos infectados por malware, logré evitar el impacto del ransomware Not – Petya y finalmente logré mejorar el tiempo de respuesta para la detección de equipos infectados, logrando recuperarlos y vacunarlos en tan sólo dos días, siendo que el tiempo anterior era una semana.

Por otra parte, gracias a la implementación de Carbon Black, ganaremos visibilidad de todos los equipos y servidores críticos para la producción, en caso de un incidente lograremos identificar al paciente cero y contener la infección rápidamente logrando que el nivel de equipos infectados sea mucho menor incluso al ocurrido cuando la infección de Wannacry.

Como nuevas medidas de seguridad para la infraestructura, implementé un proceso de escaneo y monitoreo mensual para tener los servidores con las actualizaciones más recientes y así evitar el robo de información sensible como, por ejemplo, la información de clientes o de diseños de la compañía. Continué con el proceso de certificación de usuarios privilegiados, la cual es una práctica para garantizar que las cuentas con accesos privilegiados o especiales sean las correctas, sean bajas aquellos que no sigan en la compañía y garantizar que aquellos usuarios con acceso en verdad lo requieran. De esta manera podemos prevenir la fuga de información, controlar los accesos e identificar de una mejor forma las intermitencias o incidencias en los diferentes servicios y aplicaciones.

En conclusión, la seguridad en la compañía ha aumentado considerablemente, llevamos más de un año sin un incidente de seguridad como el de Wannacry. Todos los activos de la compañía están siendo monitoreados y recibiendo las últimas actualizaciones de seguridad, las cuales son liberadas el segundo martes de cada mes y a su vez, en caso de una vulnerabilidad de día cero, creé un proceso de identificación y aplicación de parches críticos emergentes en un lapso no mayor a tres días.

GLOSARIO

Active Directory

Active Directory almacena datos como objetos. Un objeto es un elemento único, como un usuario, grupo, aplicación o dispositivo, como una impresora. Normalmente, los objetos se definen como recursos, como impresoras, computadoras, usuarios y grupos.

Active Directory clasifica los objetos por nombre y atributos. Por ejemplo, el nombre de un usuario puede incluir la cadena de nombre, junto con la información asociada con el usuario, como contraseñas, área, puesto, entre otras.

El servicio principal en Active Directory es Domain Services (AD DS), que almacena información del directorio y maneja la interacción del usuario con el dominio. AD DS verifica el acceso cuando un usuario inicia sesión en un dispositivo o intenta conectarse a un servidor a través de una red. AD DS controla qué usuarios tienen acceso a cada recurso. Por ejemplo, un administrador generalmente tiene un nivel de acceso a los datos diferente al de un usuario final.

Ataque de fuerza bruta

Implica intentar descifrar una clave intentando cada palabra y clave posible hasta que se obtenga la traducción legible del texto cifrado en texto en claro.

Black Box

En una asignación de prueba de caja negra o Black Box, el pentester se coloca en el rol de hacker promedio, sin conocimiento interno del sistema objetivo. Los pentesters no reciben ningún diagrama de arquitectura o código fuente que no esté disponible públicamente. Una prueba de penetración de caja negra determina las vulnerabilidades en un sistema que se pueden explotar desde fuera de la red.

Esto significa que las pruebas de penetración de la caja negra se basan en el análisis dinámico de los programas y sistemas actualmente en ejecución dentro de la red objetivo. Un pentester de caja negra debe estar familiarizado con las herramientas y metodologías de escaneo automatizadas para las pruebas de penetración manual. También deben ser capaces de crear su propio mapa de una red objetivo en función de sus observaciones, ya que no se les proporciona ningún diagrama de este tipo.

El conocimiento limitado proporcionado hace que las pruebas de penetración de caja negra sean las más rápidas de ejecutar, ya que la duración de la asignación depende en gran medida de la capacidad del pentester para localizar y explotar vulnerabilidades en los servicios externos del objetivo. El principal inconveniente de este enfoque es que, si los evaluadores no pueden acceder al perímetro, las vulnerabilidades de los servicios internos permanecen sin descubrir y sin parchar.

Blacklisting

La lista negra de una computadora detalla las entidades maliciosas o sospechosas conocidas a las que no se les debería permitir el acceso o los derechos de ejecución en un sistema o red.

Estas entidades incluyen software malicioso como virus, troyanos, gusanos, spyware, keyloggers y otras formas de malware. Pero dependiendo del entorno y el alcance de la aplicación, las entidades incluidas en la lista negra pueden extenderse para incluir usuarios, aplicaciones empresariales, procesos, direcciones IP y organizaciones que se consideran una amenaza para una empresa o individuo.

Las listas negras se han implementado tradicionalmente como un elemento clave en las suites de software antivirus y de seguridad, generalmente en forma de "base de datos de virus" de firmas digitales conocidas, heurísticas o características de comportamiento asociadas con virus y malware que se han identificado en la naturaleza.

Es importante hacer énfasis que este concepto se basa en las amenazas conocidas. Las firmas de virus y otras formas de listas negras se basan en la inteligencia de seguridad y en la experiencia de los vectores de ataque, las vulnerabilidades, malware y para aquellas amenazas que ya se conocen o desarrollaron contramedidas. Contra amenazas desconocidas como las amenazas de día cero, las listas negras tienen un valor muy limitado o nulo.

Capa 1 - Física

La capa Física del modelo OSI es la que se encarga de la topología de red y de las conexiones globales de la computadora hacia la red, se refiere tanto al medio físico como a la forma en la que se transmite la información

Capa 2 - Enlace de datos

Al obtener datos de la capa física, la capa de enlace de datos comprueba los errores de transmisión física. La capa de enlace de datos también administra esquemas de direccionamiento físico, como direcciones MAC para redes Ethernet, controlando el acceso de varios dispositivos de red al medio físico.

Capa 3 – Red

La capa de red agrega el concepto de enrutamiento sobre la capa de enlace de datos. Cuando los datos llegan a la capa de red, se examinan las direcciones de origen y destino contenidas dentro de cada marco para determinar si los datos han alcanzado su destino final. Si los datos han llegado al destino final, esta capa 3 formatea los datos en paquetes entregados hasta la capa de transporte. De lo contrario, la capa de red actualiza la dirección de destino y empuja el marco hacia las capas inferiores.

Para admitir el enrutamiento, la capa de red mantiene direcciones lógicas, como direcciones IP para dispositivos en la red. La capa de red también administra la asignación entre estas direcciones lógicas y direcciones físicas.

Capa 4 – Transporte

La capa de transporte proporciona datos a través de las conexiones de red. TCP es el ejemplo más común de un protocolo de red de capa 4. Los diferentes protocolos de transporte pueden admitir un rango de capacidades opcionales que incluyen recuperación de errores, control de flujo y soporte para la retransmisión.

Capa 5 – Sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

Capa 6 – Presentación

La capa de presentación es la más simple en función de cualquier pieza del modelo OSI. En la Capa 6, maneja el procesamiento de la sintaxis de los datos del mensaje, como las conversiones de formato y el cifrado / descifrado necesario para admitir la capa de aplicación que se encuentra por encima de ella.

Capa 7 – Aplicación

La capa de aplicación proporciona servicios de red a las aplicaciones de usuario final. Los servicios de red suelen ser protocolos que funcionan con los datos del usuario. Por ejemplo, en una aplicación de navegador web, el protocolo de capa de aplicación HTTP empaqueta los datos necesarios para enviar y recibir contenido de la página web. Esta capa 7 proporciona datos para (y obtiene datos de) la capa de presentación.

DMZ

Por sus siglas en inglés: De-Militarized Zone o Zona desmilitarizada es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa los equipos en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS. Y es precisamente estos servicios alojados en estos servidores los únicos que pueden establecer tráfico de datos entre el DMZ y la red interna, por ejemplo, una conexión de datos entre el servidor web y una base de datos protegida situada en la red interna.

Domain Admin

Los miembros de este grupo tienen el control total del dominio. De forma predeterminada, este grupo es miembro del grupo Administradores en todos los controladores de dominio, todas las estaciones de trabajo del dominio y todos los servidores miembros del dominio en el momento en que se unen al dominio. De forma predeterminada, la cuenta de administrador es un miembro de este grupo. Debido a que el grupo tiene control total en el dominio, hay que agregar usuarios con precaución.

Endpoints

Equipo personal o de usuario final.

Escaneo de vulnerabilidades

Una evaluación de vulnerabilidades es una auditoría interna de la red y seguridad del sistema; cuyos resultados indican la confidencialidad, integridad y disponibilidad de la red. Por lo general, la evaluación de vulnerabilidad comienza con una fase de reconocimiento, durante la cual se recopilan datos importantes sobre los sistemas y recursos de destino. Esta fase conduce a la fase de preparación del sistema, donde el objetivo se verifica esencialmente para todas las vulnerabilidades conocidas. La fase de preparación culmina en la fase de presentación de informes, donde los resultados se clasifican en categorías de crítico, alto, mediano y bajo riesgo; y los métodos para mejorar la seguridad (o mitigar el riesgo de vulnerabilidad) del objetivo se discuten.

Exploit

Un exploit es un software ilegal que se aprovecha de las vulnerabilidades de las aplicaciones, las redes o el hardware. Tienen como objetivo obtener el control de un sistema o robar datos guardados en una red.

Gray Box

El siguiente paso de la prueba de caja negra es la prueba de caja gris. Mientras que un pentester de caja negra está examinando un sistema desde la perspectiva externa de la red, un pentester de caja gris tiene los niveles de acceso y conocimiento de un usuario, posiblemente con privilegios elevados en un sistema. Los pentesters de caja gris generalmente tienen algún conocimiento de los aspectos internos de una red, lo que incluye potencialmente la documentación de diseño y arquitectura y una cuenta interna de la red.

El propósito de pentesting de caja gris es proporcionar una evaluación más enfocada y eficiente de la seguridad de una red que una evaluación de caja negra. Al usar la documentación de diseño para una red, los pentesters pueden enfocar sus esfuerzos de evaluación en los sistemas con el mayor riesgo y valor desde el principio, en lugar de dedicar tiempo a determinar esta información por su cuenta. Una cuenta interna en el sistema también permite probar la seguridad dentro del perímetro y simula a un atacante con acceso a la red a largo plazo.

IIS

Por sus siglas en inglés: Internet Information Services. Este servicio convierte una PC en un servidor web para Internet o una intranet, es decir que en los equipos que tienen este servicio instalado se pueden publicar páginas web tanto local como remotamente.

LAN

Por sus siglas en inglés: Local Area Network. Es la red interna de una organización.

Malware

Malware hace referencia a cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los hackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo.

Pruebas de penetración (Pentest)

La prueba de penetración es el proceso de intentar obtener acceso a recursos sin conocimiento de nombres de usuario, contraseñas y otros medios de acceso normales. Si está enfocado en los recursos de la computadora, entonces ejemplos de una penetración exitosa sería obtener documentos confidenciales, listas de precios, bases de datos y otra información protegida.

Lo principal que separa a un pentester de un atacante es el permiso. El pentester, tendrá permiso del propietario de la organización para realizar las pruebas y será responsable de proporcionar un informe. El objetivo de una prueba de penetración es aumentar la seguridad de la organización.
La diferencia entre evaluaciones de vulnerabilidad y pruebas de penetración es que una evaluación de vulnerabilidad es el primer paso para una prueba de penetración. La información obtenida de la evaluación se usa para las pruebas. Mientras que la evaluación se lleva a cabo para detectar agujeros y vulnerabilidades potenciales, las pruebas de penetración realmente intentan explotar los hallazgos.

En muchos casos, el pentester tendrá acceso a nivel de usuario y en esos casos, el objetivo sería elevar los privilegios de la cuenta para obtener acceso a información adicional que un usuario de ese nivel no tendría acceso normalmente.

Puerto
Un puerto de red es una interfaz para comunicarse con un programa a través de una red. Existen 65536 (del 0 al 65535). Aunque podemos usar cualquiera de ellos para cualquier protocolo, existe una entidad, la IANA, encargada de su asignación, la cual creó tres categorías:

Puertos bien conocidos

Los puertos inferiores al 1024 son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos" como por ejemplo HTTP (servidor Web), POP3/SMTP (servidor de e-mail) y Telnet. Si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.

Puertos registrados

Los comprendidos entre 1024 y 49151, son denominados "registrados" y pueden ser usados por cualquier aplicación. Existe una lista pública en la web del IANA donde se puede ver qué protocolo usa cada uno de ellos.

Puertos dinámicos o privados

Los comprendidos entre los números 49152 y 65535 son denominados dinámicos o privados, normalmente se asignan en forma dinámica a las aplicaciones de clientes al iniciarse la conexión. Se usan en conexiones peer to peer (P2P).

Sandbox

Sandbox protege los datos, las distribuciones de código fuente revisadas y otras colecciones de código, datos y contenidos en los equipos y servidores de cambios que podrían ser perjudiciales o de archivos maliciosos que pudieran contener virus o malware. Los Sandbox, replican al menos la funcionalidad mínima necesaria para probar con precisión los programas u otros códigos en desarrollo, por ejemplo, el uso de las mismas variables de entorno o el acceso a una base de datos idéntica a la utilizada por la implementación anterior estable que se desea modificar; muchas otras posibilidades, ya que las necesidades de funcionalidad específica varían ampliamente con la naturaleza del código y las aplicaciones para las que está destinado.

Todos los programas que se ejecutan dentro de un sandbox lo hacen de forma controlada mediante los siguientes aspectos:

- Se les asigna un espacio en disco. Estos programas no podrán acceder a ningún espacio del disco que no les haya sido asignado previamente.
- Podemos hacer que nuestros programas se ejecuten en un sistema de archivos temporal para aislarlos del resto del sistema operativo.
- También se les asigna un espacio en memoria. Los programas no podrán acceder a otras localidades de memoria que no les hayan sido asignadas.

- Se les puede dar o restringir la capacidad para acceder y consultar dispositivos de almacenamiento externos.
- Se restringe la capacidad para que puedan inspeccionar la máquina anfitriona.
- Se puede restringir el acceso de los programas a la red
- Podemos limitar el ancho de banda que usa un determinado programa.

Vulnerabilidades de día cero (zero day vulnerabilities)

Cuando un proveedor de software saca al mercado un nuevo producto con alguna brecha de seguridad de la que no son conscientes ni el proveedor ni la empresa antivirus, se denomina vulnerabilidad de día cero o exploit de día cero.

White Box

Las pruebas de caja blanca tienen varios nombres diferentes, incluyendo pruebas de caja clara, caja abierta, auxiliar y lógica. Cae en el extremo opuesto del espectro de las pruebas de caja negra ya que los pentesters tienen acceso completo al código fuente, documentación de arquitectura, etc. El principal desafío con las pruebas de caja blanca es analizar la enorme cantidad de datos disponibles para identificar los puntos potenciales de debilidad, lo que la convierte en el tipo de prueba de penetración que más tiempo consume.

A diferencia de las pruebas de caja negra y caja gris, los pentesters de caja blanca pueden realizar análisis de código estático, por lo que la familiaridad con los analizadores de código fuente, depuradores y herramientas similares son importantes para este tipo de pruebas. Sin embargo, las herramientas y técnicas de análisis dinámico también son importantes para los pentesters, ya que el análisis estático puede pasar por alto las vulnerabilidades introducidas por la mala configuración de los sistemas de destino.

Las pruebas de penetración de caja blanca proporcionan una evaluación integral de las vulnerabilidades internas y externas, lo que la convierte en la mejor opción para las pruebas de cálculo de riesgos. La estrecha relación entre los pentesters de caja blanca y los desarrolladores proporciona un alto nivel de conocimiento del sistema, pero puede sesgar los comportamientos del pentester, ya que operan con base en el conocimiento no disponible para los hackers.

Whitelisting

La lista blanca de aplicaciones es la lógica negada de la lista negra: se elabora una lista de entidades aceptables (aplicaciones de software, direcciones de correo electrónico, usuarios, procesos, dispositivos, etc.) que tienen acceso permitido a un sistema o red, y bloquea todo lo demás. Se basa en un principio de "confianza cero" que esencialmente niega todo y permite solo lo necesario.

Las técnicas de listas blancas más simples utilizadas para los sistemas y las redes identifican las aplicaciones según su nombre de archivo, tamaño y rutas de directorio. Pero el Instituto Nacional de Estándares y Tecnología de EE. UU. O NIST, una división del Departamento de Comercio, recomienda un enfoque más estricto, con una combinación de técnicas criptográficas de hash y firmas digitales vinculadas al fabricante o desarrollador de cada componente o pieza de software.

En el nivel de red, la compilación de una lista blanca comienza por construir una vista detallada de todas las tareas que los usuarios necesitan realizar, y las aplicaciones o procesos que necesitan para realizarlas. La lista blanca puede incluir infraestructura de red, sitios y ubicaciones, todas las aplicaciones válidas, usuarios autorizados, socios de confianza, contratistas, servicios y puertos.

La lista blanca para aplicaciones de nivel de usuario podría incluir correo electrónico (filtrado de correo no deseado y contactos no aprobados), programas y archivos, y organizaciones comerciales o no comerciales aprobadas y registradas con proveedores de servicios de Internet (ISP).

En todos los casos, las listas blancas deben mantenerse actualizadas, y los administradores deben considerar tanto la actividad del usuario (por ejemplo, qué aplicaciones tienen permiso para instalar o ejecutar) como los privilegios del usuario (es decir, asegurarse de que no se otorga a los usuarios una información inadecuada).

Existen servicios de lista blanca de terceros que a veces son empleados por empresas que buscan aliviar la carga de gestión asociada con el proceso. Estos servicios a menudo se basan en la reputación y utilizan tecnología para otorgar calificaciones a los procesos de software y red según su antigüedad, firmas digitales y tasa de ocurrencia.

ANEXOS

A) Carbon Black Protection

Es un producto de control de aplicaciones que se utiliza para bloquear ejecuciones en servidores y sistemas críticos, evitar cambios no deseados y garantizar el cumplimiento continuo de las regulaciones de seguridad. Aprovechando los servicios de reputación en la nube, las políticas de confianza basadas en TI y las múltiples fuentes de inteligencia de amenazas de Cb Predictive Security Cloud (PSC), Cb Protection garantiza que solo el software confiable y aprobado pueda ejecutarse en los sistemas y endpoints críticos de una organización.

Cb Protection combina el whitelisting, la supervisión de la integridad de archivos, el control de dispositivos con todas las funciones y la protección de memoria / sabotaje en un único agente. Observa los indicadores de comportamiento de actividad maliciosa y realiza un registro continuo de los detalles del ataque para proporcionar una vasta visibilidad de todo lo que los atacantes intentan hacer.

Para realizar la instalación de Carbon Black se ocupó un Windows Server 2012 R2 donde se instaló el agente de la consola, SQL Enterprise, 64Gb de memoria RAM y para propósitos de pruebas, 1Tb de disco duro. Adicionalmente se otorgó acceso en el firewall a los puertos requeridos. Esta consola es vital para el funcionamiento de Carbon Black ya que es de donde se actualizarán sus firmas de reconocimiento de amenazas y también donde se mantendrá la base de datos de todos los eventos y alertas que se registren durante el uso de Carbon Black.

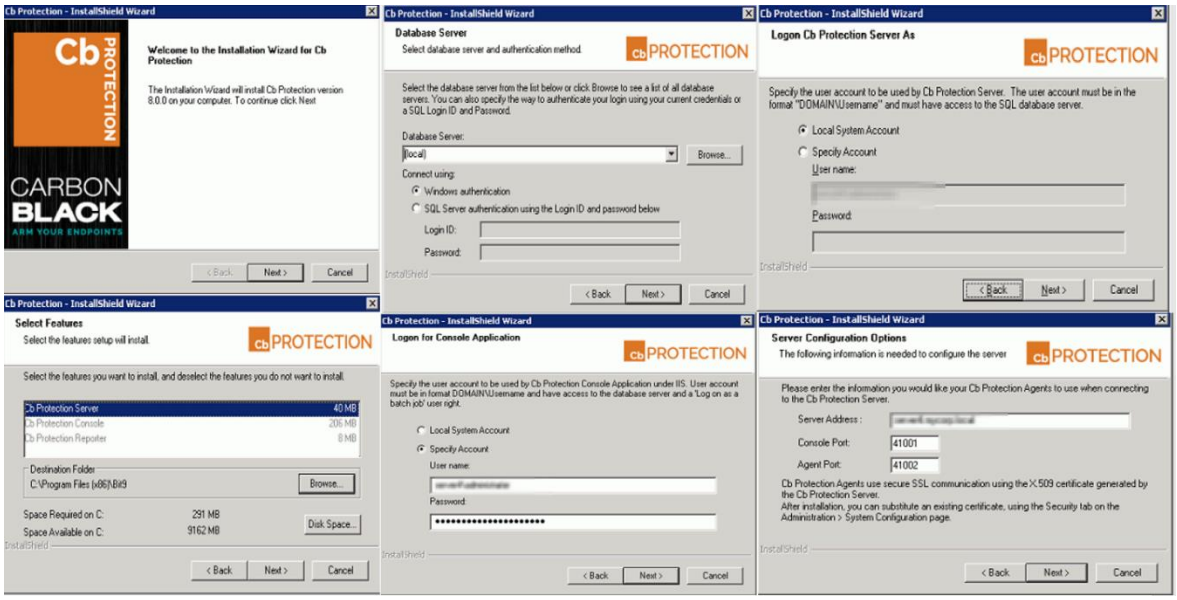


Figura 13. Proceso de instalación de Carbon Black

Una vez instalada la consola, se puede acceder a ella por medio de un navegador donde la interfaz de inicio de sesión es la siguiente:

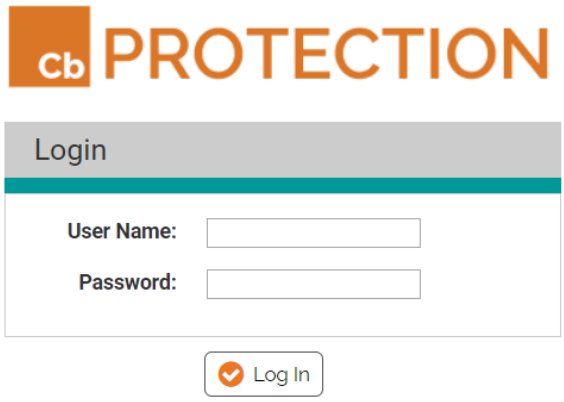


Figura 14. Inicio de sesión web CB Protection

Una vez dentro de la consola de Carbon Black, en la pantalla principal podemos apreciar lo siguiente:

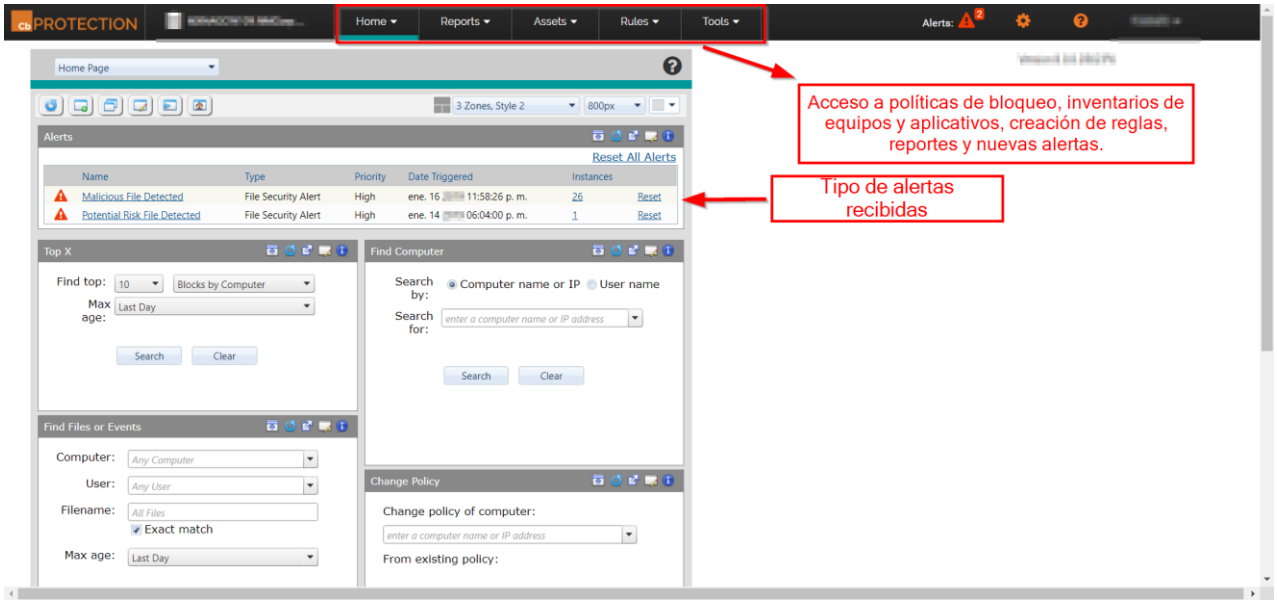


Figura 15. Página principal de Carbon Black

Dentro de CB, podemos crear nuevas políticas de bloqueo que se ajusten a los requerimientos de cada área o usuario, bloquear ejecuciones no deseadas, crear reglas para evitar recibir alertas de falsos positivos, aprobar o banear de manera global o local e incluso eliminar de manera remota un archivo en caso que éste sea malicioso.

B) Kali

Es un sistema operativo basado en Linux el cual está dedicado a la seguridad de la información. Cuenta con diversas herramientas para detección, prevención y explotación de vulnerabilidades, auditorías de sistemas, así como para pruebas de penetración (Pentest).

En mi caso, utilizo Kali en una máquina virtual ya que por el tipo de escaneos de seguridad que se realizan, es necesario que se hagan en un ambiente controlado. En la página de Kali uno puede descargar el Sistema Operativo en diferentes tipos de archivos, es decir, como tipo .iso para instalarlo desde cero, Kali Linux VMware o Vbox para instalarlo dentro de un ambiente controlado como es mi caso. Este tipo de archivos son una imagen creada por los desarrolladores la cual ya viene pre-configurada y lo único que se debe realizar es importarla al virtualizador:

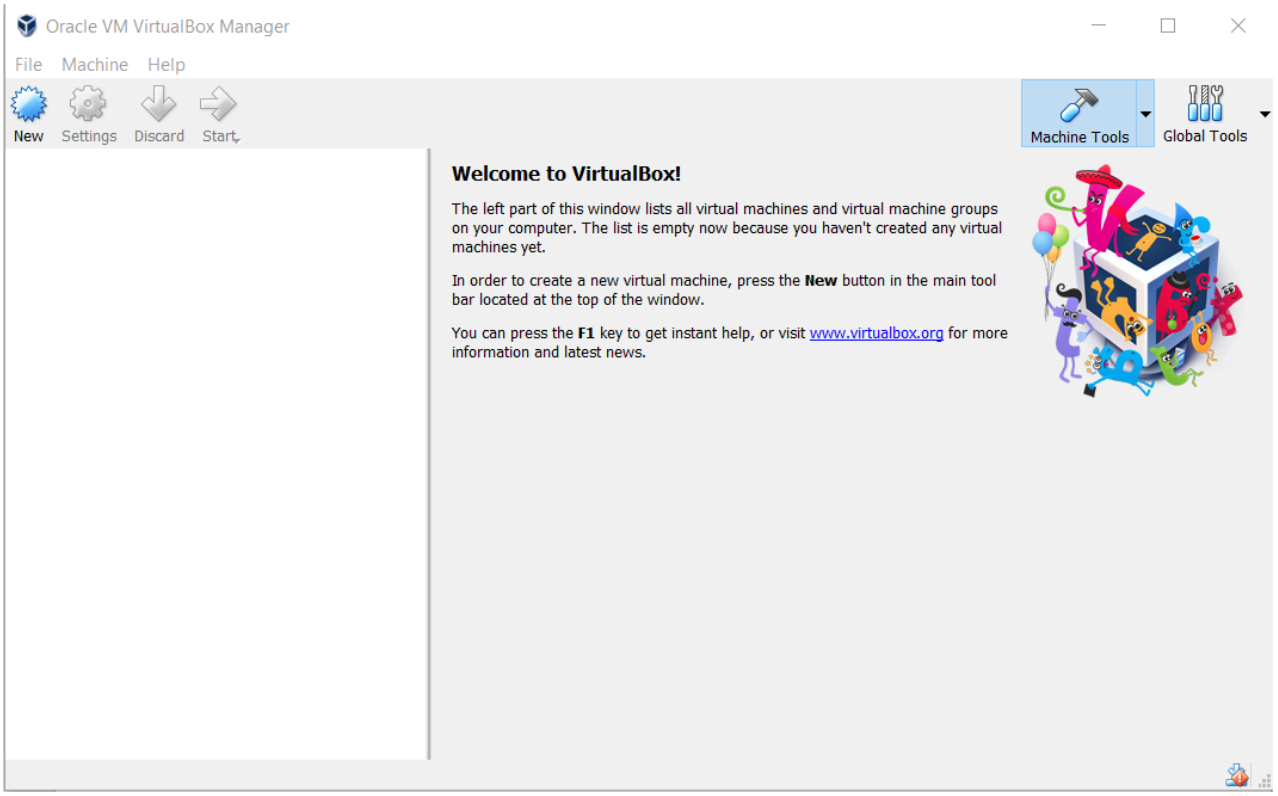


Figura 16. Interfaz Virtual Box

Para importar la imagen de Kali a Virtual Box es necesario seguir los siguientes pasos:

1) Click en File y en Import Appliance:

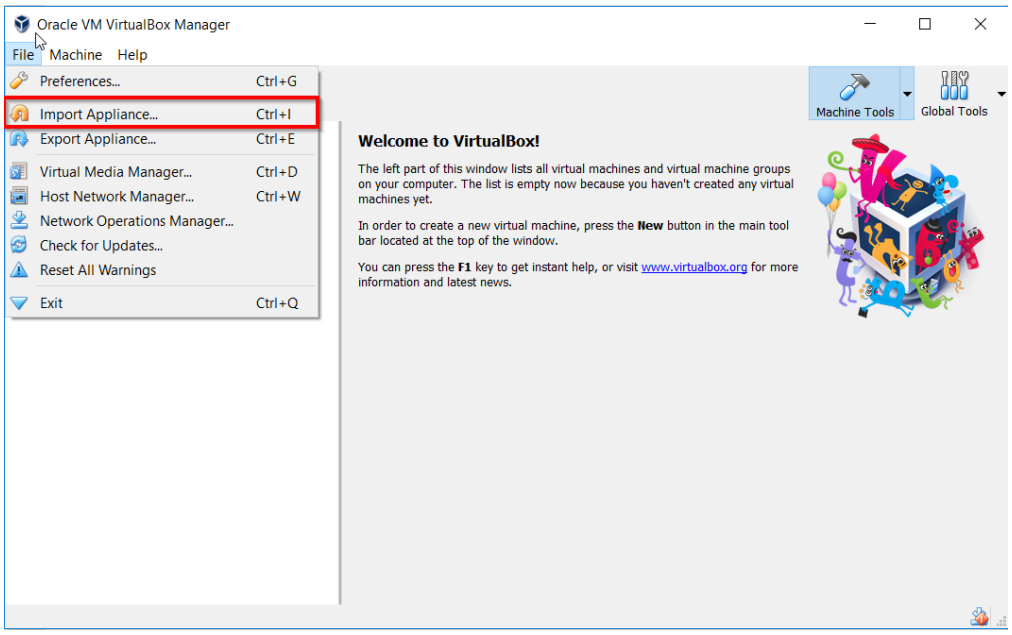


Figura 17. Import Appliance en menú File

2) Seleccionar la imagen previamente descargada del sitio de Kali:

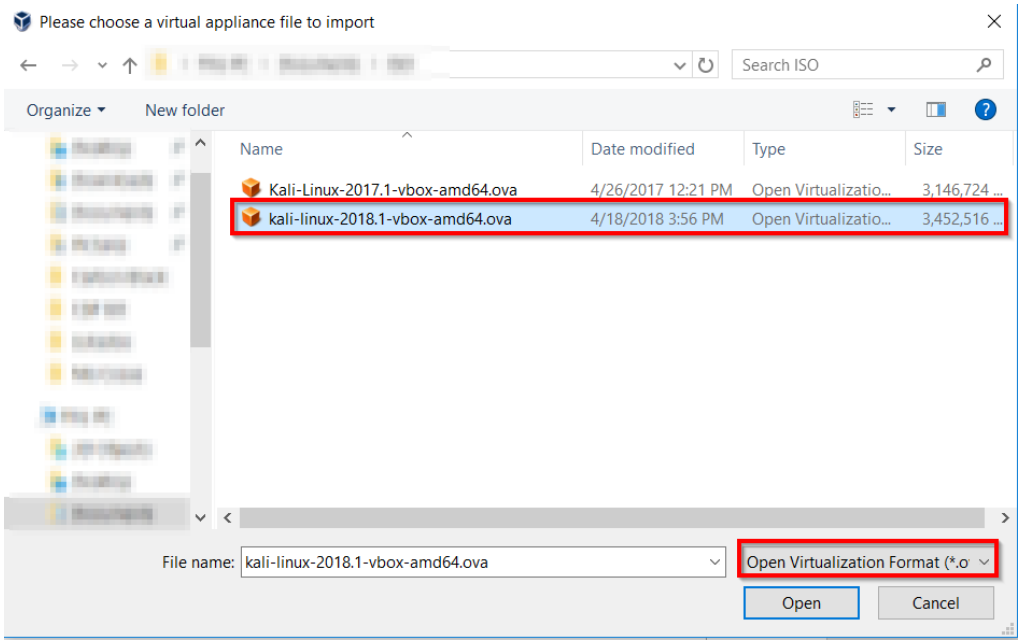


Figura 18. Selección de imagen de Kali

3) Cuando se importa la imagen a Virtual Box, aparecerá la siguiente ventana donde podemos apreciar la configuración por default que trae Kali. Esta configuración puede ser modificada por ejemplo en la RAM utilizada, nombre, controladores y adaptador de red.

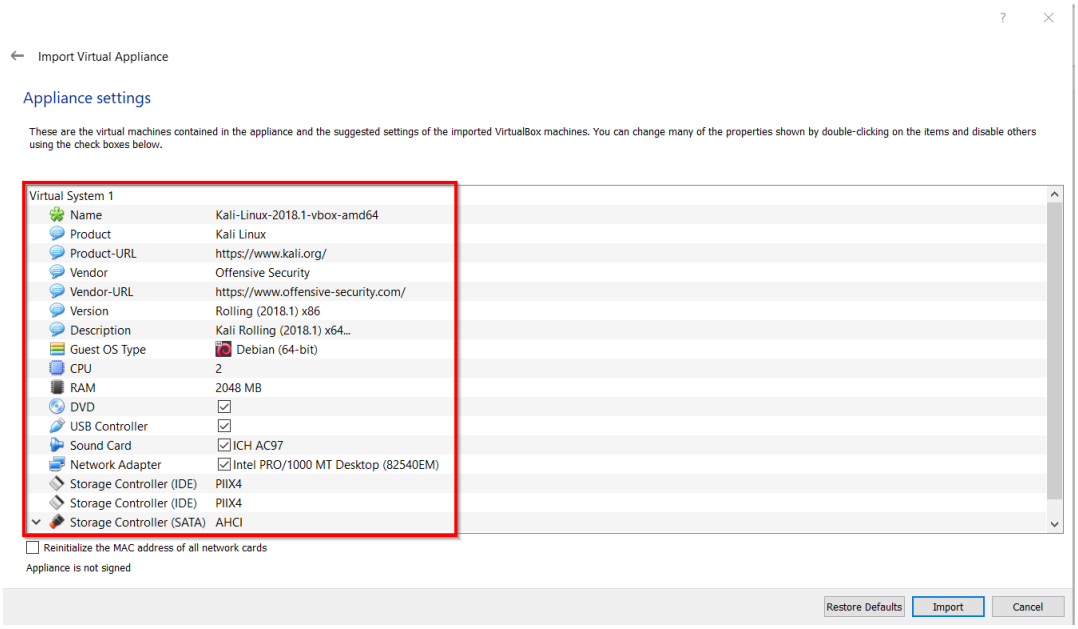


Figura 19. Características de imagen de Kali

Una vez que concluye el proceso de importación de la imagen virtual de Kali, ésta aparecerá en el menú principal de Virtual Box.

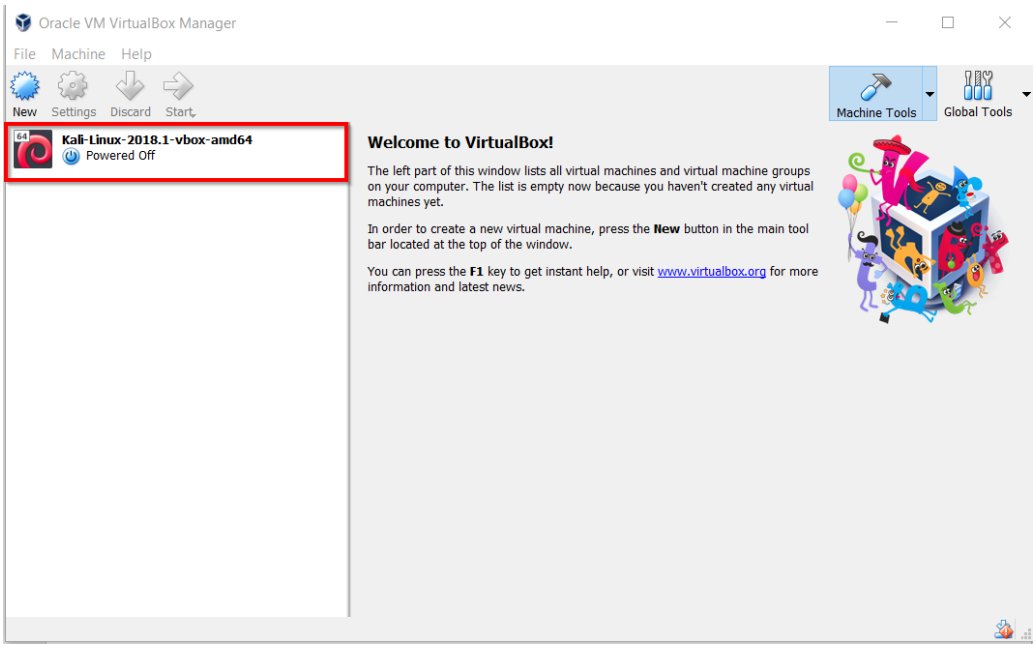


Figura 20. Menú principal con Kali ya instalado

Para iniciar sesión en Kali se debe ingresar las credenciales por default

- **User:** root
- **Password:** toor

Figura 21. Pantalla de inicio de sesión de Kali

La interfaz de Kali se encuentra distribuida de la siguiente manera:

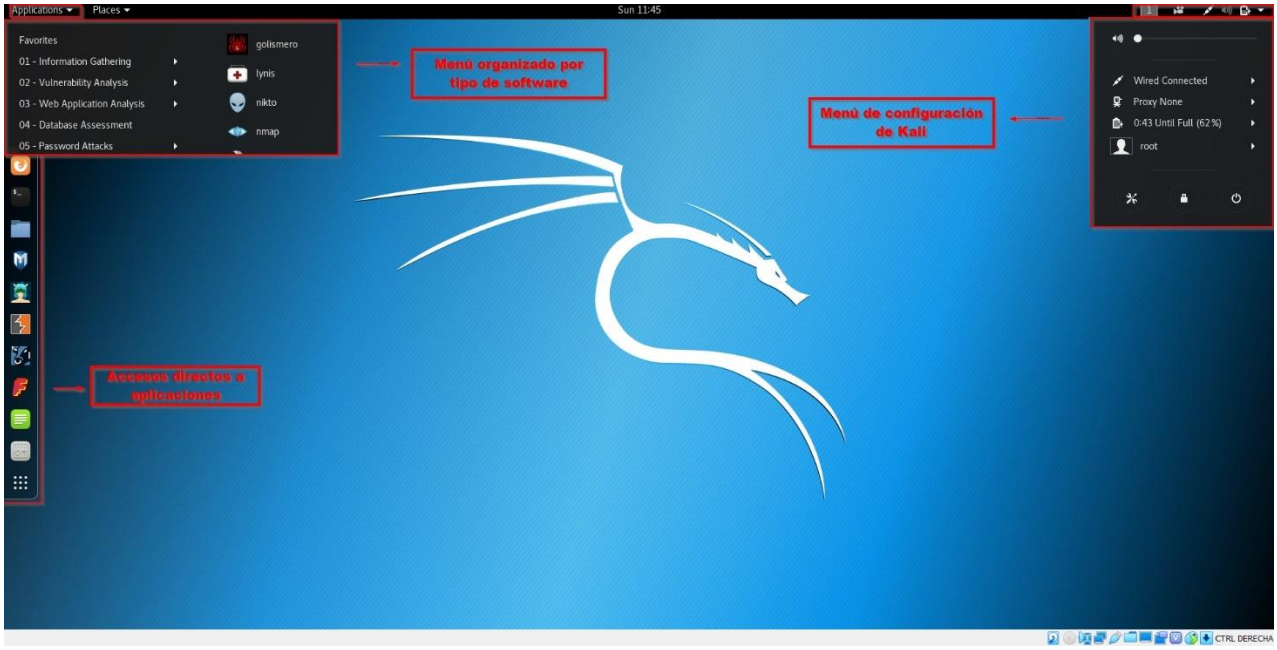


Figura 22. Pantalla principal de Kali

C) Metasploit

Es una herramienta que viene precargada en Kali la cual permite cargar diferentes exploits para aprovechas las vulnerabilidades. Normalmente es utilizado para hackear, sin embargo, yo lo utilicé para la detección de equipos vulnerables a Wannacry, escanenado los diferentes segmentos de la red utilizando el exploit the EternalBlue, el cual se aprovecha de las vulnerabilidades de SMB v1 y permite la ejecución de código remoto. De esta manera logré identificar más equipos en la red que eran vulnerables para prevenir su infección y aplicarles el parche necesario.

Existen distintas maneras para acceder a Metasploit, en este caso detallaré cómo acceder por terminal y directo desde el menú de aplicaciones.

1) Abres la terminal

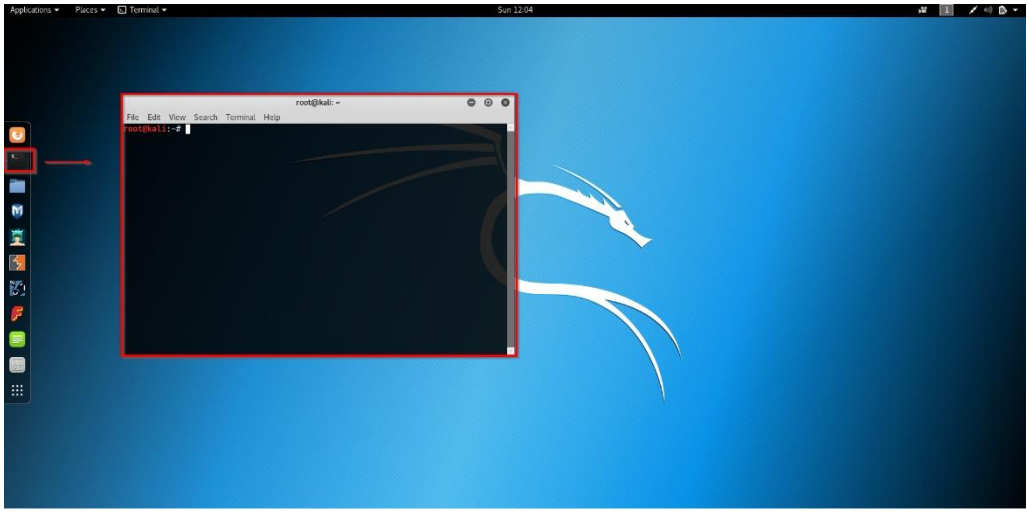
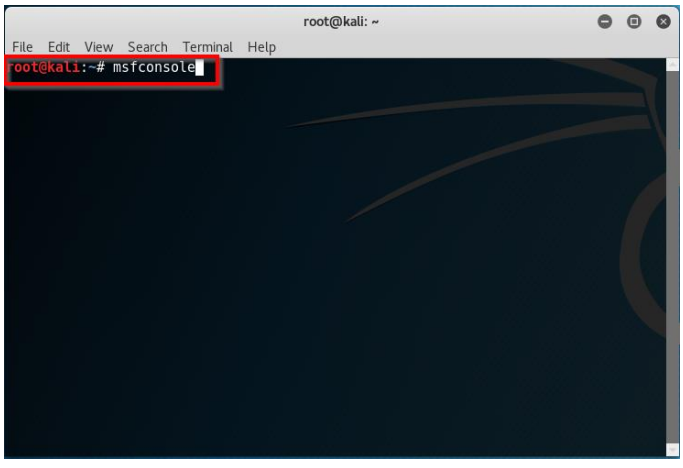


Figura 23. Terminal de Kali

2) En la terminal, escribes msfconsole



3) Presionas enter y se cargará la interfaz de Metasploit desde la cual uno ya puede comenzar a trabajar:

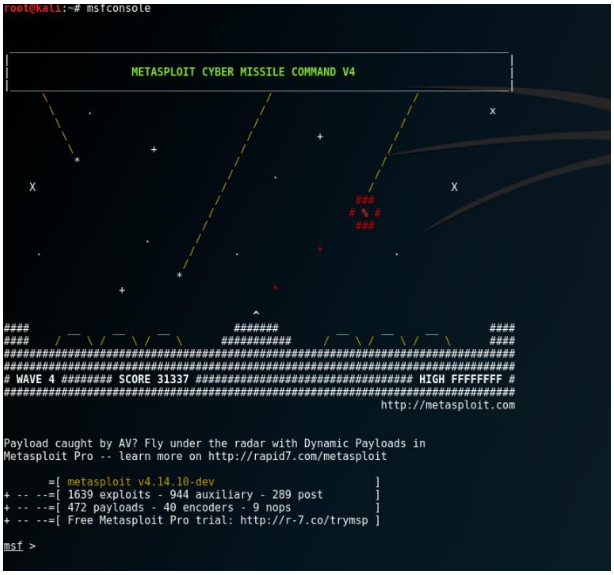


Figura 24. Interfaz de Metasploit

Ahora para acceder desde el menú de aplicaciones, es necesario:

1) Abrir el menú en la categoría “Exploitation tools” y de lado derecho estará Metasploit:

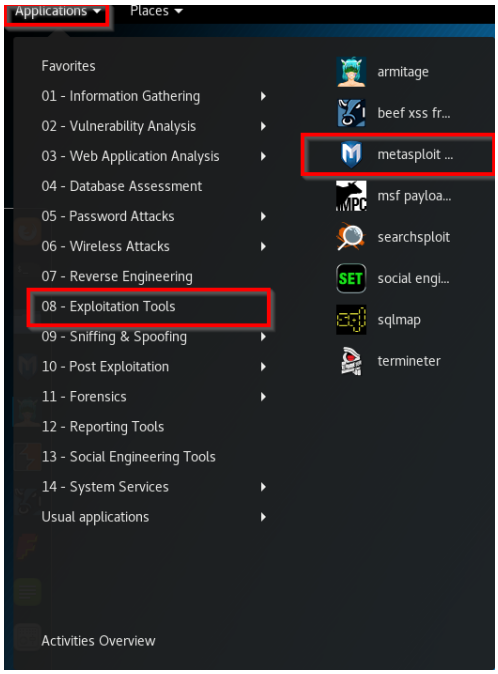


Figura 25. Apertura de Metasploit mediante el menú de aplicaciones

D) Nessus

Es la solución de evaluación más implementada de la industria para identificar las vulnerabilidades, problemas de configuración y malware que utilizan los atacantes para penetrar la red. Con la cobertura más amplia, la última inteligencia, las actualizaciones rápidas y una interfaz fácil de usar, Nessus ofrece un paquete de exploración de vulnerabilidades eficaz e integral.

Esta herramienta es de gran importancia en mi trabajo diario ya que me permite mantener un nivel alto de seguridad en la organización y así prevenir el impacto ante alguna nueva amenaza como un ransomware.

La ventana de inicio de sesión para Nessus Professional se ve de la siguiente manera:

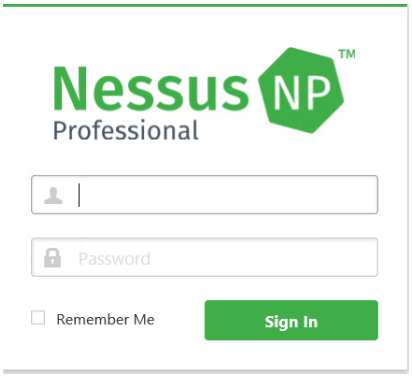


Figura 26. Pantalla de inicio de sesión de Nessus Professional

En Nessus uno puede crear diferentes tipos de escaneos de acuerdo al requerimiento. La siguiente imagen es la plantilla de los tipos de escaneos disponibles en Nessus:

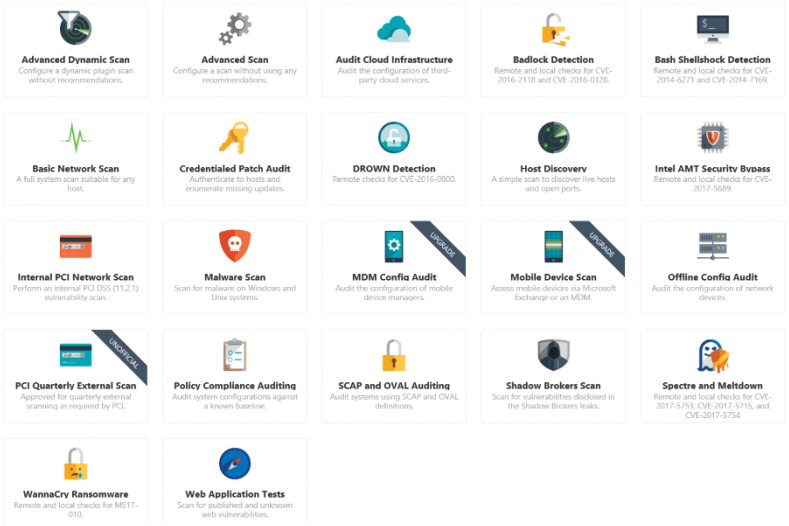


Figura 27. Plantilla de escaneos disponibles en Nessus

Para crear un escaneo en Nessus:

1) Seleccionar un tipo de escaneo de la plantilla previamente mostrada.
2) Elegir un nombre, descripción, carpeta destino y objetivos del escaneo los cuales pueden ser páginas web, IPs y segmentos por máscara o incluso subir un archivo con los objetivos:

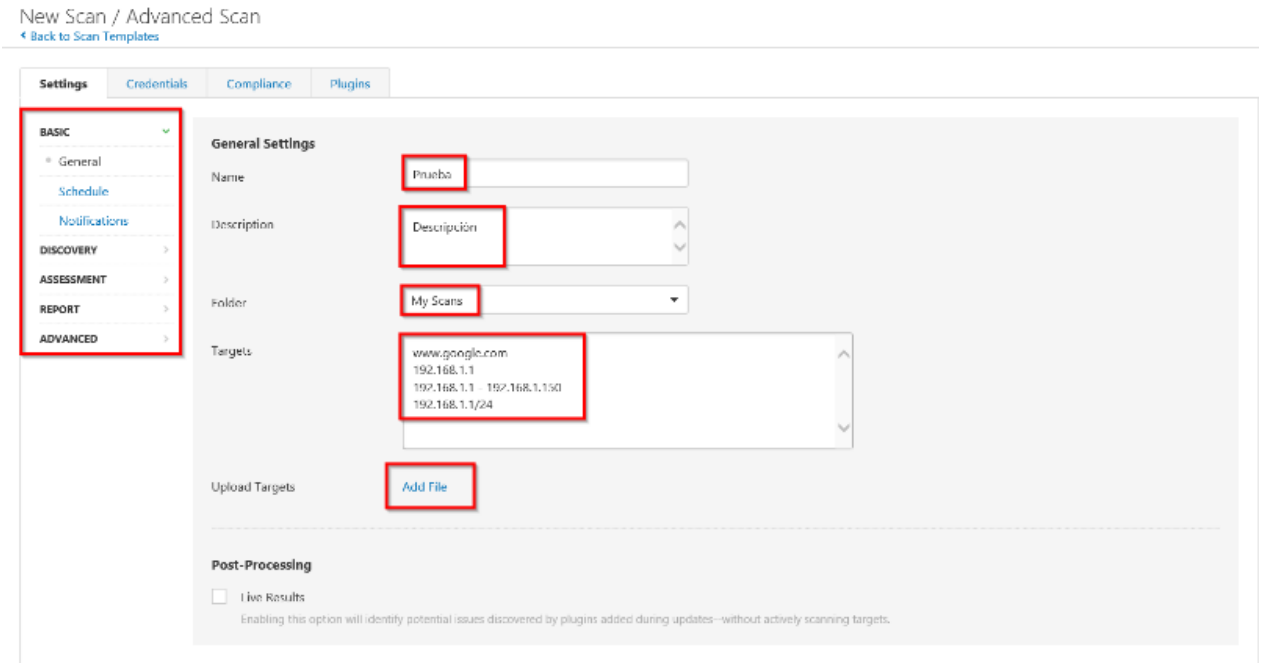


Figura 28. Configuración de escaneo

3) En la misma ventana anterior, se puede configurar el tiempo, intentos para alcanzar un host, envío de resultados a correo electrónico y programar los escaneos.
4) Posteriormente es necesario configurar los plugins que se utilizarán para escanear y proporcionar las credenciales. Una vez seleccionadas, le das click en “Save” y corres el escaneo.

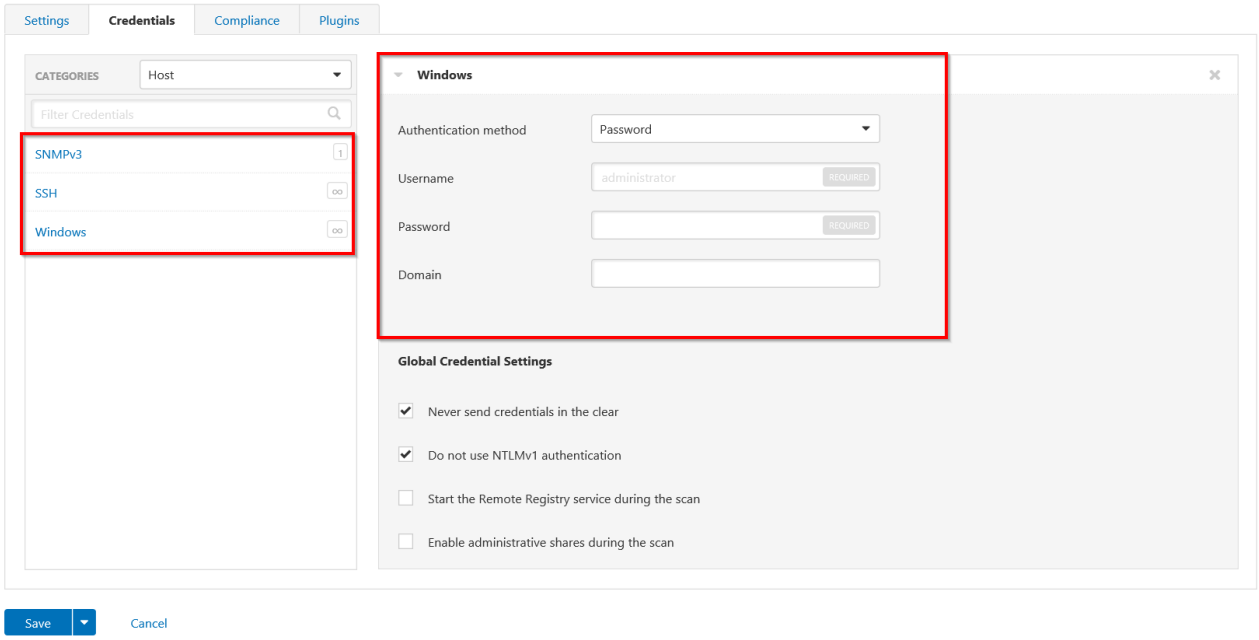


Figura 29. Configuración de Credenciales

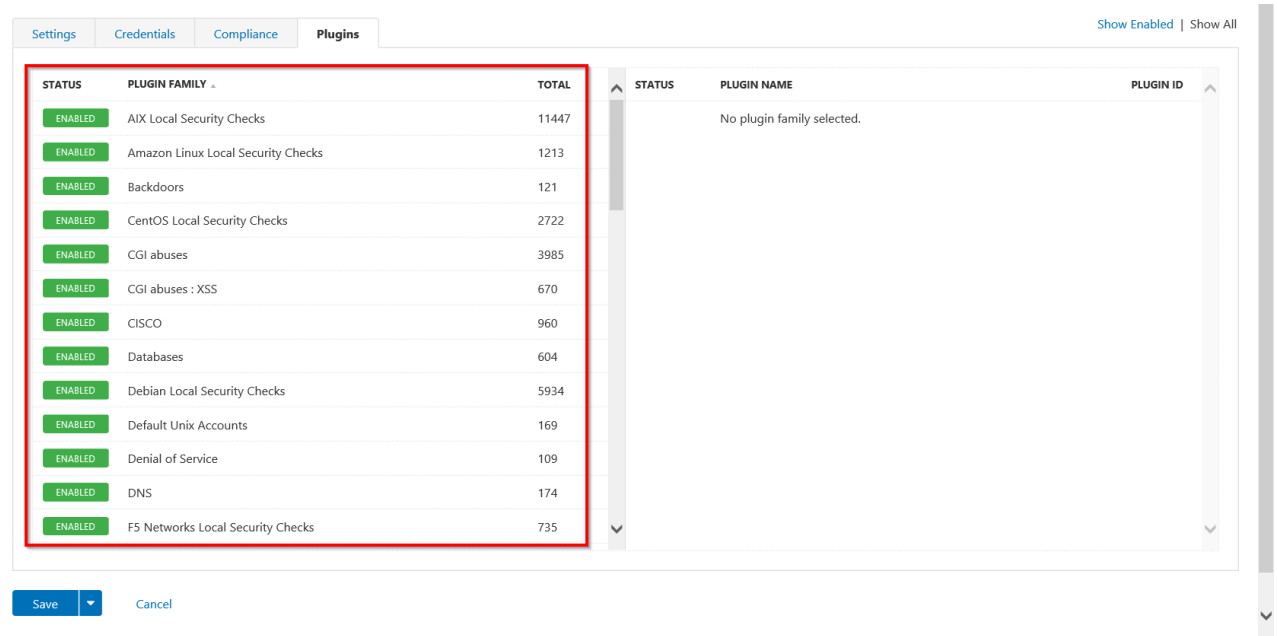


Figura 30. Selección de plugins para escaneo

E) NMAP

Es una utilidad de código abierto y gratuito para detección de redes y auditoría de seguridad. Muchos sistemas y administradores de red también lo encuentran útil para tareas tales como inventario de red, administración de programaciones de actualización de servicio y monitoreo de tiempo de actividad de host o servicio. Nmap utiliza paquetes IP sin procesar de maneras novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen esos hosts, qué sistemas operativos (y versiones del sistema operativo) están ejecutando, qué tipo de filtros de paquetes / firewalls están en uso, y docenas de otras características.

Fue diseñado para escanear rápidamente redes grandes, pero funciona bien contra hosts únicos. Nmap se ejecuta en todos los principales sistemas operativos de la computadora, y los paquetes binarios oficiales están disponibles para Linux, Windows y Mac OS X. Además del ejecutable clásico de la línea de comandos Nmap, la suite Nmap incluye una GUI avanzada y un visor de resultados (Zenmap). una herramienta flexible de transferencia de datos, redirección y depuración (Ncat), una utilidad para comparar resultados de escaneo (Ndiff) y una herramienta de análisis de generación y respuesta de paquetes (Nping).

La siguiente captura de pantalla es un ejemplo de un escaneo con NMAP para reconocer: sistema operativo, puertos y protocolos abiertos, etc.

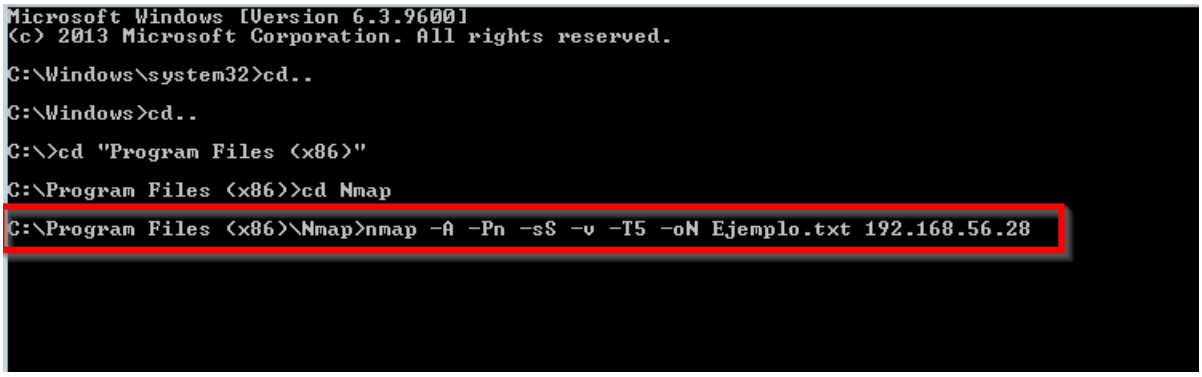


Figura 31. Escaneo con NMAP

-A: Habilita la detección de sistema operativo, versión y traceroute.
-Pn: Trata a todos los hosts como activos, evitando el descubrimiento de hosts.
-Ss: Verificación de triple – hand – shake.
-V: Incrementa los detalles obtenidos.
-T5: Incrementa el tiempo de escaneo de acuerdo al número después de T.
-oN: Exporta los resultados obtenidos al documento de texto especificado después, si no existe el archivo, lo crea y exporta los resultados.

REFERENCIAS

Sean Wilkins. (2012). TCP/IP Ports and Protocols. 30/05/2010, de Pearson Certification Sitio web: http://www.pearsonitcertification.com/articles/article.aspx?p=1868080

Maria Korolov, Lysa Myers. (2017). What is the cyber kill chain? Why it's not always the right approach to cyber attacks. 07/11/2017, de CSO Sitio web: https://www.csoonline.com/article/2134037/cyber-attacks-espionage/strategic-planning-erm-the-practicality-of-the-cyber-kill-chain-approach-to-security.html

Jreport. (NA). 3-Tier Architecture: A Complete Overview. 2018, de JReport Sitio web: https://www.jinfonet.com/resources/bi-defined/3-tier-architecture-complete-overview/

Tenable. (2018). Plugins Tenable. 2018, de Tenable Inc. Sitio web: https://www.tenable.com/plugins

Exploits DB. (2018). NA. 2018, de Exploits DB Sitio web: https://www.exploit-db.com/

The Nmap Project. (1996). NMAP. 2018, de The Nmap Project Sitio web: https://nmap.org/

Carbon Black. (2018). Carbon Black Datasheet. 2018, de Carbon Black Sitio web: https://www.carbonblack.com/resource/cb-protection-datasheet/?cn-reloaded=1

SANS Institute. (2006). Penetration Testing: Assessing Your Overall Security Before Attackers Do. 2018, de SANS Institute Sitio web: https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Jahoda M., Gkioka I., Krátký R., Prpič M., Čapek T., Wadeley S., Ruseva Y. & Svoboda M.. (2014). 1.3. Vulnerability Assessment. En A Guide to Securing Red Hat Enterprise Linux 7(pp.1-30). Estados Unidos: Red Hat, Inc.. Sitio web: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/index

Howard Poston. (2018). What are Black Box, Grey Box, and White Box Penetration Testing?. 30/07/2018, de INFOSEC Institute Sitio web: https://resources.infosecinstitute.com/what-are-black-box-grey-box-and-white-box-penetration-testing/#gref

Microsoft. (2011). Default groups. 17/11/2018, de Microsoft Sitio web: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756898(v=ws.10)

Bradley Mitchell. (2018). The Layers of the OSI Model Illustrated. 17/11/2018, de Lifewire Sitio web: https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017