CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM & REDTEAM

SANTOS CAMARGO GUZMÁN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM & REDTEAM

SANTOS CAMARGO GUZMÁN

TUTOR
M.Sc. JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
NEIVA
2021

TABLA DE CONTENIDO

LISTADO DE TABLAS

Pág.

LISTADO DE FIGURAS

Pág.

RESUMEN

En el siguiente documento se presentan todos los aspectos relevantes de cada escenario de análisis del seminario de seguridad de TI, lo que permite entender cómo se trabaja en los equipos RedTeam y BlueTeam. Para el primer escenario se realiza el montaje de un banco de trabajo con las siguientes maquinas (Windows 7 y Kali Linux) para desarrollar las próximas actividades, el segundo escenario, es el análisis de un contrato proporcionado por Whitehouse Security para observar si existen en fragmentos ilegales, el tercer escenario consiste en analizar la información de fuga en uno de los equipos que tiene instalado el software Rejetto, para que se tenga un contexto claro de la información y vulnerabilidades de la aplicación. En el último escenario estudia un ataque en tiempo real, las posibles formas para contener el mismo, las medidas de hardenización que pueden ser implementadas para evitar que los ataques se repitan, finalmente, definir CIS (Centro para la seguridad Interite), SIEM y posibles herramientas utilizadas.

Palabras calves: Vulnerabilidad, herramientas, ataques informáticos, sistemas, técnicas, seguridad, amenazas, riesgos, delitos, debilidades, OWASP, aplicaciones web.

GLOSARIO

AMENAZA: cualquier acción que aproveche una vulnerabilidad para realizar un ataque a los sistemas de información.

ATAQUE INFORMÁTICO: Implica aprovechar una vulnerabilidad del sistema o una falla para causar daños o fallas en la información.

BLUE TEAM: es el equipo de seguridad proactivo que protege a la organización de los ataques.

CIBERAMENAZA: Es una operación destinada a violar la seguridad sistema de información cambiando la disponibilidad, seguridad o la seguridad del sistema o la información que contiene.

CIBERCRIMINAL: Él es quien explota las debilidades de redes y sistemas de información para realizar las labores que estipula la ley tales como crimen: robo de información, destrucción de información, extorsión, divulgación Información confidencial, difusión de pornografía infantil, correo spam, terrorismo, fraude, robo de identidad, fraude de información, violación de derechos de propiedad.

CIBERRIESGO: Son aquellos que, como su nombre lo indica, funcionan mientras están en uso ciencias de la computación.

COPNIA: es el consejo de ingeniería, cuya función es inspeccionar, vigilar y control el ejercicio profesional de los ingenieros y profesiones afines.

CVE: Son identificadores asignados a una vulnerabilidad común en los sistemas informáticos, permiten esfuerzos colectivos entre organizaciones para abordar y mejorar dichas vulnerabilidades.

DATO: Constituye el elemento básico de los tres elementos que deben protegerse, ya que es el más importante amenazado y sin duda el más difícil de recuperar.

EXPLOITDB: consiste es una base de datos donde se encuentran las vulnerabilidades, para saber como explotarlas y sacar provecho de cada una.

FIREWALL: es un programa que identifica y bloquea los intentos de intrusión en las redes informáticas.

METASPLOIT: es un proyecto de seguridad informática de código abierto que proporciona información sobre vulnerabilidades de seguridad y admite el "pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

RED TEAM (Seguridad Ofensiva): Este es un grupo de empleados a tiempo completo en una empresa enfocada en penetrar la infraestructura, las plataformas, los inquilinos y las aplicaciones de los clientes. Son enemigos leales (un grupo de piratas informáticos éticos) que toman acciones deliberadas y persistentes para atacar.

RIESGO: es la capacidad de estar expuesto a amenazas que se pueden presentar en un activo de TI a una persona u organización.

SEGURIDAD: esta es una característica que tiene cualquier sistema o computadora. Donde se indique que el sistema está libre de cualquier peligro, daño o riesgo y de alguna manera confiable.

VULNERABILIDAD: es debilidad o falla en el sistema de información que amenazan la seguridad de la información, puede permitir que un atacante comprometa la integridad y la usabilidad, o su secreto, por lo que es necesario encontrarlo y eliminarlo tan pronto como sea posible. Estas "vulnerabilidades" pueden tener diferentes orígenes, por ejemplo: Un error de diseño, error de configuración o deficiencia del proceso.

INTRODUCCIÓN

Actualmente el activo más importante para la empresas es la información razón por la cual es importante conocer las diferentes leyes que se utilizan en Colombia con relación delitos informáticos que se puedan presentar como son el robo de datos personales, suplantación de sitios web entre otros delitos.

Dado que los diferentes sistemas operativos son cada vez más vulnerables, el objetivo de este trabajo es aprender a detectar y prevenir un ataque a una máquina virtual por parte de un atacante en Linux, lo que simplificará la investigación sin cambiar la infraestructura corporativa, confirmar las vulnerabilidades que pueden ser encontrado e investigue el exploit con un framework Trabaje o explote e identifique el objeto de hackear un archivo específico.

Adicionalmente es necesario conocer las vulnerabilidades que afectan el correcto funcionamiento de los sistemas de información y las herramientas para solucionar las mismas.

OBJETIVOS

OBJETIVO GENERAL

Analizar el funcionamiento de los equipos de trabajo RedTeam y BlueTeam en una organización a través de los diferentes escenarios realizados en desarrollo del seminario.

OBJETIVOS ESPECÍFICOS

- Conocer la legislación de Colombia en los delitos informáticos.
- Identificar las fases de las pruebas de penetración.
- Analizar las principales herramientas para detectar vulnerabilidades.
- Identificar las faltas en las que se pueden incurrir al cometer acciones delictivas .
- Conocer la postura como profesional ante estos procesos ilegales.
- Conocer las medidas de hardenización.
- Identificar las diferencias entre equipo Blueteam y un equipo de respuesta a incidentes informáticos
- Analizar las herramientas para contener ataques

CONCEPTO EQUIPOS DE SEGURIDAD

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

La Ley 1273 de 2009, por medio de la cual se realiza una adición al código penal con relación a la protección de la información y los datos en los sistemas que utilicen las tecnologías de la información y las comunicaciones, [1] en sus 10 artículos desde el 269A al 269J en donde se regula los delitos informáticos que se pueden presentar en Colombia.

Tabla 1 Legislación de los delitos informáticos

Artículos	Descripción
Artículo 269A: Acceso abusivo a un sistema informático.	Incluye el acceso no autorizado a sistemas de información protegidos o desprotegidos.
Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación	Consiste en obstaculizar el funcionamiento normal de los sistemas de información.
Artículo 269C: Interceptación de datos informáticos	Es la apropiación de información privada de un sistema de información sin ninguna autorización legal.
Artículo 269D: Daño Informático	Consiste en realizar daño a los sistemas de información mediante la alteración, borrado y modificación de la información.
Artículo 269E: Uso de software malicioso	Es realización de software con el fin de apropiarse de maneja ilegal de la información, como son los programas de virus.
Artículo 269F: Violación de datos personales	Es la utilización de datos personales de terceros para realizar acciones delictivas.
Artículo 269G: Suplantación de sitios web para capturar datos personales.	Es la creación de paginas web falsas para obtener informaciones de los usuarios.

[1] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273. Bogotá. (Enero 05 de 2005). Diario Oficial 47.223 de enero 05 de 2005. p. 1-6.

Artículos	Descripción
Artículo 269G: Modificación del sistema de resolución de nombres de dominio	Consiste en la modificación de la IP con fin de obtener información personal de los usuarios.
Artículo 269H: Circunstancias de agravación punitiva	Se aumenta la pena de tres cuartas partes si se comete dentro de las siguientes conductas. • Ataques sistemas oficiales y el sector financiero. • Funcionario publico en cumplimiento de sus funciones. • Aprovechar la confianza del depositario de la información. • Divulgar la información de un tercero. • Sacar provecho para sí mismo del tercero. • Con fines terroristas. • Utilización de buena fe.
Artículo 269I: Hurto por medios informáticos y semejantes	Incluye el robo de datos a través del acceso no autorizado a los sistemas de información.
Artículo 269J: Transferencia no consentida de activos.	Es la transferencia de activos a terceros sin ninguna autorización.

Fuente Propiedad del Autor

Ley Estatutaria 1266

"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".[2]

Ley 1341 de 2009

"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones".[3]

Ley 1480 de 2011

[2] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.
[3] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341. Bogotá. (Julio 30 de 2009). Diario Oficial 47.227 de diciembre 31 de 2008. p. 1-30.

“Protege al consumidor que realiza transacciones y movimientos por medios electrónicos, estableciendo criterios que permitan garantizar la seguridad del usuario y de la plataforma de servicios”. [4]

Ley Estatutaria 1581 de 2012

“Por la cual se dictan disposiciones generales para la protección de datos personales” [5]

Ley 1928 de 2018

“Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.” [6]

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Pruebas de penetración: Se realiza la representación de una clase de ataque malicioso *outsiders* (que no está autorizado a acceder a los sistemas de la empresa) y de malicioso *insiders* (que cuentan con algún nivel de acceso autorizado). Se lleva a cabo el análisis activo del sistema para encontrar las vulnerabilidades que podrían resultar de configuración deficiente o inadecuada del sistema.

Figura 1 El Proceso para Pruebas de Penetración

Fuente El Proceso para Pruebas de Penetración». [En línea] [Consultado 29 Agosto de 2021] disponible (http://www.reydes.com/d/?q=El_Proceso_para_Pruebas_de_Penetracion)

[4] COLOMBIA, CONGRESO DE LA REPÚBLICA Ley 1480 de 2011. [ONLINE]. Bogotá. (Octubre 12 2011). Diario Oficial 48.220 de octubre de 12 de 2011. p. 1-11.
[5] COLOMBIA, CONGRESO DE LA REPÚBLICA Ley 1581 de 2012. [ONLINE]. Bogotá. (Octubre 18 2012). Diario Oficial No. 48.587 de 18 de octubre de 2012. p. 1-188
[6] COLOMBIA, CONGRESO DE LA REPÚBLICA Ley 1928 de 2018. [ONLINE]. Bogotá. (Julio 24 2018). Diario Oficial No. 50.664 de 24 de julio de 2018 de 24 de julio de 2018. p. 1-15

A continuación una breve de explicación de cada fase:

- Captura de información: Incluye obtener tanta información de la empresa como sea posible a través de arañas y escáneres para comprender los sistemas y programas que se están ejecutando. Las actividades de los empleados en la red social de la empresa también pueden revelar los sistemas y correos electrónicos que utilizan. Toda esta información te es útil. Para esta fase se puede utilizar la siguiente herramienta FOCA (análisis de metadatos) la cual permite recolectar toda la información necesaria para esta fase.

- Modelamiento de amenazas: en este momento, en base a la información recopilada previamente, se debe considerar que la estrategia de penetración se puede convertir en un atacante. ¿Cuál debería ser el objetivo? ¿De qué manera se debe lograr? Lo que se piensa que era la puerta de entrada se convierte en un callejón sin salida. Al final, se sigue en un camino diferente e inesperado. En cualquier caso, siempre es necesario proponer inicialmente la estrategia primero. Esta fase se puede desarrollar mediante la utilización de diagramas de flujos de datos.

- Análisis de vulnerabilidades: para ello, se debe evaluar el posible éxito de la estrategia de penetración mediante la identificación proactiva de vulnerabilidades. Es entonces cuando se pueden demostrar las habilidades de Pentester, porque su creatividad selecciona de manera decisiva y utiliza correctamente todas las herramientas que tiene a su disposición para lograr los objetivos establecidos en los pasos anteriores. En fase se puede utilizar la herramienta Acunetix se utiliza para verificar y confirmar vulnerabilidades, lo que también coincide con un número muy bajo de falsos positivos.

- Explotación: ahora es el momento de intentar acceder al sistema objetivo de la prueba de penetración, para ello se ejecuta los exploits contra las vulnerabilidades encontradas en la fase anterior, o solo se usará las credenciales obtenidas para acceder al sistema. Se puede utilizar la herramienta Metasploit, para realizar la escaneo de las vulnerabilidades.

- Explotación posterior: desde el momento en que se ingresa al sistema del cliente, se debe comenzar la etapa de demostrar lo que la vulnerabilidad de seguridad puede significar para el cliente. No es lo mismo acceder a una computadora vieja que ni siquiera es parte del dominio que ingresar directamente a un DC. En esta etapa, se trata de lograr los máximos privilegios, información de red y acceso a tantos sistemas como sea posible para determinar los datos y / o servicios que podemos utilizar. Se utiliza la herramienta Nessus, la cual permite realizar escaneos a diferentes programas.

- Reporte: finalmente, se debe presentar los resultados de la auditoría al cliente, para que comprenda la gravedad de los riesgos que traen las vulnerabilidades descubiertas, y enfatice la correcta implementación de la seguridad, los puntos que deben ser corregidos y lo sucedido. Para ambas partes, esta etapa puede ser posible. es lo más importante. Dado que el informe puede ser leído por personal de TI y gerentes sin conocimientos técnicos, se recomienda que el informe se divida en partes de descripción general, y las partes más técnicas divididas en una parte se convertirán en informes ejecutivos e informes técnicos. En esta fase se puede utilizar Kali Linux, la cual posee diferentes herramientas para la generación de reportes.

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

Herramientas:

Metasploit: Herramienta que pose gran cantidad de exploits, los cuales son usados para explotar las vulnerabilidades que se pueden presentar en los sistemas de información, con ella se escoge un objeto de ataque y se comienza hacer uso de los exploits que se utilizan contra el sistema, esta herramienta hace más que solo verifica vulnerabilidades, administrar evaluaciones de seguridad y mejorar la conciencia de seguridad; empodera y arma a los defensores para estar siempre un paso (o dos) por delante del ataque. Tiene una versión de pago y gratuita.

Nmap: Herramienta utilizada para escanear los puertos e indicar cuales se encuentran abiertos y cerrados, mediante la cual se puede realizar auditorías de seguridad e inventario de red, de esta manera planificar la actualización y monitorización de los servicios en tiempo real.

OpenVas: Este es un escáner de vulnerabilidades completo. Sus características incluyen pruebas de validación y no autenticación, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para análisis a gran escala y un potente lenguaje de programación interno para realizar cualquier tipo de prueba de vulnerabilidad. El escáner recopila evidencia de vulnerabilidades de un feed que tiene un largo historial y se actualiza a diario.

Servicios en línea

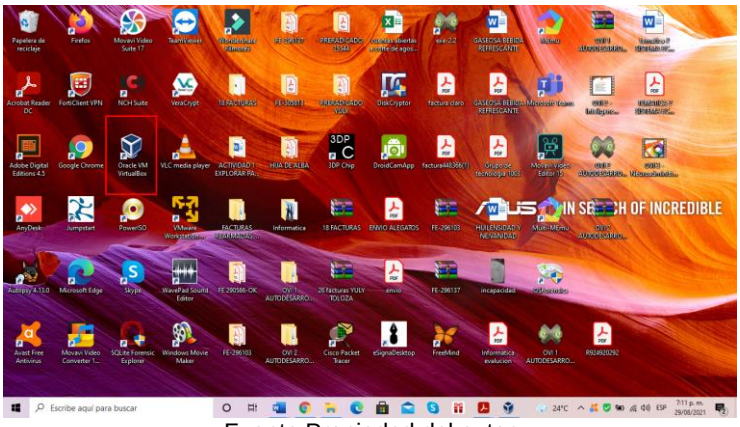
ExploitDB: Consiste en un directorio de exploits donde se pueden encontrar diferentes vulnerabilidades de aplicaciones y como solucionarlas de manera detallada las instrucciones para cada una, constantemente se actualiza esta información.

• CVE: Es una lista de nombres estandarizados para las diferentes vulnerabilidades y exposiciones de seguridad, con el fin de estandarizar los nombres para la vulnerabilidades para que realice búsqueda de la vulnerabilidad y todo la información sobre la misma.

Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

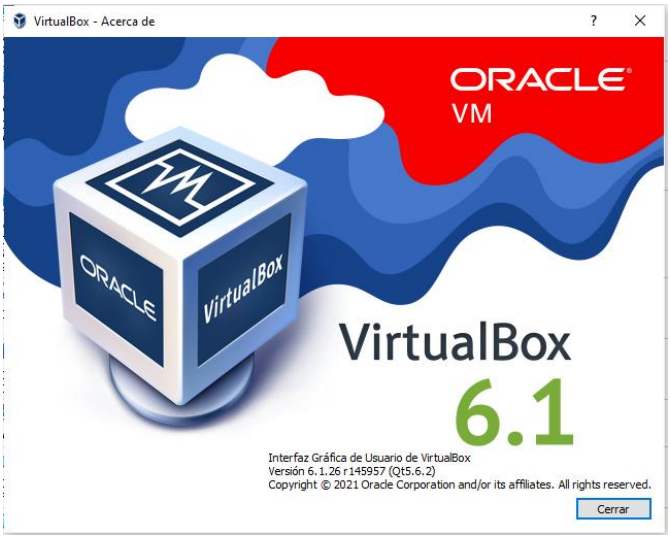
Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Figura 2 Descarga de VirtualBox.



Fuente Propiedad del autor

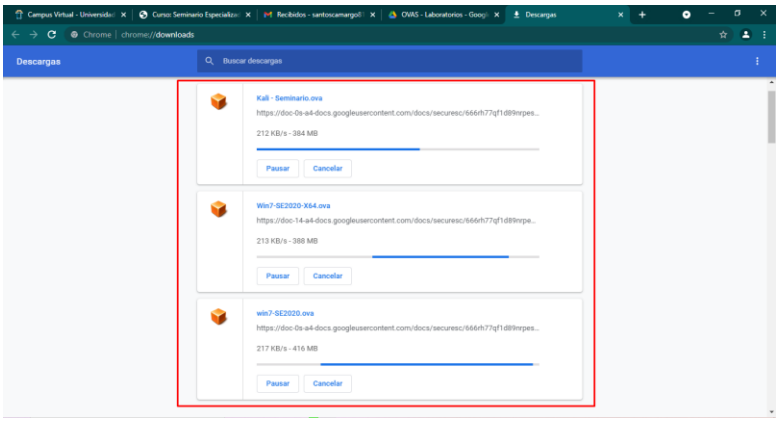
Figura 3 Instalación de la última versión de VirtualBox



Fuente Propiedad del autor

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

Figura 4 Descarga del software

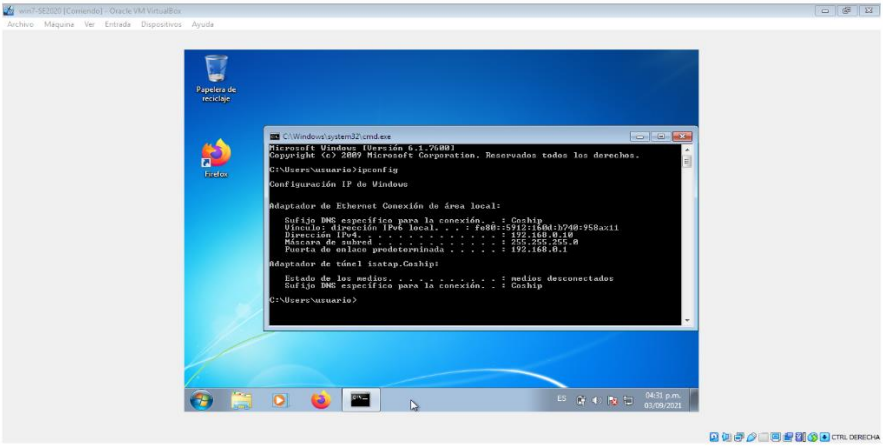


Fuente Propiedad del autor

Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Con el comando ipconfig se conoce la ip asignada para esta máquina. 192.168.0.10

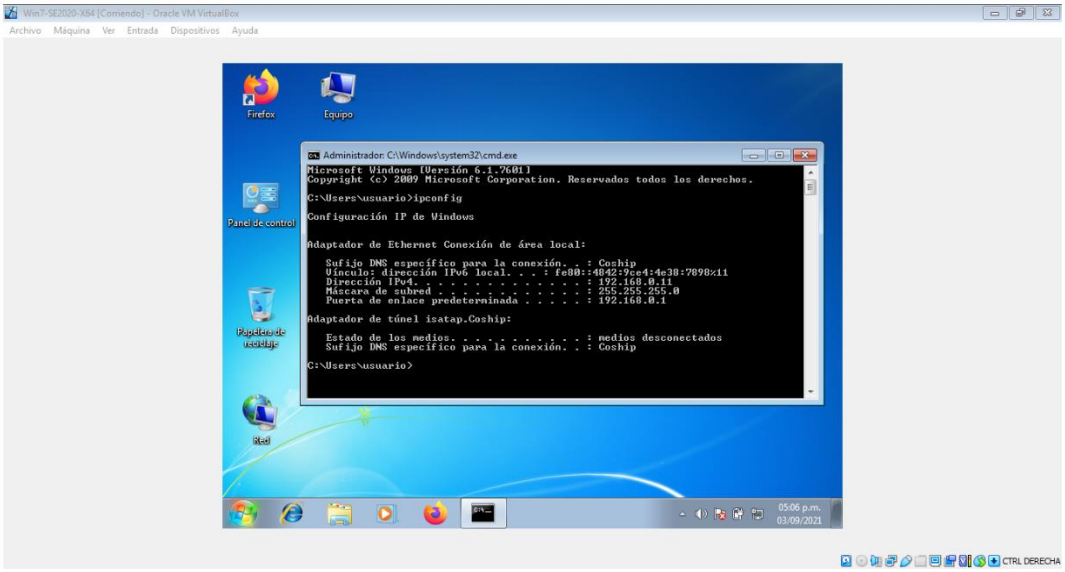
Figura 5 Ip Windows 7 32 Bit



Fuente Propiedad del autor

A continuación se observa la ip asignada a esta máquina que es 192.168.0.11

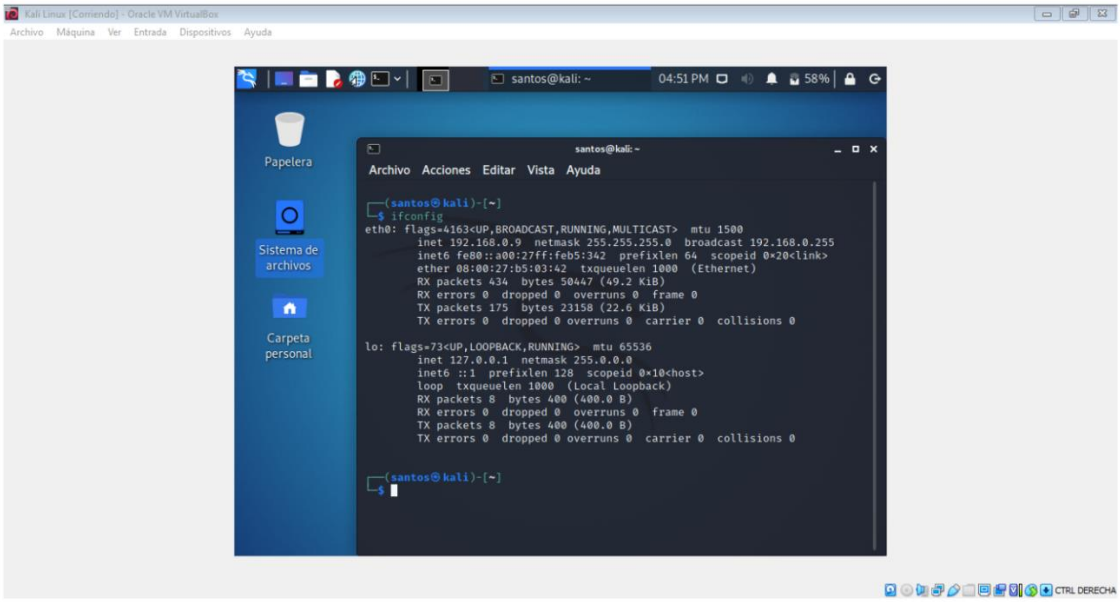
Figura 6 Ip Windows 7 64 Bit



Fuente Propiedad del autor

Para conoce la ip de maquina Kali se utiliza el comanda ifconfig la asignada es 192.168.0.9

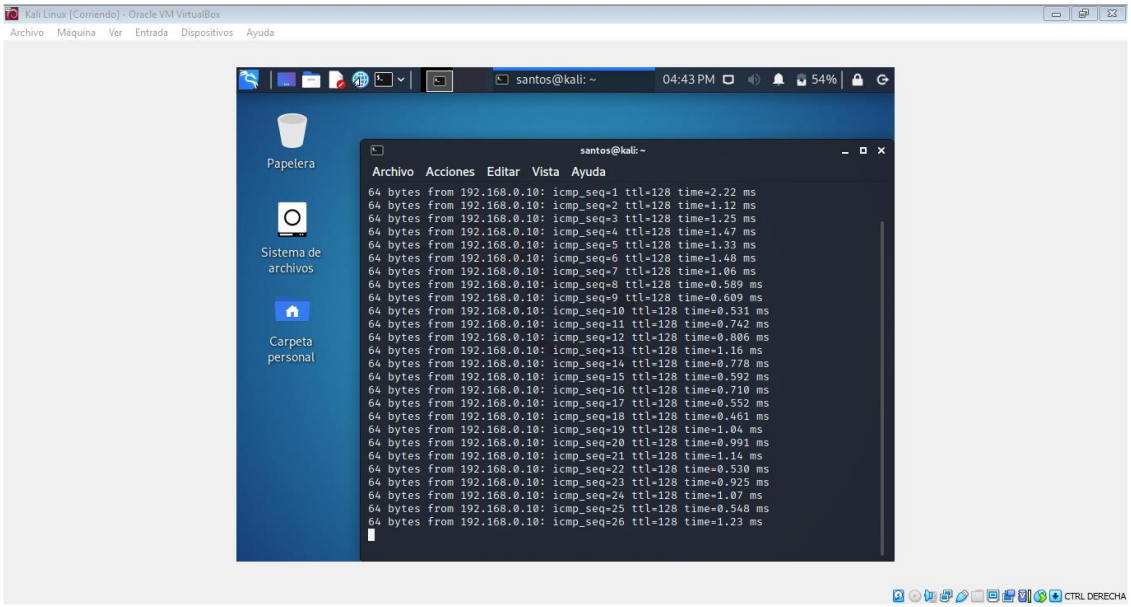
Figura 7 Ip Kali Linux



Fuente Propiedad del autor

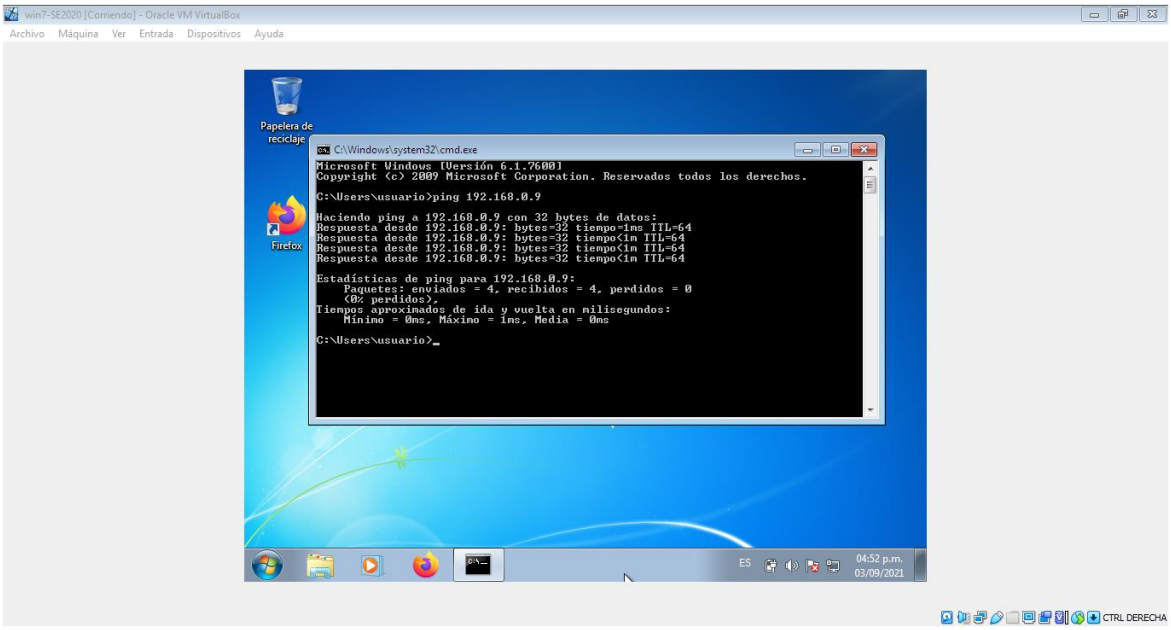
Comunicación entre la máquina de con Kali la maquina con Windows 7 32 bit.

Figura 8 Comunicación Kali Linux con Windows 7 32 Bit



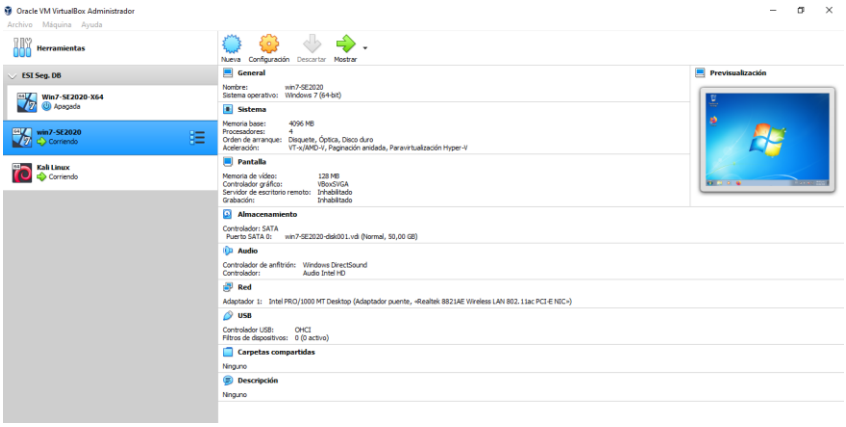
Fuente Propiedad del autor

Figura 9 Comunicación Windows 7 32 Bit con Kali Linux



Fuente Propiedad del autor

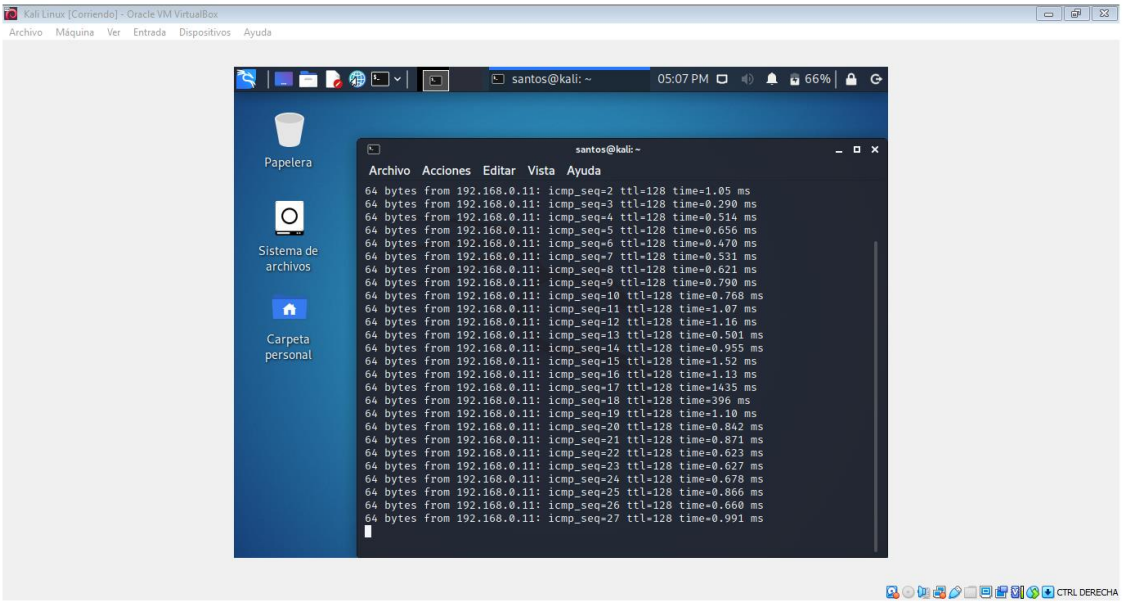
Figura 10 Maquina Windows 7 32 Bit y Kali Linux



Fuente Propiedad del autor

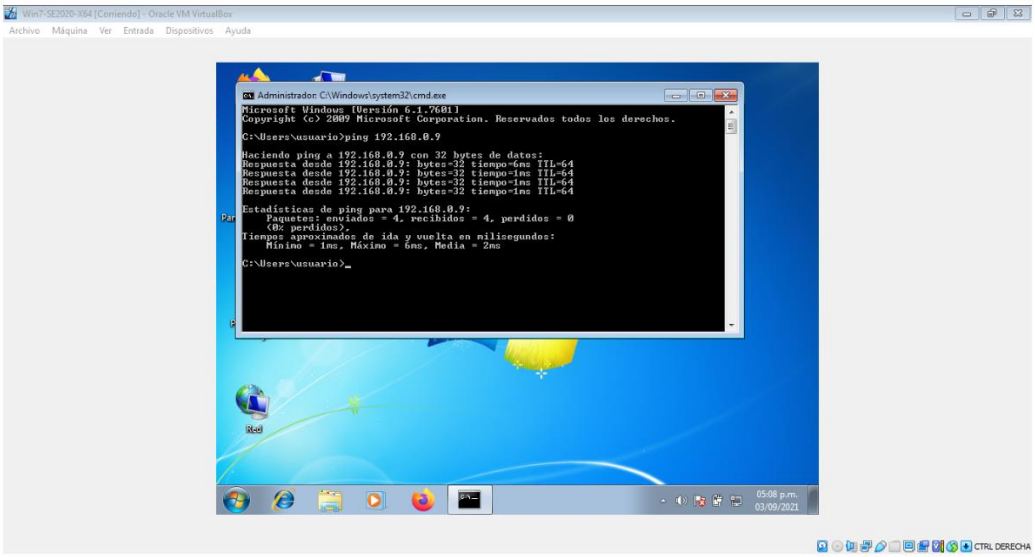
Comunicación entre la máquina de con Kali la maquina con Windows 7 64 bit

Figura 11 Comunicación Kali Linux con Windows 7 64 Bit



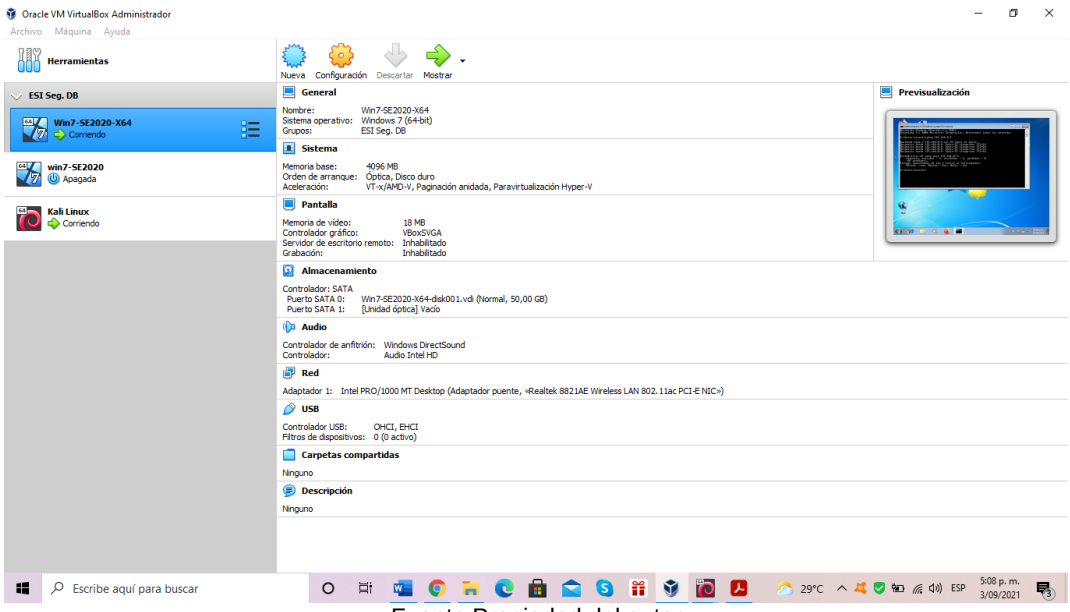
Fuente Propiedad del autor

Figura 12 Comunicación Windows 7 64 Bit con Kali Linux



Fuente Propiedad del autor

Figura 13 Maquina Windows 7 64 Bit y Kali Linux

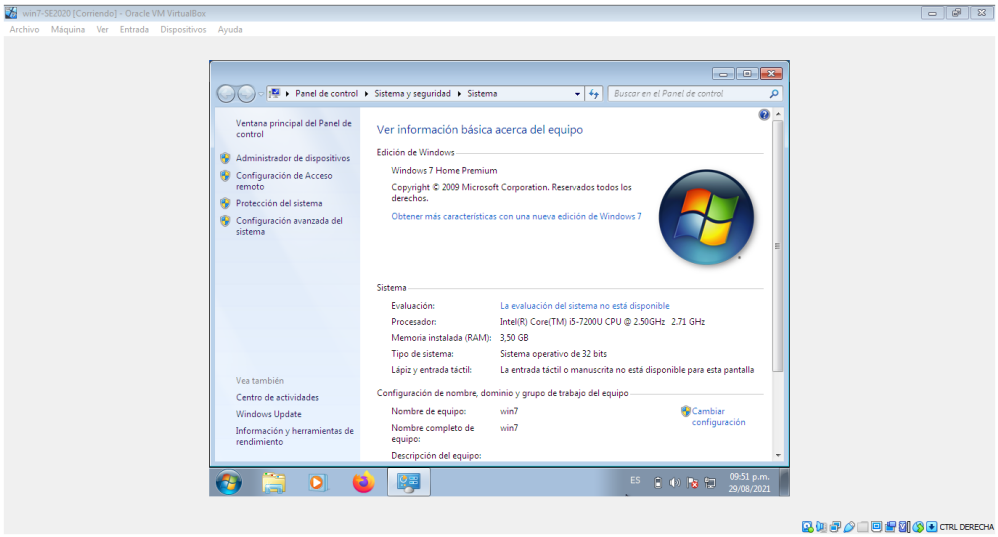


Fuente Propiedad del autor

Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

A continuación se muestra las propiedades de la máquina virtual con Windows 7 de 32 bit, para conocer la características de esa primera máquina.

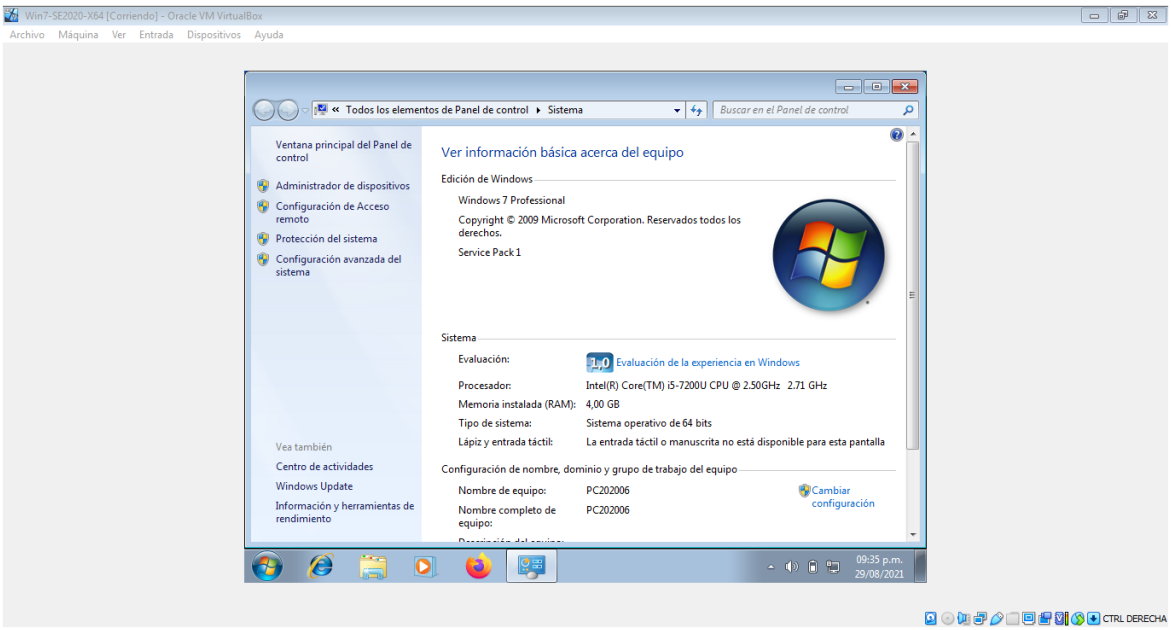
Figura 14 Características Windows 7 32 Bit



Fuente Propiedad del autor

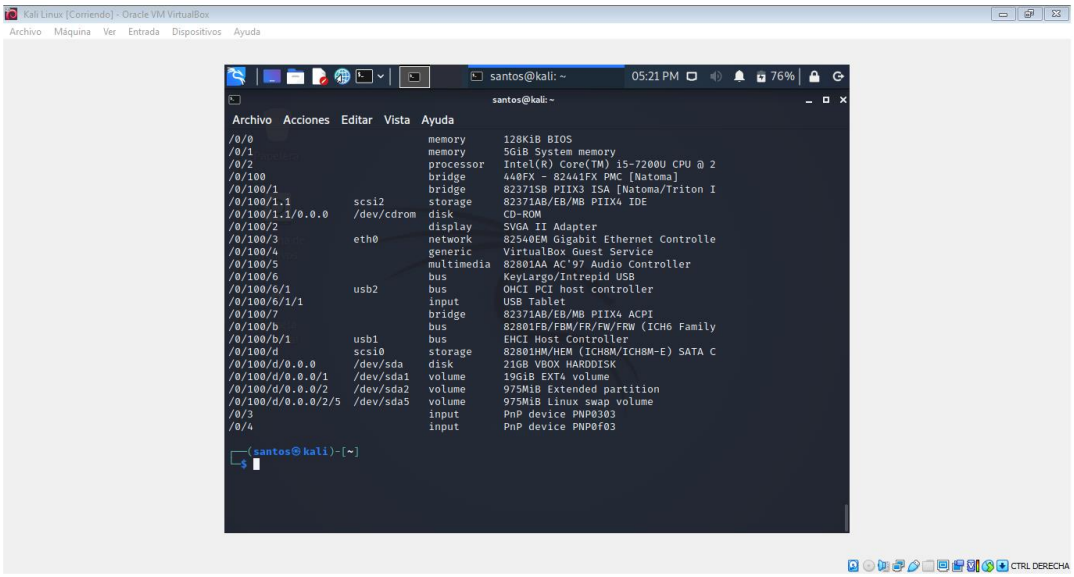
Características segunda máquina virtual Windows 7 64 bit.

Figura 15 Características Windows 7 64 Bit



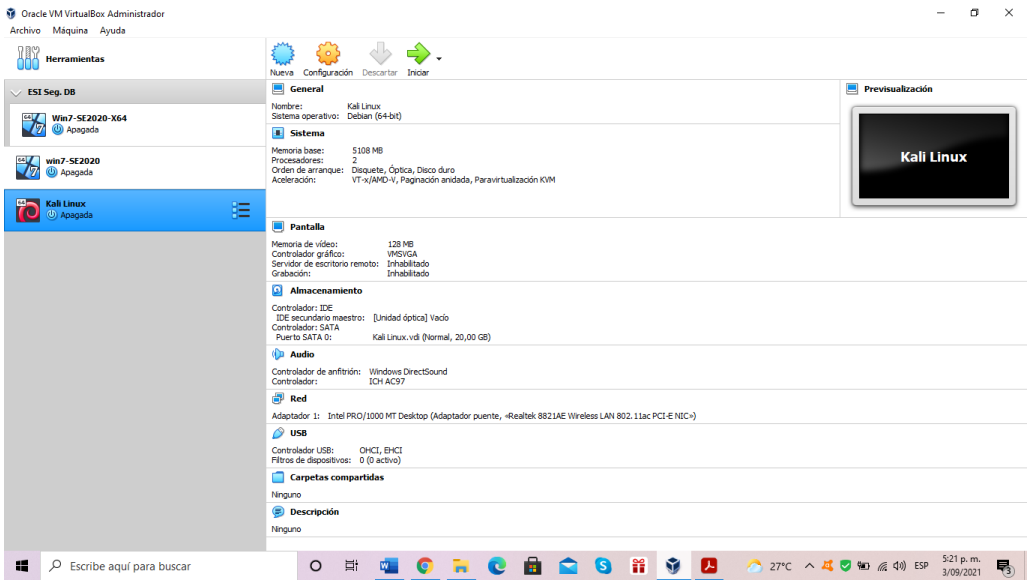
Fuente Propiedad del autor

Figura 16 Características de la máquina de Kali



Fuente Propiedad del autor

Figura 17 Montaje Banco de Trabajo



Fuente Propiedad del autor

ACTUACIÓN ÉTICA Y LEGAL

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

De acuerdo con el anexo 2

Se puede concluir que la gerencia de WhiteHouse Security no realizó un análisis detallado sobre las personas que trabajarán para ellos, sino que simplemente hacen recomendaciones y dejan contratos sin revisar donde se pierde la posibilidad realizar las modificaciones si son necesarias, teniendo en cuenta la importancia de salvaguardar la información sensible de la empresa que las contrata.

De otro lado, la empresa puede están incurriendo en delitos informáticos dentro de su organización sin darse cuenta, porque el simple hecho de que una tarea sea tan sutil como el conocimiento y verificación de la información del personal contratado se deja a la información del tercero susceptible de ataque.

Del mismo modo, es inapropiado "utilizar" y publicar información de la empresa en el proceso de selección sin una relación laboral clara, incluso aquellos que realizarán el procesamiento como información de terceros. Nombre de la empresa WhiteHouse Security.

Es importante que los diferentes procesos se realicen se hagan siguiendo los procedimientos para definidos para desarrollar de manera adecuada la respectiva gestión con relación revisión de los contratos para el personal de la organización.

Con relación al anexo 3.

“Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.” [7]

De acuerdo con lo anterior se observa que la organización Whitehouse Security se pueden estar presentando procesos ilegales, razón por la cual no desean que las

[7] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

personas que ingresen a trabajar con ellos reveles las irregularidades que se puedan encontrar en desarrollo de sus funciones.

Es importante tener en cuenta quien implemente los procedimientos en contra de la ley colombiana estipulados en la violación de la conducta, que derivará en delito y falta de ética profesional, pues la identificación de conductas ilícitas debe ser denunciada a las autoridades competentes.

Ahora bien, si los resultados de la investigación obtenidos a través de los procedimientos legalmente establecidos, si se denuncia un procedimiento ilegal, se debe revisar con un superior que tenga la autoridad para garantizar la protección de la información, y clasificar según los parámetros de la Whitehouse Security.

"Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la parte receptora con ocasión del proceso de selección de personal.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

   parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones." [8]

En esta cláusula se puede evidenciar que la Whitehouse Security lleva a cabo actividades de interceptación de información que pueden ser derivas del desarrollo de sus funciones, mediante la aplicación de procedimientos adecuados para esta actividad, ahora bien, si esto se realiza de manera ilegal la empresa estaría

[8] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

incurriendo actividades que se encuentran reglamentadas y penalizadas por la ley de Colombia, se estaría contravía de la ética profesional.

Es importante conocer que al realizar estas actividades ilícitas se está incurriendo en conductas delictivas, en caso de ser así se debe asumir las consecuencias por cometer dicho delito.

"Cláusula cuarta Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella.

Parágrafo 3 No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros." [9]

Se observa que el receptor se compromete a no revelar información sobre actividades sospechosas dentro Whitehouse Security, ni ningún tipo de trámites ilegales que puedan ocurrir y ejecutarse dentro de la misma. Teniendo en cuenta la legislación colombiana, esto puede derivar en delito y falta de ética profesional, pues es necesario denunciar ante las autoridades competentes al momento de identificar hechos ilícitos.

"Cláusula cuarta Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella.

Parágrafo 4 Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas." [10]

En este parágrafo la parte receptora, se comprometerse no solo a no divulgar la información confidencial de Whitehouse Security, sino también a no divulgar ningún tipo de programas ilegales que puedan mostrarse y llevarse internamente. Implementado por la Whitehouse Security esto puede derivar en delito y falta de ética profesional, pues cuando se identifica un acto ilícito, se debe denunciar a la autoridad competente.

"Cláusula cuarta Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella.

[9] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.
[10] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

Parágrafo 7 Responder por el mal uso que le den sus representantes a la información confidencial.” [11]

La organización Whitehouse Security, quiere que el profesional que asuma el cargo también asuma la responsabilidad por los procedimientos ilegales que se puedan estar desarrollando al interior de la empresa ante un eventual auditoria u operación de allanamiento a la misma.

“Cláusula cuarta Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella.

Parágrafo 8 Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.” [12]

Se evidencia que la organización Whitehouse Security, con este parágrafo busca que el profesional responda por la información que tenga en su poder ante las autoridades competentes ante una posible investigación.

“Cláusula cuarta Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella.

Parágrafo 9 La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security.” [13]

En el parágrafo se observa que al aceptar el cargo se compromete no divulgar la información de empresa, sino también los procesos ilegales que se puedan estar llevando al interior de la entidad, en este caso se incurriría falta a la ética como profesional, al identificar conductas ilegales que deben ser denunciadas ante las autoridades competentes para adelantar las respectivas investigaciones del caso.

“Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial

[11] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.
[12] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.
[13] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security. ” [14]

Al aceptar la oferta, el profesional se compromete a responder por la información que tenga de Whitehouse Security en su poder y liberar de toda responsabilidad a la organización.

“Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.” [15]

En esta cláusula es muy ambigua ya que en las cláusulas previamente mencionadas se habla de ilegalidad y procesos ilegales que se están realizando en la organización como son métodos ilegales y ocultar información, de igual manera se sugiere que se regirán por las leyes colombianas.

Finalmente, se puede concluir que las actividades que realiza la empresa Whitehouse Security hay procesos ilegales, que el profesional que asuma el cargo se va a ver comprometido en su ética profesional como personal, además de asumir la responsabilidad por las acciones realizadas por la empresa Whitehouse Security.

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Luego de realizar el análisis se evidencia que la empresa Whitehouse Security, posiblemente este cometiendo delitos informáticos.

En la ley 1273 de 2005, se puede enmarcar las siguientes cláusulas primera y segunda, clausula cuarta, parágrafo 3; en el artículo 269A cual se habla de todo acceso abusivo a diferentes sistemas de información sin tener autorización para realizar dicho laboral, en el mismo se menciona las chuzadas que se acuerdo se evidencian claramente.

La cláusula segunda también se puede observar una infracción al artículo 269C, el cual se habla de la interceptación de datos informáticos entre otros.

De acuerdo con el análisis realizado se concluye que este acuerdo de alguna manera afecta todos los artículos de la ley 1273 de 2009, ya se presenta de muchos procedimientos irregulares que afectan el buen funcionamiento de los sistemas de información.

[14] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.
[15] Anexo 3 Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted como experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

Teniendo en cuenta el análisis que se realizó, si este acuerdo es definitivo No Aplicaría, ya en el desarrollo de estas actividades ilícitas se vería afecta la integridad como profesional integro, con valores claros, que respeta el conocimiento adquirido, que la carta de navegación como buenos profesionales es el código emitido por el COPNIA el cual se indica como el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. En su artículo 31 inciso b "Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados" [16] al aceptar esta oferta claramente se está violando a este artículo.

De igual manera en el inciso f "Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder." [17] Este deber se vería afectado al aceptar la oferta económica para trabajar WhiteHouse ya que en dentro de su acuerdo claramente se prohíbe cumplir con los deberes que se tiene como profesional y como ser humano que respecta las leyes y normas para el desarrollo efectivo de su labor como profesional.

El artículo 34 se enumeran las prohibiciones especiales para los profesionales con relación a la sociedad en su inciso a "Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación" [18] este inciso claramente advierte al profesional que el aceptar trabajos que vayan en contra de las leyes, pueden llevar afrontar las consecuencias de dichas acciones.

[16] «Código de ética para ingenieros». Consultado septiembre en línea https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
[17] «Código de ética para ingenieros». Consultado septiembre en línea https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
[18] «Código de ética para ingenieros». Consultado septiembre en línea https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Deberá buscar la noticia del caso “OPERACIÓN ANDROMEDA BUGGLY” en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar.

Las operaciones militares realizadas en nombre de "Andrómeda" han provocado escándalos por su influencia social y política. Es un marco de acción legal creado por agencias de inteligencia militar, y su propósito es utilizar el conocimiento informático civil para la búsqueda de información por medios abusivos. Comprenda a los civiles como piratas informáticos y tenga un amplio conocimiento del uso de herramientas informáticas para aprovechar las vulnerabilidades. De esta manera, se creó un lugar de recepción aparentemente informal en el barrio de Galerías de Bogotá, denominado Buggly, con elementos atractivos para los jóvenes como tatuajes, comida, paintball, y por supuesto, equipado con computadoras. Las habitaciones y la mezcla de civiles. y el personal está fusionado. Por lo tanto, Bagley Andromeda es una operación secreta legítima, y el ejército usa mentiras para atraer a civiles a actos ilegales.

La implicación del llamado hacker Carlos Andrés Sepúlveda hizo aún más apasionante el caso, quien aparentemente compró y obtuvo información valiosa de Bagley, y también contribuyó a la democracia de la época. Centro Oscar Iván Zuluaga, servicio de campaña del candidato presidencial. Contrata sus servicios de forma indirecta. A lo largo de la historia de la humanidad, la información y su disponibilidad están estrechamente relacionadas con los intereses o perjuicios de los seres humanos, entidades y naciones, pero ahora que la información se almacena en medios, dispositivos electrónicos y viaja a través de redes informáticas, no solo es necesario comprender su Los métodos de procesamiento correctos, pero también para entender Su protección es muy importante, porque habrá delincuentes que lo conseguirán a toda costa.

En lo que a los militares se refiere, este es un comportamiento no ético, utilizando civiles, y pueden usar los mismos fondos para operaciones de engaño para capacitar a oficiales. Es aún más inmoral atraer y engañar para obtener datos e información. Una forma obvia de abuso expuso a civiles que cometieron delitos informáticos (como interceptación y robo de datos) que ya habían sido promulgados bajo la Ley No. 1273 de 2009. A nivel legal, "Andrómeda" no tiene control, lo que permite que personas conocedoras obtengan información al mejor precio, estas personas obviamente saben cómo manejar la información obtenida en la acción, y esta información puede ser utilizada para cualquier propósito. tipo de delito, incluso para ganar una elección o sabotear al candidato de la oposición.

EJECUCIÓN PRUEBAS INTRUSIÓN

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

- Fase de recolección de información

  Luego de recibir una solicitud indicando lo sucedido, se analizó la información brindada:

  se evidencia de que existe una fuga de información dentro de la organización en una de sus dependencias. La información preliminar es que la computadora donde se filtró la información instaló una aplicación llamada Rejetto bajo Windows 7 de la arquitectura X64.

  Se debe considerar que el sistema operativo Windows 7 ya no tiene actualizaciones de seguridad que Microsoft dejo de lanzar a partir de enero de 2020, y que el sistema operativo ha llegado al final de su vida útil y de alguna manera forzado y dejado paso a Windows 10.

  El riesgo de utilizar este sistema operativo está aumentando porque cada vez se descubren más casos de nuevas vulnerabilidades, que se explotan para socavar el pilar de la información.

- Fase de Búsqueda de vulnerabilidades

  En la información proporcionada, está la aplicación Rejetto que es un servidor de archivos HTTP, un servidor web para compartir archivos, es decir, es una aplicación libre de malware y se considera útil, pero tiene una vulnerabilidad.

  Una revisión e investigación de casos similares en la base de datos de vulnerabilidades reveló dos vulnerabilidades en esta aplicación.

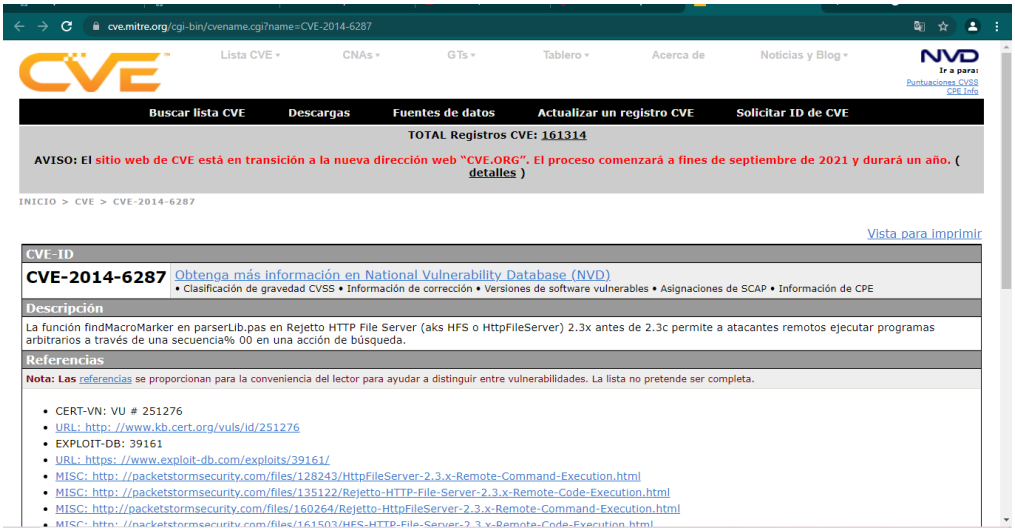
  Revisando la página de incibe que es una fuente confiable, se reveló una alerta sobre una vulnerabilidad en la aplicación Rejetto.

  Como se puede observar en la siguiente imagen.

Figura 18 Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287)

Fuente: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

Figura 19 CVE-2014-6287



Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

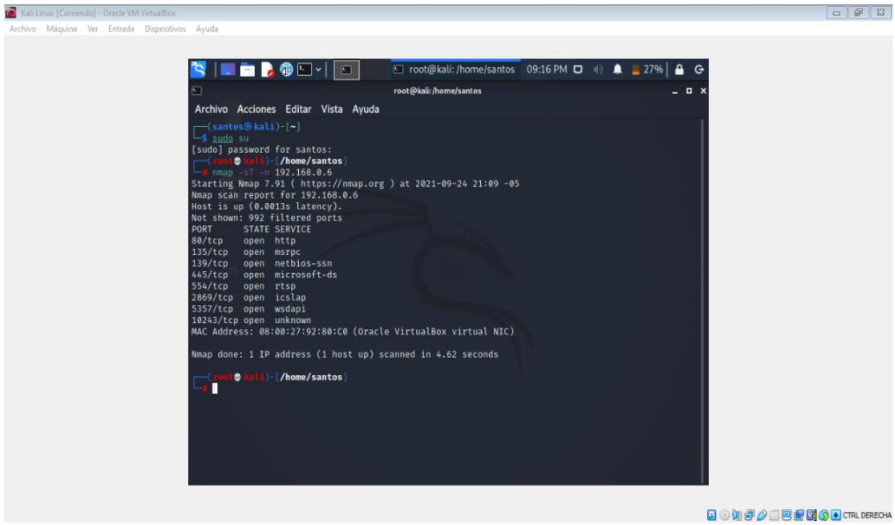
En la figura 2 se puede observar La función findMacroMarker en parserLib.pas en Rejetto, la cual permite ejecutar ataques remotos.

- Fase de Explotación de vulnerabilidades

  Se implementó un laboratorio de pruebas en el que se recreó el escenario a través de una máquina virtual, en la que el sistema operativo Windows 7 (víctima) con la arquitectura X64 tiene instalada la aplicación Rejetto, una maquina con un Kali Linux (atacante), ambos sistemas operativos se implementan en el mismo segmento de red, por lo que no solo es necesario

identificar vulnerabilidades, sino también comprender cómo operan las vulnerabilidades de seguridad y simular ataques.
Al analizar el sistema operativo Windows 7, utilizando la herramienta Nmap, se encontró que el puerto abierto producía una vulnerabilidad, que podría aprovecharse para intentar el acceso no autorizado, mediante el escaneo de la Ip de Windows que es 192.168.0.6, en la siguiente imagen se utiliza el comando nmap -sT -n 192.168.0.6 para conocer el estado de los puertos.

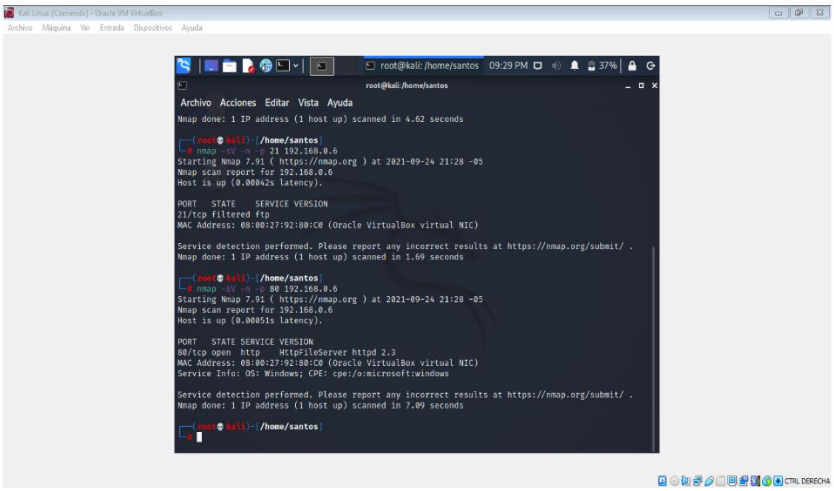
Figura 20 Comando Nmap



Fuente Propiedad del autor

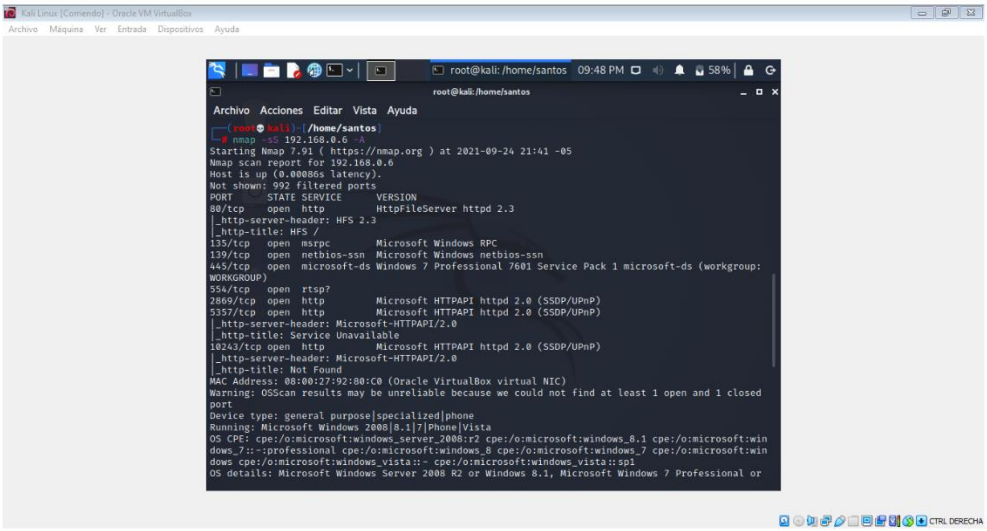
En la imagen se muestra escaneo a un puerto especifico.

Figura 21 Escanea de puerto especifico



Fuente Propiedad del autor

Figura 22 Escaneo de puertos



Fuente Propiedad del autor

- Fase Post-explotación

  En esta etapa, después de exponer posibles formas y métodos de ataque y verificar la fuga de información, se realiza una prueba para ver hasta dónde puede llegar este tipo de entrada de abuso e intentar acceder al archivo. Información, obtener usuarios y contraseñas reales, obtener derechos de administrador, crear usuarios legales, copiar, cambiar y eliminar información. Se puede acceder al sistema atacado como administrador, lo que permite acceder a toda la información del dispositivo.

- Fase de Informe

  Luego de analizar la información inicial, realizar las investigaciones necesarias de posibles vulnerabilidades, y realizar pruebas de laboratorio en un ambiente que replica la escena real, los resultados son claros, y se puede asegurar que las políticas y medidas de control no observadas definen la instalación de múltiples vulnerabilidades.

  La información de las vulnerabilidades de seguridad del programa de aplicación obviamente no ha sido revisada y probada por el responsable de seguridad de la información. No hay vulnerabilidades de actualización y múltiples vulnerabilidades de seguridad en el sistema operativo. No hay otro tipo de seguridad, pero lo proporciona el propio sistema operativo y ya no tiene la actualización proporcionada por el proveedor (en este caso, Microsoft).

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 X64.

Se tiene conocimiento sobre la fuga de información que se presenta al interior de la empresa en uno de sus equipos de determinada dependencia, en la cual se tiene instalada una aplicación Rejetto en un equipo con las siguientes características sistema operativo Windows 7 arquitectura 64 bit.

Al analizar la aplicación Rejetto, se tiene que es un HTTP file server, el cual sirve para compartir archivos, la cual es libre de malware, pero puede presentar vulnerabilidades, como son los exploits que pueden llevar a una Shell y una sesión abierta de Meterpreter.

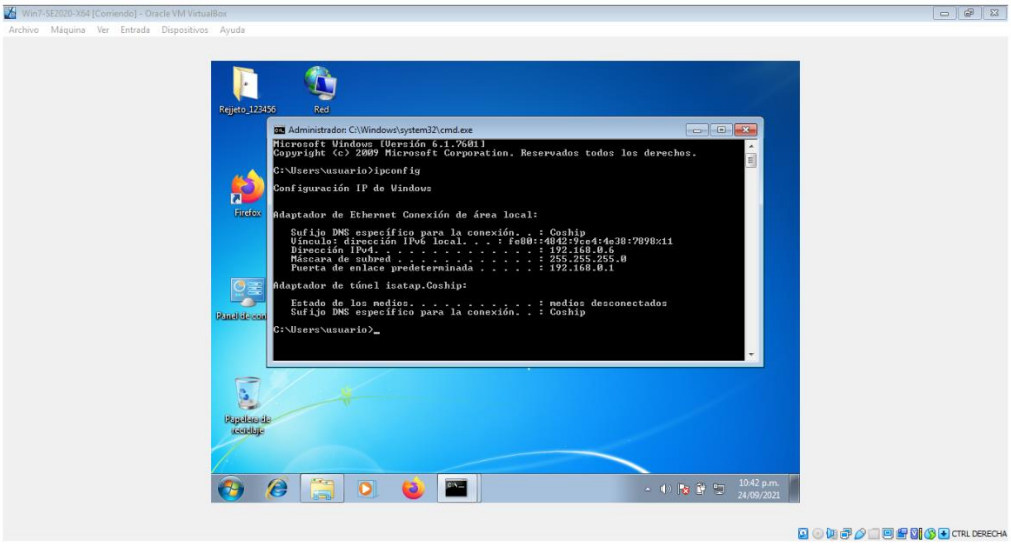
La principal razón por la que los atacantes suelen utilizar shell inverso es la forma en que se configuran la mayoría de los cortafuegos. El servidor atacado generalmente solo permite conexiones en puertos específicos. Por ejemplo, un servidor web dedicado solo aceptará conexiones en los puertos 80 y 445. Esto significa que no es posible configurar un escucha de Shell en el servidor atacado. Abrir un puerto o estar en modo de escucha es una mala práctica porque el sistema operativo y las aplicaciones (como correo, almacenamiento de información, navegadores, bases de datos, almacenamiento de contraseñas y usuarios) están completamente expuestos al seguimiento de los puertos a través de Metasploit, Nessus, Nmap, etc. Herramienta para escanear.

Teniendo en cuenta que estos puertos generan una gran cantidad de vulnerabilidades para la seguridad de la información siendo uno de los activos más importantes para las organizaciones, razón por cual es importante realizar una alta política para salvaguardar la información.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 7”? ¿Qué puerto abre la aplicación específica en el anexo?

Mediante la utilización del comando ipconfig, se visualiza la ip asignado al equipo con Windows, como se puede observar en la siguiente imagen.

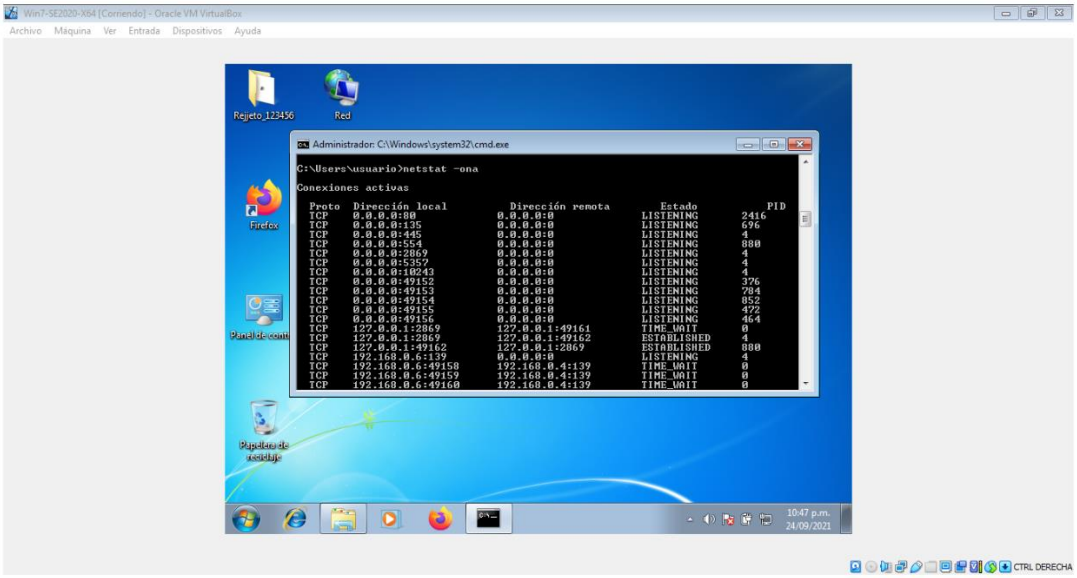
Figura 23 Ip Windows 7



Fuente Propiedad del autor

Con el comando netstat muestra los puertos abiertos y con estado de Listening como se puede ver en la siguiente imagen.

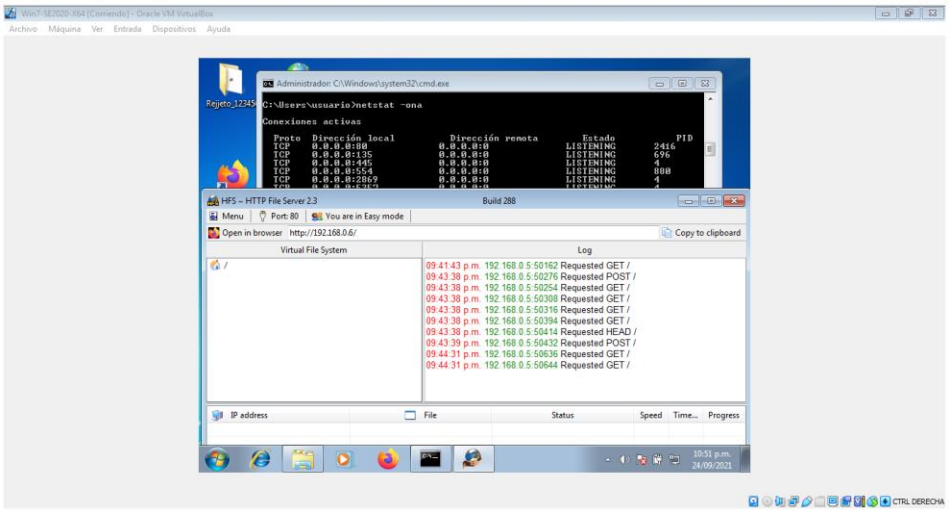
Figura 24 Comando Netstat



Fuente Propiedad del autor

La aplicación Rejetto que se ejecuta en la máquina de Windows se puede observar que el puerto 80 se abre con esta aplicación como se observa en la siguiente imagen.

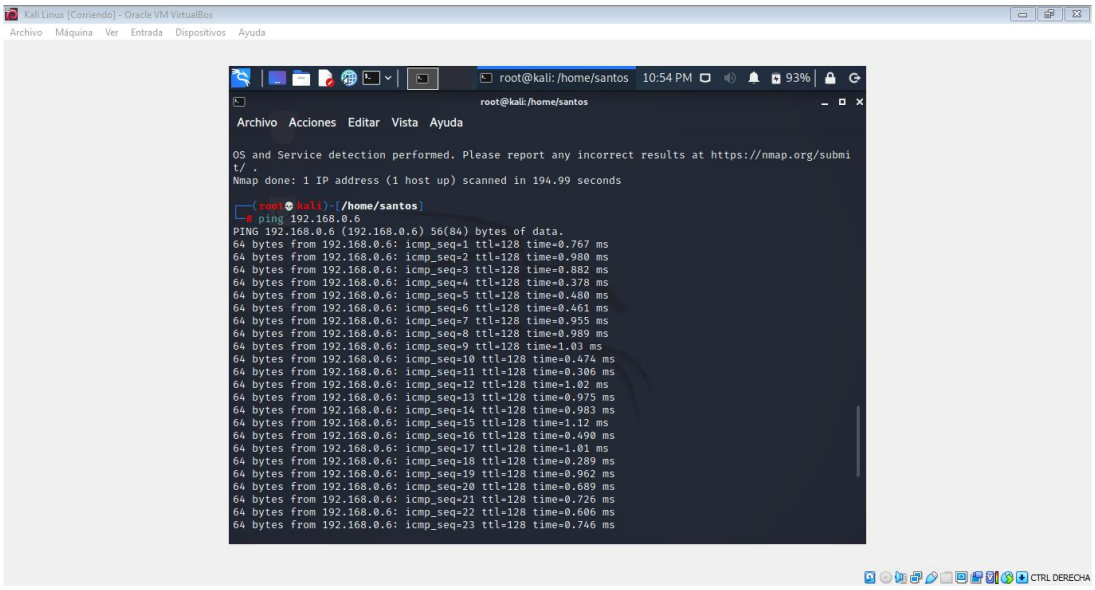
Figura 25 Utilización Puerto 80



Fuente Propiedad del autor

Al encontrase en red los equipos se puede realizar el ataque desde sistema operativo Kali.

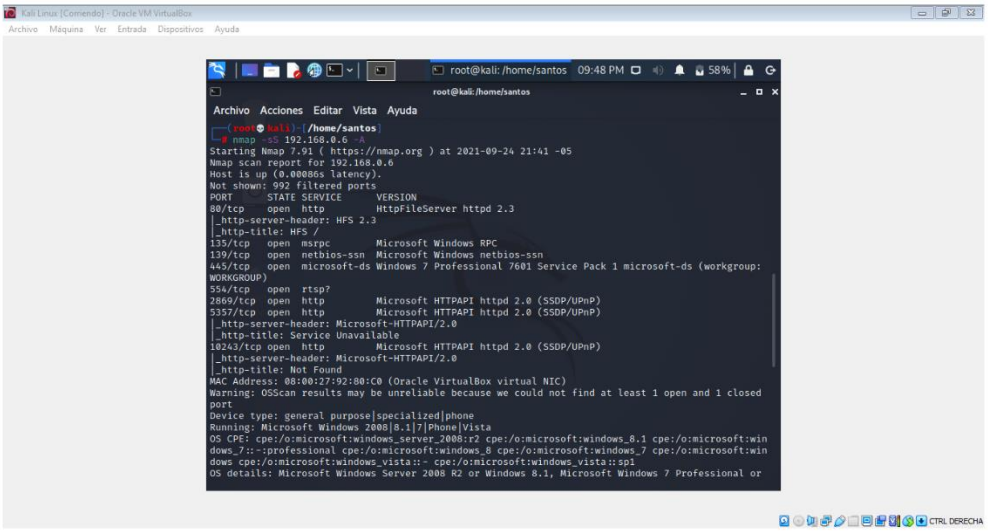
Figura 26 Ping a la máquina de Windows 7



Fuente Propiedad del autor

Mediante el comando Nmap, un intruso puede identificar los puertos abiertos para realizar el ataque en determinado momento.

Figura 27 Utilización comando Nmap



Fuente Propiedad del autor

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

Entonces, el atacante puede conocer las vulnerabilidades conocidas de la aplicación de acuerdo con la versión del software que se ejecuta en el host remoto. Si no hay un parche, existe el riesgo de ser explotado. Como se hace en esta PoC, se aprovecha de un error conocido que permite a un atacante remoto ejecutar código arbitrario en el servidor (host) que aloja la aplicación.

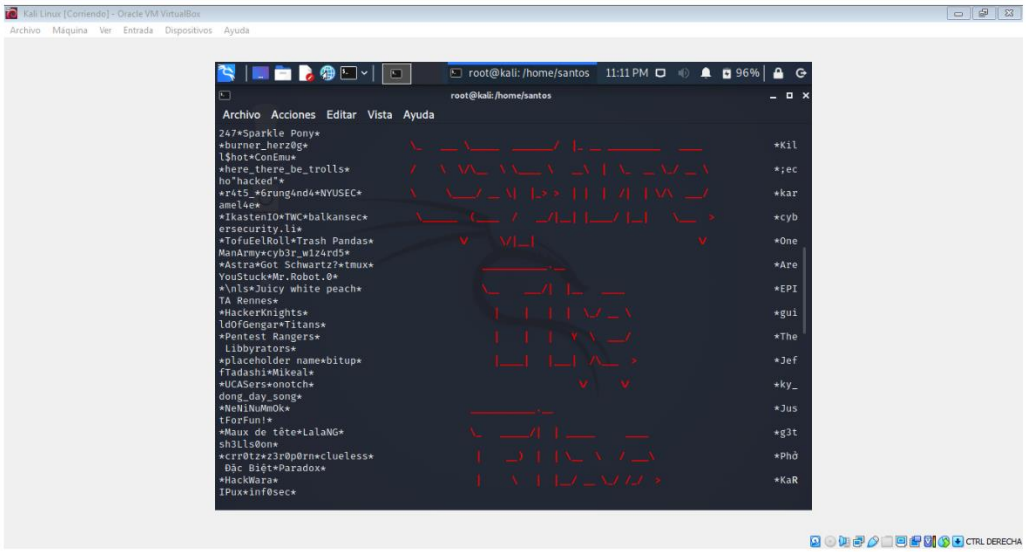
En este caso, la computadora con la dirección IP: 192.168.0.6 La función de comentario de archivo en Rejetto HTTP File Server (hfs) 2.3cy versiones anteriores permite a los atacantes remotos ejecutar código arbitrario cargando archivos con ciertas secuencias de bytes UTF-8 no válidas, que se interpretan como símbolo de macro ejecutable.

Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Teniendo en cuenta que ya se conoce que el puerto 21 es vulnerable, se realiza un ataque mediante Metasploit.

En la siguiente imagen se inicia el comando Metasploit.

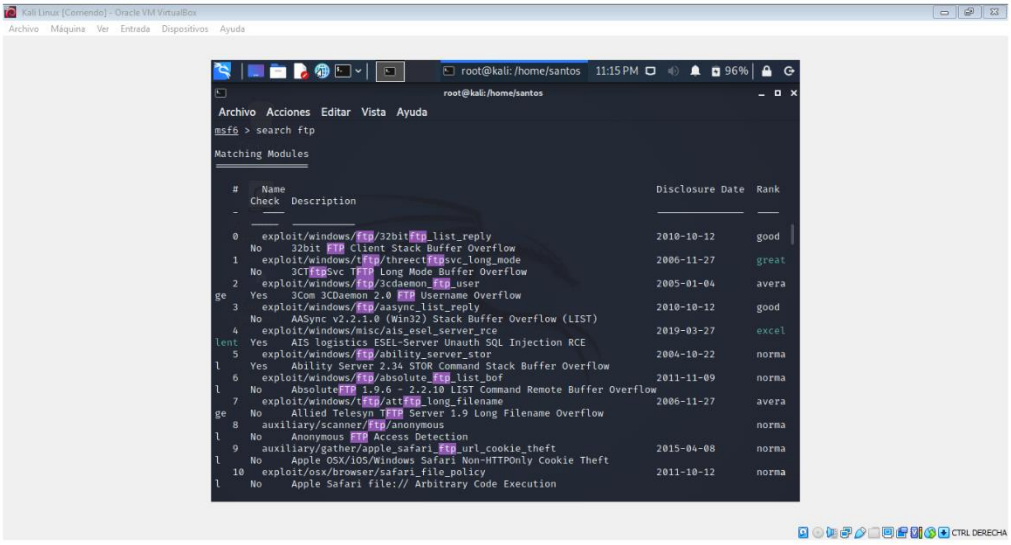
Figura 28 Comando Metasploit



Fuente Propiedad del autor

Se realiza escaneo de las vulnerabilidades al servicio Ftp como se muestra en la siguiente imagen.

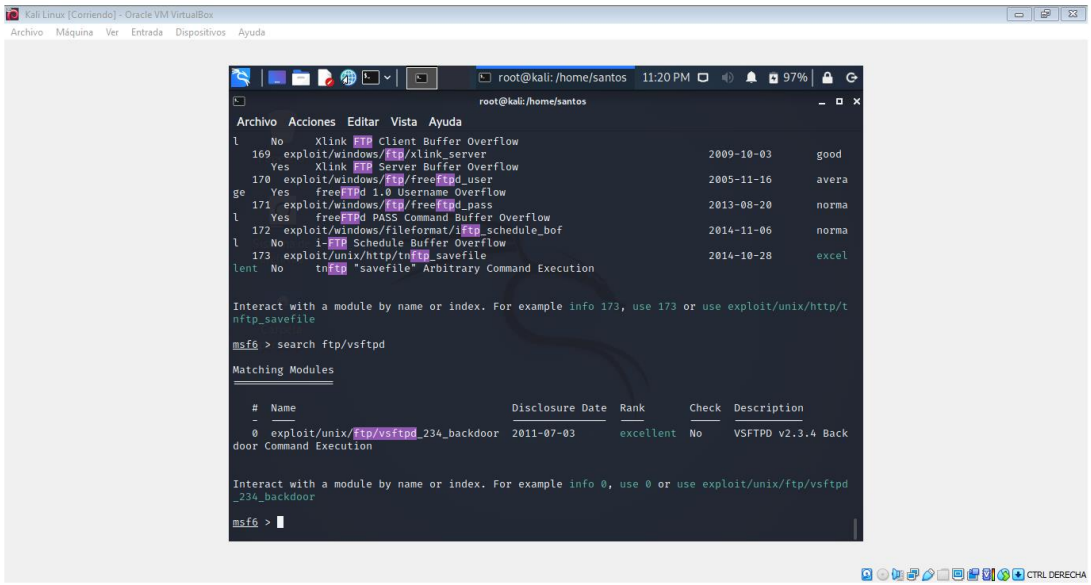
Figura 29 Servicio Ftp



Fuente Propiedad del autor

Para especificar la vulnerabilidad se utiliza el comando search ftp/vsftpd

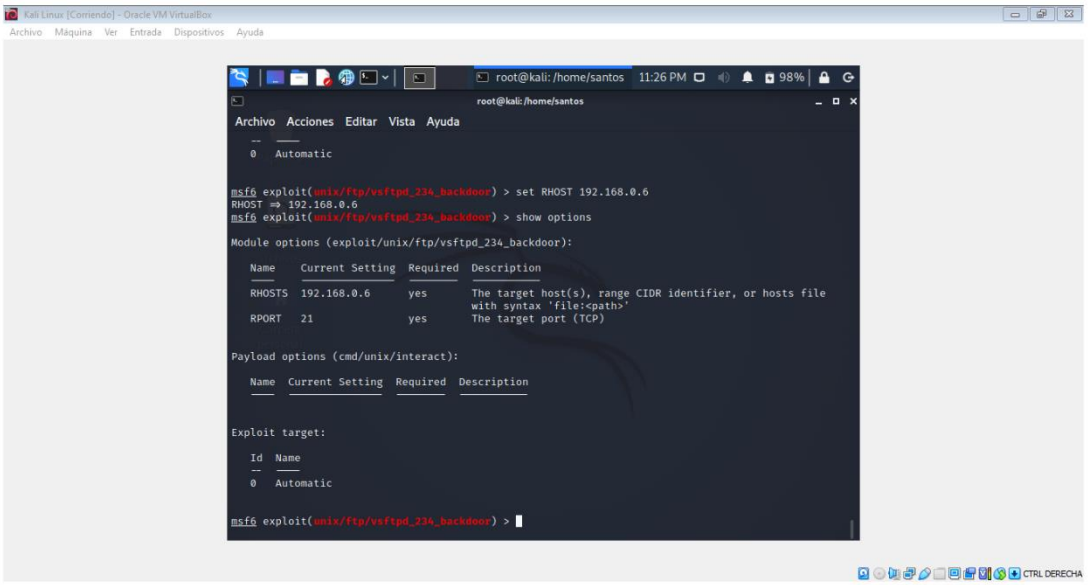
Figura 30 Comando search ftp/vsftpd



Fuente Propiedad del autor

En la siguientes imagen se muestra el puerto 21 y la ip de la máquina de Windows.

Figura 31 Puerto 21 y Ip Windows



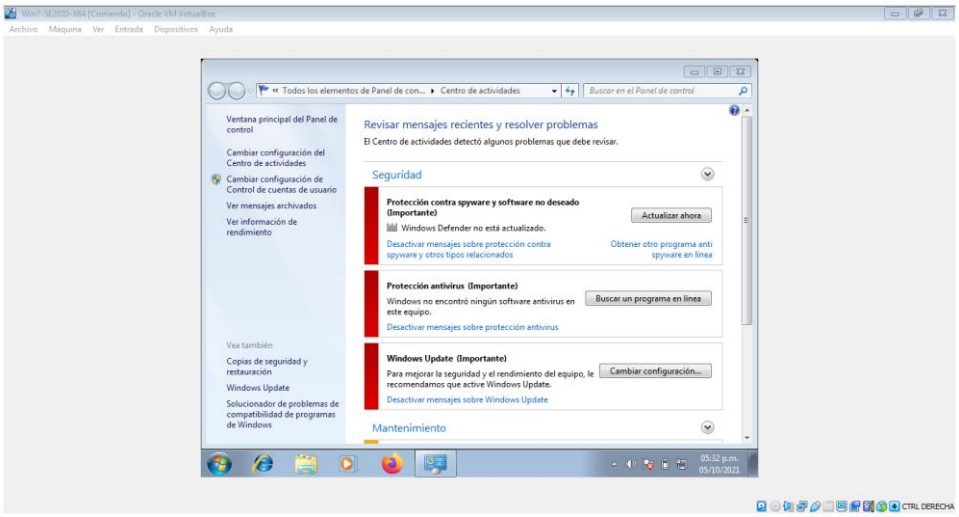
Fuente Propiedad del autor

CONTENCIÓN DE ATAQUES INFORMÁTICOS

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Inicialmente se debe realizar la validación de que tipo de ataque se está presentando y conocer las vulnerabilidades del sistema con el equipo de Red Team, para de esta manera afrontar de la mejor manera ataque del cual están siendo víctimas, de esta forma proceder de manera oportuna ante el ataque, con la realización de dicha validación se encuentra que la maquina con Windows 7 64 bit presenta las siguientes vulnerabilidades en el firewalls y antivirus. Como se puede observar en la siguiente imagen.

Figura 32 Vulnerabilidades Windows 7



Fuente Propiedad del autor

Una vez verificada esta información se debe dar a conocer inmediatamente para activar los protocolos que se tengan en la organización para combatir el ataque del que son víctimas los sistemas de información, es importante que activen los protocolos desde la detección de la amenaza, recuperación y respuesta en caso de que sea necesaria.

En detección se debe realizar las siguientes actividades:

- Verificar los equipos que están siendo objeto del ataque.
- Conocer el progreso del ataque las afectaciones en los sistemas de sistemas.
- Utilizar herramientas para conocer vulnerabilidades del sistema.
- Desconectar de la red los equipos víctimas del ataque.

En la recuperación: se debe implementar un plan organizado de recuperación de los sistemas afectados, para dejarlos igual como estaban antes del incidente presentado mediante la utilización backups de los sistemas, copias de seguridad entre otras técnicas.

Respuesta, consiste en informar al personal tanto interno como externo de la organización del ataque que se presentó para que el personal este enterado de la situación de la organización, proceder con las respectivas denuncias que haya a lugar.

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Redteam qué medidas de hardenización propondría para que el ataque no se repita?

Es importante tener en cuenta que la hardenización son las medidas de aseguramiento de los sistemas de información contra los diversos ataques, de esta manera estar protegidos ante los posibles incidentes que se puedan presentar en determinado momento, a continuación se enuncia algunas medidas.

- Actualizar los sistemas operativos, demás programas para que funcione efectivamente cada equipo y evitar posibles ataques.
- Implementar en la organización buenas prácticas para la gestión de la fuga de información.
- Tener una política de seguridad y procedimientos para la información.
- Crear contraseñas seguras y robustas para evitar fuga de la información.
- Contar con software licenciado.
- Activar el cortafuego para evitar ataques.
- Limitar el uso de archivos compartidos en la red.
- Realizar copias de seguridad.
- Control de los dispositivos extraíbles.
- Tener planes de formación en ciberseguridad, seguridad de la información y buenas prácticas en los sistemas de información, con el objetivo sensibilizar a los usuarios de la importancia de salvaguardar la información.

- Habilitar solo los puertos necesarios de acuerdo con la necesidades de cada usuario.

- Implementar programas para escaneo de vulnerabilidades.

- Verificar las aplicaciones instaladas en cada equipo.

¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Tabla 2 Diferencia entre Equipo BlueTeam y Respuesta a incidentes de seguridad (CSIRT)

El equipo BlueTeam	Los equipos de respuesta a incidentes de seguridad (CSIRT)
Es un equipo profesional diseñado para detectar amenazas de ciberataques de manera oportuna. Blueteam está siempre en modo de defensa, lo que lo hace siempre en modo de detección y estado de gestión experta de incidentes de seguridad. • Siempre están buscando un ataque • Buscan debilidades en la empresa. • Analiza el sistema para encontrar cambios. • Defiéndete de los ataques y anticípate a ellos. • Revisar modelo y personal. • Comprometidos con la mejora continua de la identificación de fallas. • Recomendar un plan de acción para mitigar el ataque. • Investigue y analice el malware para comprender cómo se comporta.	Es un equipo que brinda servicios de prevención y respuesta ante incidentes de seguridad informática que afectan a entidades y comportamientos, y cómo reaccionan cuando se ejecuta el incidente y cuando ocurre el incidente. Además, se encargan de coordinar, dar respuesta y gestionar soluciones a incidencias o incidencias informáticas, lo mejor es estar preparado para lo que está por suceder, no saber actuar y no tener un plan de seguridad. La hora en que ocurrió el incidente. CSIRT está directamente relacionado con el plan de gestión de seguridad. • Prevenir y responder a incidentes de seguridad informática. • Soluciones para responder y gestionar incidentes informáticos • Realizan actividades como educación, análisis de riesgos o publicidad regulatoria, y actividades de prevención sistemática. • Investigue cómo y por qué ocurrieron los ataques y evite que vuelvan a ocurrir.

Fuente Propiedad del autor

¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS “Center For Internet Security” usted lo utilizaría para qué fin?

CIS (Center for Internet Security) Es una organización sin ánimo de lucro, cuya misión es hacer del mundo conectado un lugar más seguro mediante el desarrollo, la validación y la promoción soluciones oportunidades de mejores prácticas que ayudan a las personas , las empresas y los gobiernos a protegerse contra las amenazas cibernéticas generalizadas.

Teniendo en cuenta lo anterior, se utiliza la CIS como un banco de información para actualizar las buenas prácticas dentro del equipo Blue Team, con fin de revisar constantemente la información publicada sobre las diferentes vulnerabilidades, adicionalmente crear un listado de las acciones a realizar según cada ataque se presente en determinado momento, asi como las recomendaciones a seguir y mejoras a implementar.

Al hacer uso de esta herramienta, se tendría un conjunto de acciones para utilizar de acuerdo con el ataque se presente, ya que se encuentran en orden cronológico de forma de permite hacer uso de ella de manera más efectiva y eficiente para la protección de los sistemas de información de la organización.

Explique y redacte las funciones y características principales de lo que es un SIEM

SIEM es un tipo de software. Su principal objetivo es ayudar a los analistas de seguridad de TI de una manera estandarizada a analizar los sistemas de TI para su protección. El principal problema es que cuando un sistema de software está mal configurado, lógicamente crea problemas de seguridad y protección. Se utilizan diferentes herramientas para probar diferentes áreas de la empresa en busca de amenazas potenciales, pero como no existe un formato estándar entre ellas, analizar esta información se convierte en un desafío obvio. Se vuelven más complejos y, finalmente, el sistema de seguridad no puede protegerse. De cualquier manera, no mostrará alarmas que deban conocerse a tiempo ni amenazas específicas que sean solo ruido.

Dentro de las características encontramos las siguientes:

- Permite la respuesta automática a eventos y amenazas.
- Disminución del tiempo de detección de ataques.
- Obtener información de manera rápida y eficiente para realizar análisis forenses.
- Alertas de seguridad efectivas.
- Analizar y vincular registros en tiempo real
- Mantenga un registro de los eventos.
- Gestión de riesgos.

- Gestionar métricas de seguridad.
- Divulgación de la propiedad.
- Permite la evaluación de vulnerabilidades.
- Detectar brechas de seguridad

Funciones de un programa SIEM:

Recopilación de datos de contexto y de registro: esta función recopila los datos de registro de los dispositivos de la empresa, los datos procesados por cada usuario, las vulnerabilidades de cada dispositivo y los datos de identidad utilizados por cada persona.

Clasificación y normalización: esta función incluye estandarizar el formato de almacenamiento de todos los registros de usuario y asignar pasos normales y anormales para que SIEM pueda procesarlos.

Vinculación: en esta función, el proceso de vincular reglas a datos de contexto a través de operaciones estadísticas y algorítmicas. Normalmente esta correlación se realiza en tiempo real, pero también hay datos que no se pueden utilizar de esta forma, por lo que se vincula a una base de datos de eventos ocurridos.

Alertas y notificaciones: Esta característica está relacionada con los administradores de programas y / o gerentes de TI, las principales alertas están enfocadas a los servicios de mensajería y SNMP (Network Management Protocol).

Prioridad: esta función le permite priorizar eventos de seguridad importantes y eventos sin importancia, y luego enviar una alerta solo cuando sean realmente relevantes. Para ello, utilizan la correlación de datos de vulnerabilidad cruzada con la información de los activos de la empresa.

Acceso en tiempo real: se implementa en la mayoría de los casos a través de controladores de eventos, que pueden ser administrados por software como SolarWinds. La desventaja de este producto es que tienes que pagar por él, pero vale la pena. Es muy flexible, lo que no solo le permite ver eventos en tiempo real, sino que también le permite monitorear eventos a partir de datos históricos.

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Firewall De Hardware Y De Software.

FIREWALL es conocido como un sistema para proteger nuestros dispositivos en la red. Cuando hablamos de firewalls de hardware, nos referimos a un dispositivo

físico. Por supuesto, esta es una opción mucho más cara. Su propósito es prevenir comunicaciones potencialmente peligrosas.

En cambio, un firewall de software es un programa de computadora. Es mucho más barato o incluso gratis. Hay muchas opciones que podemos instalar en todo tipo de sistemas operativos y dispositivos. Software de firewall instalado en el dispositivo.

Esto significa que si llevamos nuestro portátil o teléfono móvil a otro lugar, la protección seguirá ahí. En cambio, generalmente se conecta un firewall de hardware al enrutador.

GATEWAY

El software antivirus y de puerta de enlace explota el papel del servidor proxy como un obstáculo natural para el paso del tráfico web entre su infraestructura corporativa y el mundo exterior, protegiendo sus redes de TI corporativas al detener las amenazas temprano y reducir su exposición a las amenazas.

MISP (Malware Information Sharing Platform)

Plataforma de inteligencia de amenazas para compartir, almacenar y vincular métricas de penetración de ataques dirigidos, información de amenazas, información de fraude financiero, información sobre vulnerabilidades o incluso información de lucha contra el terrorismo.

DMZ o zonas desmilitarizadas

Las regiones militares forman parte de una red aislada en la intranet de la organización. Por lo general, se encuentra en esta área de redes, servicios y recursos necesarios para acceder a Internet más que servidores de mensajería y servidores web.

Las características principales de un área no milita no deben permitir la conexión DMZ a la intranet, pero permite conexiones a Internet e Intranet de la empresa, donde los equipos de trabajo de los empleados son como, cuál es el estudio principal para los servicios de red que son sensibles a Los Internet son vulnerables, permiten una mayor capacidad de pérdida de información, al implementar soluciones de encarcelamiento, mantener esto a los atacantes, atacarán en la primera línea con el servicio que no está involucrado en la intranet, ya que la conexión DMZ está bloqueada.

Como firewall también puede ser hardware o software.

Snort

Es un sistema de código abierto basado en el Sistema de detección de intrusiones (IDSN). Es un software de detección y monitoreo de intrusiones en la red que utiliza una base de datos y un modelo de ataques de red conocidos, y se basa en la creación de las reglas que conforman el modelo de monitoreo de la red.
El programa funciona bien con las reglas y filtros que se configuraron en la instalación inicial para adaptar la monitorización a lo que necesitamos. Tiene la ventaja de actuar como una esnifer, lo que significa que podemos ver el tráfico en paquetes desde la consola o como un sistema de detección de intrusos (IDS) en modo automático o semiautomático.

Cuando un patrón de los generados coincide con un paquete de datos, se comunica, y de esta manera se conocen las características básicas del ataque, como cuándo, cómo y dónde, permitiendo que la respuesta activa de la Blue Team frene el ataque. En lo que respecta a las funciones, es de transmisión gratuita, liviano, permite análisis en tiempo real, utiliza filtros y detecta canales.

WAZUH EDR (Endpoint Detection and Response)

El perímetro o borde de la red no es el único punto donde se establecen políticas de seguridad independientemente de su importancia, las redes modernas tienden a ser cada vez más abiertas y sin fronteras, y existen escenarios externos para proveedores de servicios externos como VPN, proveedores y proveedores de nube. que crean desafíos de ciberseguridad para los administradores de información. Las herramientas de EDR se enfocan en respuestas automatizadas desde el punto de vista del dispositivo terminal, servidor o computadora del usuario final.

Cyber Triage

Es una herramienta que permite la respuesta a incidentes informáticos, donde Cyber Triage monitorea constantemente los puntos finales de una organización, si algo inusual comienza a suceder, Cyber Triage envía notificaciones a través de la red o USB requerido en el punto final para recopilar información de anomalías. Esta información se envía a los programas centrales y genera una serie de informes que pueden ayudar a los equipos de seguridad a saber cómo actuar.

ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS

En el equipo Blueteam y el Redteam, se recomienda que los expertos en seguridad informática sigan investigando y aprendiendo, porque las nuevas tecnologías o ataques que implementan contra diferentes organizaciones aparecen todos los días, aprende de ellas y deja que otras organizaciones estén preparadas para evitar lo mismo. Les sucedió algo.

En la actualidad, existen diversas certificaciones en el campo de la seguridad informática, por lo que se recomienda que los expertos en este campo se capaciten y certifiquen en ramas específicas, para que se conviertan en expertos técnicos en temas específicos, para que puedan tomar decisiones ágiles y ser preparado para cualquier situación que pueda surgir.

CONCLUSIONES

- A través del trabajo realizado, se pudo conocer las leyes y disposiciones vigentes en Colombia en materia de seguridad de la información y leyes de procesamiento de datos.

- Según el análisis realizado, es posible saber qué paso se utiliza en el proceso de pentesting y qué se hace en cada paso.

- Se han identificado las herramientas de código abierto más utilizadas para detectar vulnerabilidades y explotar varios sistemas.

- Se instalaron las maquinas virtuales de acuerdo con las indicaciones para cada una de ellas.

- Se observaron procesos ilegales en el acuerdo de confiabilidad, claramente afectan los artículos del código de ética del Copnia para los ingenieros.

- Es importante conocer las diferentes vulnerabilidades que afectan los sistemas de información, y de esta manera saber que herramientas y técnicas se deben utilizar ante la ocurrencia de una vulnerabilidad en determinado momento.

- Teniendo en cuenta en avance tecnológico que se ha desarrollado actualmente en el mundo, es importante avanzar de igual manera en la protección e implementación de políticas de seguridad claras para que las organizaciones se encuentren protegidas antes las diferentes vulnerabilidades.

- Realice copias de seguridad periódicas del sitio web y la base de datos. De esta forma, si se produce algún imprevisto, podemos restaurar la versión actualizada sin tener que rehacer el trabajo desde el principio.

- Es necesario que las empresas inviertas en seguridad informática para proteger la integridad de la información, mediante la implementación una arquitectura de seguridad informática, donde las empresas tengan definida claramente la ruta de procedimientos para afrontar posibles ataques que puedan recibir de los ciberdelincuentes o fallos en la seguridad.

RECOMENDACIONES

- Establezca una contraseña segura, cámbiela con regularidad y no utilice la misma contraseña para diferentes servicios. Como se menciona ocasionalmente, la fuerza del código de acceso es la principal barrera de seguridad. Para crear una contraseña segura, se recomienda que la contraseña tenga al menos 6 caracteres y contenga letras, números y símbolos.

- De acuerdo con los roles y necesidades de cada usuario, se establece una estrategia de perfil para acceder, escribir y modificar directorios y archivos públicos en la organización. Siempre que sea posible, aplique los permisos más estrictos posibles a carpetas, archivos y usuarios.

- Las empresas deben estar en constante actualización de las herramientas y técnicas que utilizan para la identificación de las vulnerabilidades, teniendo en cuenta que las mismas también se actualizan obteniendo nuevas versiones de estas, que al no tener las herramientas actualizadas pueden ser blancos fáciles para estos riesgos.

- Hoy en día es importante que las organizaciones tengan claridad de las técnicas y herramientas existentes para estar protegidos ante los diferentes ataques a los que se encuentran expuestos.

- Las empresas al hacer uso adecuado de las recomendaciones en seguridad tienen la ventaja de hacer sus sistemas de información seguros ante las diferentes vulnerabilidades que se presentan actualmente.

- Teniendo en cuenta que el activo más importante hoy en día es la información, es adecuada utilizar las recomendaciones de seguridad para que se tengan sistemas más seguros.

- Formación continua de los usuarios, se generan muchos ataques informáticos porque los usuarios desconocen las buenas prácticas y políticas que existen en la organización, y en muchos casos el usuario es el principal responsable en la aparición de los ciberataques.

REFERENCIA BIBLIOGRÁFICAS

Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? ». [En línea] [Consultado 29 septiembre de 2021] disponible en (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian)

Ataques informáticos ». [En línea] [Consultado 05 octubre de 2021] disponible en (https://seguridadeinformaticabrm.wordpress.com/2017/02/01/ataques-informaticos/)

BEYONTRUST, «Web Vulnerability Management Software | Assessment Software». [En línea] [Consultado 10 octubre de 2021] disponible en (http://www.beyondtrust.com/Products/RetinaWebSecurityScanner/)

Ciber Riesgos ». [En línea] [Consultado 07 Junio de 2020] disponible en (https://www.mpmsoftware.com/es/blog/ciber-riesgos/)

Ciberamenazas: ¿Cuáles son las técnicas más utilizadas por los hackers? ». [En línea] [Consultado 07 Junio de 2020] disponible en (https://www.gb-advisors.com/es/ciberamenazas-tecnicas/)

COPNIA (2003). Ley 842 de 2003. | Copnia. ». [En línea] [consultado 4 de octubre de 2021]. disponible en https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

COPNIA. (2020). Código de ética | Copnia. ». [En línea] [consultado 4 de octubre de 2021]. disponible en https://www.copnia.gov.co/tribunal-deetica/codigo-de-etica

Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. p. 1-15.

Ley 1273. Bogotá. (Enero 05 de 2005). Diario Oficial 47.223 de enero 05 de 2005. p. 1-6.

Ley 1341. Bogotá. (Julio 30 de 2009). Diario Oficial 47.227 de diciembre 31 de 2008. p. 1-30.

Ley 1480 de 2011 Bogotá. (Octubre 12 2011). Diario Oficial 48.220 de octubre de 12 de 2011. p. 1-11.

Ley 1581 de 2012.Bogotá. (Octubre 18 2012). Diario Oficial No. 48.587 de 18 de octubre de 2012. p. 1-188

Ley 1928 de 2018. Bogotá. (Julio 24 2018). Diario Oficial No. 50.664 de 24 de julio de 2018 de 24 de julio de 2018. p. 1-15

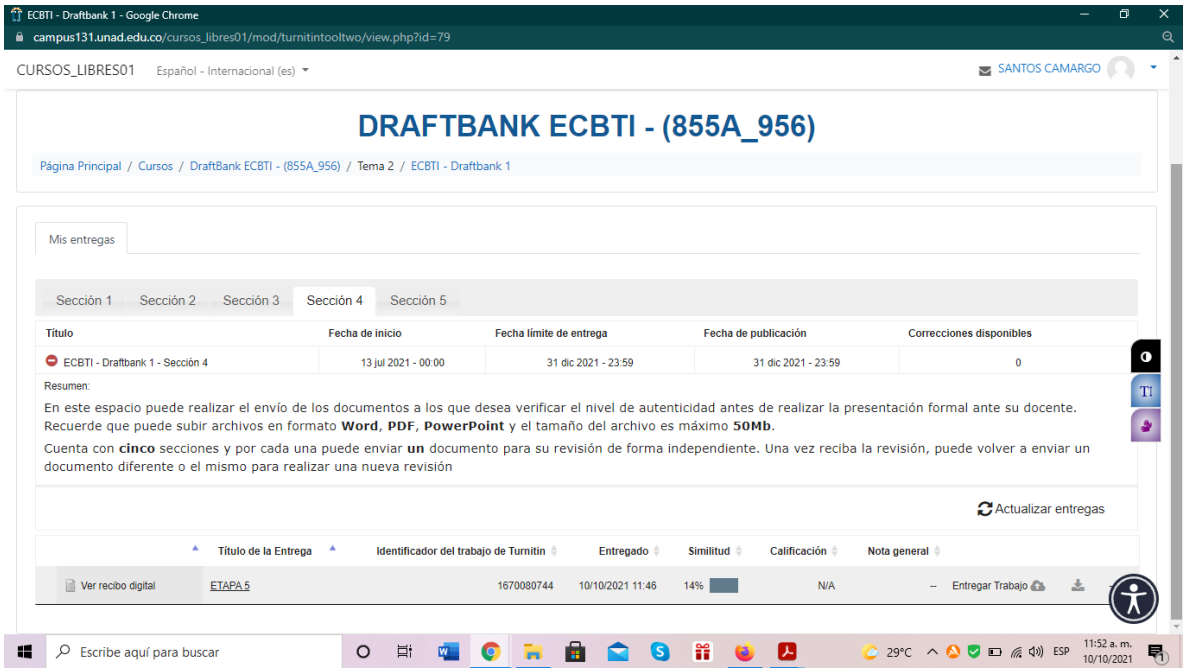
Morning Start Security «WhatWeb». [En línea] [consultado 4 de octubre de 2021]. disponible en (http://www.morningstarsecurity.com/research/whatweb)

OpenVAS. (s.f.). OpenVAS. [En línea] [consultado 4 de octubre de 2021]. disponible en https://www.openvas.org/

Red Team, Blue Team y Purple Team: funciones y diferencias». [En línea] [consultado 4 de octubre de 2021]. disponible en https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/.

SIEM: herramientas de registro y gestión de eventos.[En línea] [consultado 4 de octubre de 2021]. disponible en https://www.softhoy.com/conoce-puedes-hacer-herramientas-registro-gestion-eventos.html.

Snort - Network Intrusion Detection & Prevention System. [En línea] [consultado 4 de octubre de 2021]. disponible en https://www.snort.org/#get-started.
Upguard. [En línea] [consultado 4 de octubre de 2021]. disponible en https://www.upguard.com/blog/cve



Link Video

https://www.youtube.com/watch?v=rCZ3uBnaWF0