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

LUIS ARMANDO SAMACÁ TORRES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

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

LUIS ARMANDO SAMACÁ TORRES

Alexander Larrahondo N
Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

Amenaza: Según MINTIC21,son las causas o factores potenciales que pueden provocar daños dentro de una organización.

Blue Team: Equipo encargado de estudiar el comportamiento del sistema y de sus usuarios en una organización con el fin de identificar rápidamente cualquier incidente informático.

CVE: vulnerabilidades y exposiciones comunes, programa de intercambio de información entre diferentes herramientas y bases de datos, enlazando información de parches y soluciones aportadas por fabricantes[2].

Delito informático: Los delitos informáticos son todas aquellas acciones ilegales, delictivas o no autorizadas que hacen uso de dispositivos electrónicos.

Intrusión: Acceso no permitido de seguridad a un sistema.

Pentesting: Practica de atacar diversos entornos con el fin de identificar o vulnerabilidades.

Red Team: Equipo encargado de realizar los ataques informáticos con el fin de establecer los fallos en la infraestructura tecnológica de una determinada organización.

Vulnerabilidad: Debilidad o fallo en un sistema que pone en riesgo la seguridad de la información de una organización permitiendo a un atacante comprometer la integridad o disponibilidad.

---

[1] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 10]. (06 octubre de 2021). Seguridad y Privacidad de la Información. Guía para la preparación de las TIC para la continuidad del negocio. Bogotá, Colombia: MINTIC.p.3.

[2] CVE “CVE”. {En línea}. {06 octubre de 2021} disponible en: (https://cve.mitre.org/).

RESUMEN

De acuerdo con las actividades realizadas en el seminario de especialización equipos estratégicos en ciberseguridad red team & blue team se consolida un informe técnico donde se relacionan los planteamiento de escenarios y anexos que requieren ser analizados y brindar respuesta a sucesos dentro de la organización The Whitehouse Security en los cuales se requiere el montaje de banco de trabajo, análisis de la legislación “leyes, decretos” que existen actualmente y sus características principales, definición de las etapas de pentesting, prueba de penetración, herramientas de seguridad y contención de ataques informáticos.

INTRODUCCIÓN

En el siguiente informe técnico, se presenta la consolidación de los escenarios presentados en cada una de las etapas del seminario de especialización equipos estratégicos en ciberseguridad red team & blue team en las cuales se desarrolla el montaje de banco de trabajo, análisis de la legislación “leyes, decretos”, definición de las etapas de pentesting, prueba de penetración, herramientas de seguridad y contención de ataques informáticos.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

The WhiteHouse Security ha presentado problemas al interior de la organización por lo cual requiere deberá utilizar en una serie de escenarios y problemas complejos para que estos sean gestionados por el personal postulado que busca ser parte del equipo Blue Team.

1.2 FORMULACIÓN DEL PROBLEMA

The WhiteHouse security requiere por medio de una serie de preguntas orientadoras y el montaje del banco de trabajo seleccionar el personal idóneo para hacer parte del equipo de Red Team y Blue Team con el cual se busca identificar el conocimiento mediante los diferentes escenarios planteados, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

2. JUSTIFICACIÓN

El desarrollo del informe técnico consolida todas las fases en las cuales fueron realizadas las actividades que fueron enfocadas a los escenarios y anexos que estos contienen con el fin de brindar respuesta a las preguntas orientadoras y montaje de banco de trabajo para los postulados a los equipos Red Team y Blue Team.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar un informe técnico el cual consolide las fases desarrolladas en el seminario de especialización equipos estratégicos en ciberseguridad red team & blue team.

2.2 OBJETIVOS ESPECÍFICOS

Describir margen legal en Colombia sobre delitos informáticos, etapas de pentestig, herramientas de ciberseguridad y configurar banco de trabajo.

Evaluar las acciones de los equipos Red Team & Blue Team de The WhiteHouse Security en el marco de los criterios éticos y legales.

Demostrar vulnerabilidades en un sistema informático a partir técnicas de intrusión.

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en The WhiteHouse Security.

3 MARCO REFERENCIAL

Abarca los aspectos que fundamentan la investigación, por ejemplo: marco teórico, marco conceptual, marco legal, entre otros.

3.1 MARCO CONCEPTUAL

Seguridad informática

La seguridad informática en las organizaciones cada día preocupa más debido a los ataques cibernéticos que han puesto en riesgo su información, por lo cual es indispensable identificar y eliminar cualquier tipo de amenaza que genere pérdidas económicas en las organizaciones, por ello, se establecen normas, protocolos y políticas de seguridad informática[3]. La seguridad informática está básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas[4]

De acuerdo con lo indicado por Sitel[5] cuenta que “El 70 % de las pequeñas y medianas empresas son el objetivo de ciberataques para robar sus datos o usar su infraestructura para realizar todo tipo de actividades maliciosas. La limitación de recursos hace que los tiempos para detectar y responder a los ciberataques sean altos”.

Al hablar de seguridad informática en las organizaciones, entran dos equipos como son Red Team y Blue Team los cuales realizan tareas en conjunto con el fin de identificar vulnerabilidades y prevenir amenazas[6].

Red Team

Red Team es un equipo encargado de generar escenarios de amenazas (ataques cibernéticos) de manera controlada a los diferentes sistemas informáticos de una organización, desde el punto de vista de un atacante con el fin de entrenar el equipo de seguridad Blue Team y medir la respuesta oportuna a los ataques con los diferentes sistemas de seguridad[7]

---

[3] UNITEL “Seguridad Informática en las empresas. Consejos básicos”. {En línea}. {12 octubre de 2020} disponible en: (https://unitel-tc.com/seguridad-informatica-en-las-empresas-consejos/).

[4] Tarazona, Cesar “AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN”. {En línea}. {06 octubre de 2021} disponible en: (https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/.).

[5] SITEL “Gestión de la seguridad Blue Team”. {En línea}. {06 octubre de 2021} disponible en: (https://www.sistel.es/business-information-security/gestion-seguridad).

[6] UNIR, universidad en internet “Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?”. {En línea}. {06 octubre de 2021} disponible en: (https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/).

[7] UNIR, universidad en internet, op. cit,

Blue Team

Blue Team es un equipo encargado de predecir, prevenir, detectar y brindar respuesta adecuada a los ciberincidentes reales o simulados durante un periodo de tiempo significativo, con lo cual se mide su tiempo de detección y de recuperación, con esto, el equipo aprende a reaccionar y defenderse de diferentes ataques y situaciones variadas[8].

Vulnerabilidades

Empresas tanto públicas como privadas, utilizan recursos que son denominados como activos, los cuales se encuentran expuestos a las diferentes amenazas tanto a nivel interno como externo, estas pueden ser naturales, inducidas por el hombre, de manera accidental o deliberada[9].

Incibe[10] define que "las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas. El problema es que, en el mundo real, si existe una vulnerabilidad, siempre existirá alguien que intentará explotarla, es decir, sacar provecho de su existencia".

Ciberseguridad

De acuerdo a lo reportado por destinonegocio[11] indica que "Los ciberataques a las organizaciones medianas y pequeñas con frecuentes, esto dado que no poseen los recursos económicos necesarios por lo cual se convierten en punto de ataque por los ciberdelincuentes, cuando una organización se encuentra en su etapa de crecimiento no priorizan la seguridad informática y trabajan sobre sistemas desactualizados, equipos obsoletos, falta de implementación de nuevas tecnologías, personal capacitado que brinde una reacción inmediata sobre los ataques, de 5000 ataques, solo identifican el 56 % y el 41 % son irremediables".

---

[8] EC-COUNCIL, Blog "RED TEAM VS BLUE TEAM". {En línea}. {06 octubre de 2021} disponible en: (https://blog.eccouncil.org/red-team-vs-blue-team/).

[9] SGSI "ISO 27001: Vulnerabilidades de la organización". {En línea}. {07 octubre de 2021} disponible en: (https://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/#:~:text=Las%20vulnerabilidades%20pueden%20encontrase%20asociadas,%2C%20equipos%2C%20software%20o%20informaci%C3%B3n.&text=Falta%20de%20aplicaci%C3%B3n%20de%20procedimientos,Fallos%20del%20control%20interno.).

[10] INCIBE_ "Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?". {En línea}. {07 octubre de 2021} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

[11] DESTINONEGOCIO "¿Cómo evitar un ciberataque en las empresas?". {En línea}. {07 octubre de 2021} disponible en: (https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/ciberataque/).

3.2 MARCO LEGAL

La información de las organizaciones y personas actualmente suelen ser almacenadas en bases de datos electrónicas lo cual ha provocado el nacimiento de diferentes delitos informáticos con fines lucrativos o mal intencionados[12].

A continuación, se relaciona la legislación sobre delitos informáticos y protección de datos personales que impacta en los equipos Red Team y Blue Team donde se mencionan normativas gubernamentales, estándares y metodologías.

3.2.1 Normativas Gubernamentales

LEY 1273 DE 2009

La ley 1273 de 2009 judicializa de manera penal la intrusión, obstaculización, manipulación, interceptación, daños, instalación de software malicioso, suplantación y extracción de información sobre los diferentes sistemas informáticos, los cuales afecten de alguna manera a personas u organizaciones que atenten contra su integridad, confidencialidad y disponibilidad. Está compuesta por los siguientes artículos:

- Artículo 269A
- Articulo 269B
- Articulo 269D
- Articulo 269E
- Articulo 269H

Los delitos más comunes en Colombia son hurto por medios informáticos, violación de datos personales, acceso abusivo a sistema informático, transferencia no consentida de activos y uso de software malicioso[13].

- Ley 1266 de 2008. Distinguida como la ley de hábeas data y del manejo de la información contenida en bases de datos personales.

- Ley 1581 de 2012. En esta norma se dictan disposiciones generales para la protección de datos personales.

- 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

[12] Chaparro, Maria. “Legislación informática y protección de datos en Colombia, comparada con otros países”. {En línea} {07 octubre de 2021} disponible en: (file:///C:/Users/Samakinho/Downloads/1014-Texto%20del%20art%C3%ADculo-2757-1-10-20150430.pdf).

[13] MINTIC, “Ley 1273 de 2009”. {En línea} {07 octubre de 2021} disponible en: (https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).

Información y las Comunicaciones –TIC– se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

4 DISEÑO METODOLÓGICO

En el desarrollo del informe técnico correspondiente al seminario, se genera el siguiente diseño metodológico:

La metodología es diseñada en 4 fases en las cuales se brinda información correspondiente a las escenarios y análisis de los anexos con el fin de brindar respuesta a las preguntas orientadoras establecidas en el seminario de especialización equipos estratégicos en ciberseguridad red team & blue team.

Tabla 1. Metodología para análisis, consulta, procesos y procedimientos.

Fase	Actividad
I. Conocimiento	Mediante el análisis de las actividades establecidas en los escenarios del seminario.
II. Interpretación	Se identifica y clasifica la información consultada después de realizar análisis de las actividades y anexos para llevar a cabo el desarrollo de los objetivos.
III. Análisis	Se analiza la documentación suministrada en el seminario para llevar a cabo el desarrollo de los objetivos establecidos en el seminario.
IV. Diseño	Se realizaron los siguientes pasos: Describir margen legal en Colombia sobre delitos informáticos, etapas de pentestig, herramientas de ciberseguridad y configurar banco de trabajo. Evaluar las acciones de los equipos Red Team & Blue Team de The WhiteHouse Security en el marco de los criterios éticos y legales. Demostrar vulnerabilidades en un sistema informático a partir técnicas de intrusión. Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en The WhiteHouse Security.

Fuente 2. HERRERA M. Haroldo E. https://www.gestiopolis.com/metodologia-paraevaluacion-diagnostico-y-diseno-de-procesos/.

5 DESARROLLO DE LOS OBJETIVOS

5.1 DESCRIBIR MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS, ETAPAS DE PENTESTIG, HERRAMIENTAS DE CIBERSEGURIDAD Y CONFIGURAR BANCO DE TRABAJO.

Margen Legal en Colombia

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales existen dos leyes las cuales se relacionan a continuación:

- LEY 1581 DE 2012 – Decreto 1377 de 2013:

Como lo menciona Mintic[14], es la ley de protección de datos personales que tiene como finalidad proteger la información confidencial de los ciudadanos registrada en bases de datos o archivos, ésta es regulada por la superintendencia de industria y comercio, brinda el derecho de conocer, actualizar y verificar el tratamiento que brindan a los datos personales recolectados, garantizando que estos no sean divulgados sin previo conocimiento o autorización.

Esta ley está compuesta por 28 artículos en los cuales se dictan disposiciones generales para la protección de datos personales

- LEY 1273 DE 2009:

Como lo especifica la Sic[15], Es la ley que trata sobre las penas relacionadas a delitos informáticos, de la protección de la información y de los datos, está compuesta por los artículos 269A al 269J, el incurrir en alguna de estas faltas puede llevar a pagar penas de prisión hasta de 120 meses y 1500 salarios mínimos, dentro de estas faltas se encuentran la suplantación de sitios web, uso de software malicioso, violación de datos personales, entre otros.

ETAPAS DE UN PENTESTING:

[14] MinTic, “Ley 1581 de 2012”. {En línea}. {07 octubre de 2021} disponible en: (https://www.mintic.gov.co/arquitecturati/630/articles-9011_documento.pdf).
[15] Sic, “LEY 1273 DE 2009”. {En línea}. {07 octubre de 2021} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

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.
De acuerdo con lo mencionado por la revista Hacking Ético[16], un pentesting es la manera en la cual se mide la seguridad informática de una organización (auditoria) aplicando técnicas de hackeo de una manera legal y bajo aprobación de las empresas, está compuesto por 7 fases las cuales se describen a continuación:

- Fase de Contacto:

  Es la fase donde se tiene contacto entre el auditor y el cliente, quienes acuerdan costos, tipo de test, fechas, reportes e información requerida para brindar inicio a las pruebas correspondientes.

- Fase de recolección de información:

  En esta fase se inicia con el proceso de recolección de información del objetivo, como dominios, tipos de sistemas con el fin de ir perfilando el ataque. Se puede hacer uso de herramientas como OSINT o Google Hacking.

- Fase de Análisis de Vulnerabilidades:

  Se realiza análisis para identificar las posibles vulnerabilidades sobre el objetivo con la información previamente recolectada, validando cual puede ser el vector de ataque mas efectivo. Se pueden identificar vulnerabilidades mediante herramientas como KaliLinux, OpenVAS y NMAP.

- Fase de modelado de amenaza:

  Con la información recolectada y vulnerabilidades identificadas, se perfila y estructura el ataque a realizar hacia el objetivo.

- Fase de explotación:

  De acuerdo con el modelo diseñado y estructura de la amenaza, se procede a realizar la explotación de las vulnerabilidades, este proceso puede ser realizado mediante herramientas como Metasploit Framework.

[16] Revista HackingEtico, “FASES DEL PENTESTING Aprende Como Hacer Auditoria De HACKING A Empresas”. {En línea}. {07 octubre de 2021} disponible en: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html).

- Fase de Post-explotación:

  En esta fase se evidencia el acceso a los sistemas en los cuales se ha obtenido privilegios, recolectando información como archivos alojados en servidores, demostrando que una persona con malas intenciones podría implantar troyanos o keylogger con finalidades malintencionadas.

- Fase de Informe:

  Se procede con la generación de informes técnicos y ejecutivos con el fin de brindar la información detallada de vulnerabilidades encontradas y soluciones para que estas sean mitigadas.

HERRAMIENTAS DE CIBERSEGURIDAD:

• Metasploit: De acuerdo con lo mencionado por Catoira[17], es un conjunto de herramientas de código abierto para probar las vulnerabilidades de sistemas informáticos mediante el desarrollo o ejecución de exploits, puede ser instalado en sistemas operativos Windows o Linux, adicional a ello, se encuentra integrado en Kali Linux el cual es muy utilizado para pruebas de penetración.

• Nmap: Como dice menciona NMAP[18], es una herramienta de código abierto disponible para sistemas operativos Windows, Linux y Mac OS X, el cual tiene como función el descubrimiento de redes y auditoria de seguridad, puede ser utilizado para identificar hosts disponibles en una red, puertos habilitados, descubrir nombres y versiones de aplicaciones instaladas en los hosts mediante diferentes combinaciones de comandos.

• OpenVas: Es una herramienta para la detección, análisis, gestión y escaneo de vulnerabilidades de seguridad sobre sistemas informáticos y se puede encontrar en diferentes distribuciones de Linux como Kali Linux[19].

[17] Catoira, Fernando, “PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: EXPLOTANDO UNA VULNERABILIDAD CON METASPLOIT FRAMEWORK”. {En línea}. {07 octubre de 2021} disponible en: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html).

[18] NMAP, “Escáner de seguridad de Nmap”. {En línea}. {07 octubre de 2021} disponible en: (https://nmap.org/).

[19] INFOSEC, Industries. “OpenVAS / Greenbone Community Edition”. {En línea}. {07 octubre de 2021} disponible en: (https://infosecindustries.com/vendors/greenbone/openvas-greenbone-community-edition.html).

Servicios en línea:

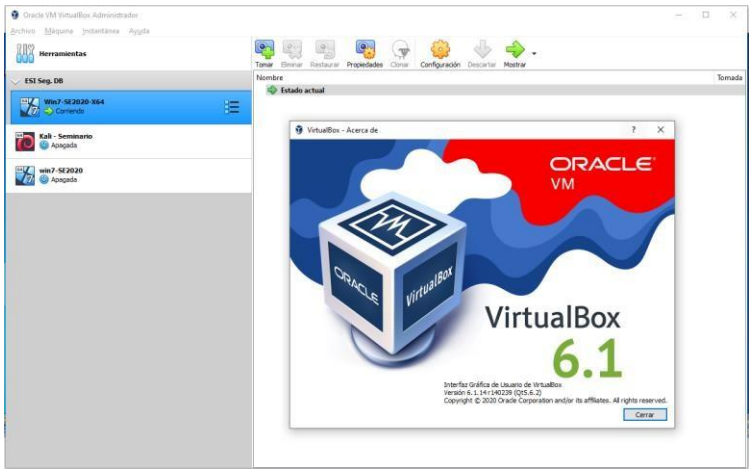
• ExploitDB: Mantenida por Offensive Security, es una base de datos de exploit con un archivo compatible con CVE que contiene exploits públicos y el software vulnerable afectado, es utilizado para investigar vulnerabilidades o pruebas de penetración.

• CVE: Identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas públicamente, las vulnerabilidades son descubiertas y publicadas por organizaciones de todo el mundo con el fin trabajar de manera conjunta y abordar las vulnerabilidades.

CONFIGURACIÓN BANDO DE TRABAJO:

- Se realiza descarga e instalación de VirtualBox 6.1 la cual corresponde a su última versión.

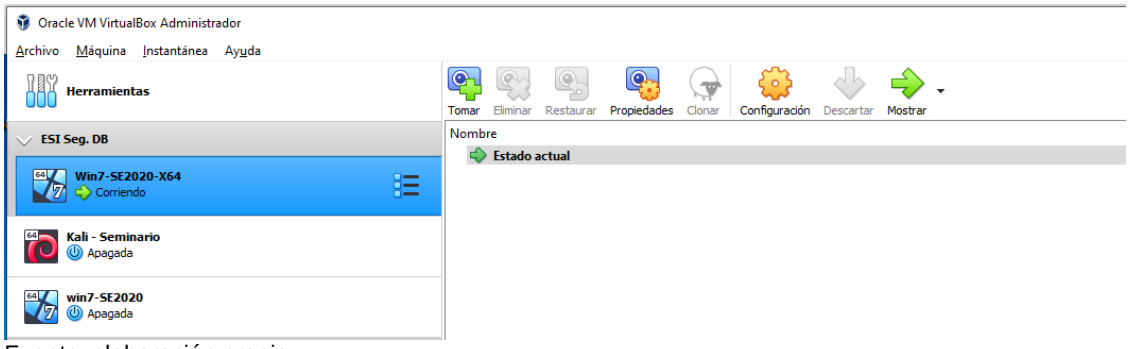
Figura 1. VirtualBox 6.1



Fuente: elaboración propia.

- Se descargan e importan imágenes en formato OVA de acuerdo con el requerimiento para el banco de trabajo.

Figura 2. OVAS.

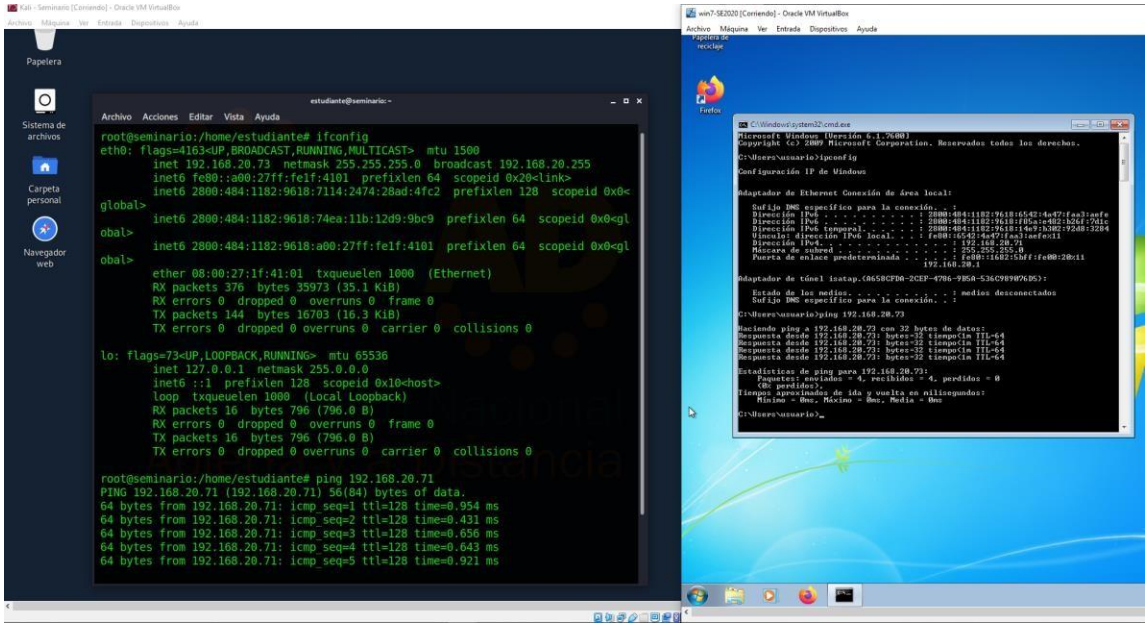


Fuente: elaboración propia.

- Validación de comunicación entre maquinas del banco de trabajo:

La máquina virtual de Kali Linux tiene un IP local 192.168.20.73 y la maquina Windows 7 de 32 Bits tiene una IP local 192.168.20.71.

Figura 3. Conectividad Máquinas virtuales.

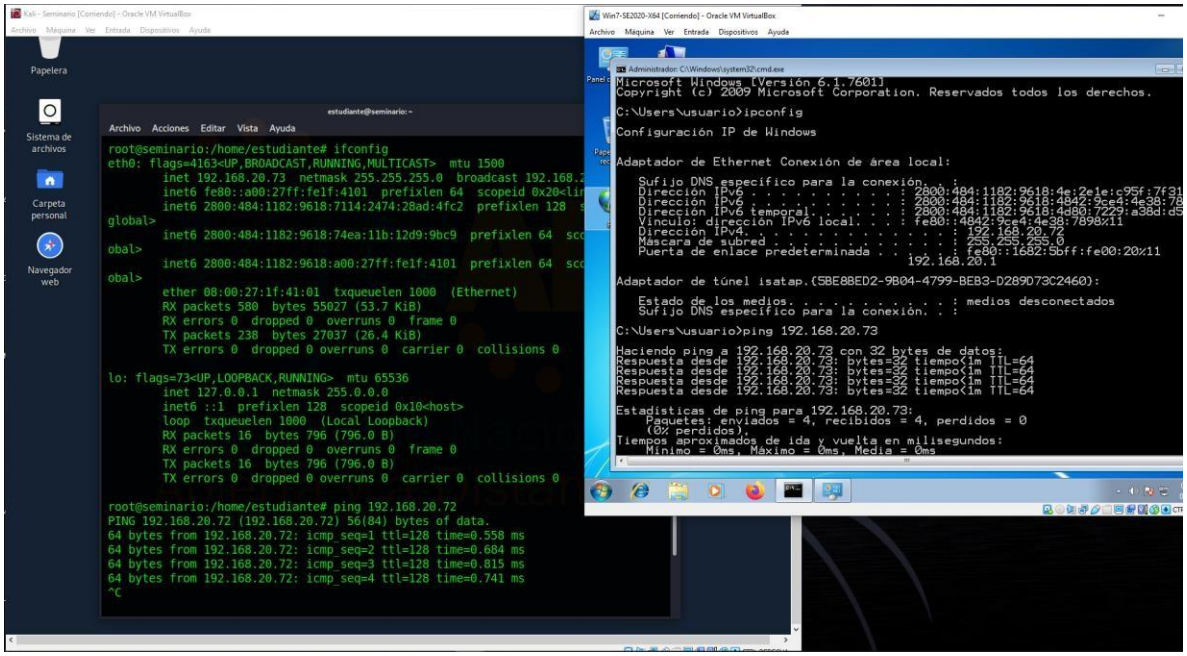


Fuente: elaboración propia.

Se evidencia ping de respuesta en los dos sentidos.

La máquina virtual de Kali Linux tiene un IP local 192.168.20.73 y la maquina Windows 7 de 64 Bits tiene una IP local 192.168.20.72.

Figura 4. Conectividad Máquinas virtuales Kali – Windows 7.

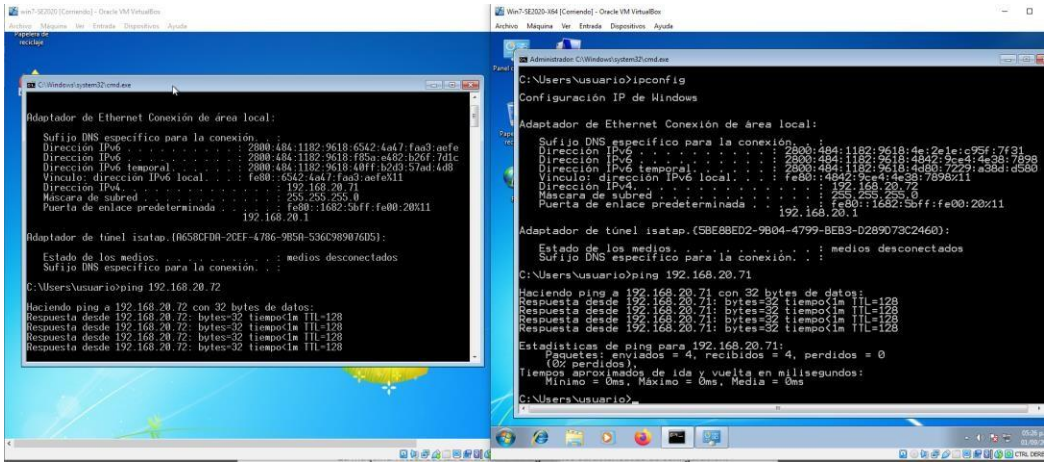


Fuente: elaboración propia.

Se evidencia ping de respuesta en los dos sentidos.

La máquina virtual Windows 7 de 64 Bits tiene una IP local 192.168.20.72 y la maquina Windows 7 de 32 Bits tiene una IP local 192.168.20.71.

Figura 5. Conectividad Máquinas Windows 7 32 Bits y Windows 7 64 Bits.



Fuente: elaboración propia.

Se evidencia ping de respuesta en los dos sentidos.

- Configuración de Banco de Trabajo:

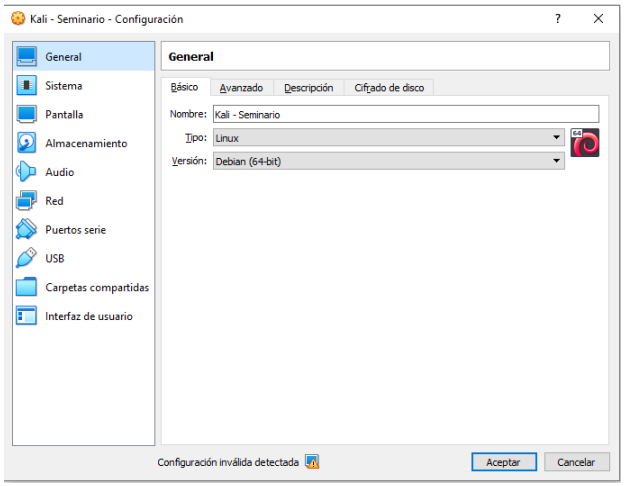
El banco de trabajo se encuentra conformado por 3 máquinas virtuales, una con el sistema operativo Kali Linux y las otras dos con Windows 7 de 32 y 64 bits.

La máquina virtual de Kali Linux tiene las siguientes características de configuración:

Sistema Operativo:

Linux Versión Debian de 64 Bits.

Figura 6. Kali Linux.

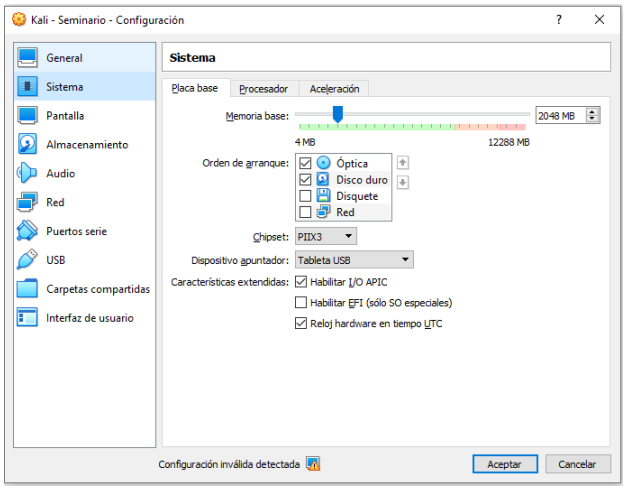


Fuente: elaboración propia.

Memoria:

Configuración de memoria de 2048 MB

Figura 7. kali Linux - Memoria.

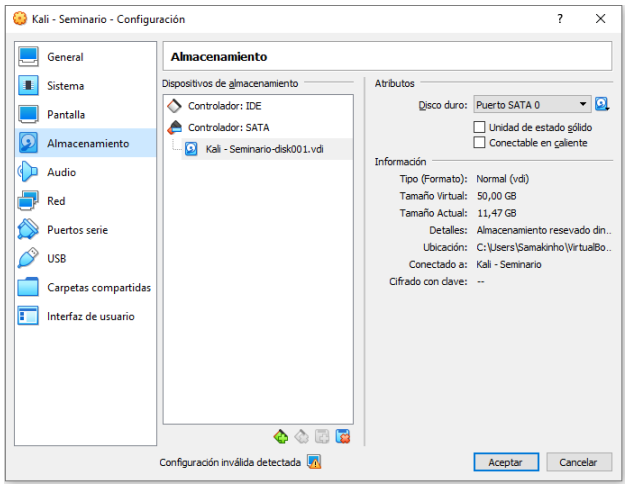


Fuente: elaboración propia.

Almacenamiento:

Configuración de disco duro de 50 GB.

Figura 8. Kali Linux - Almacenamiento.

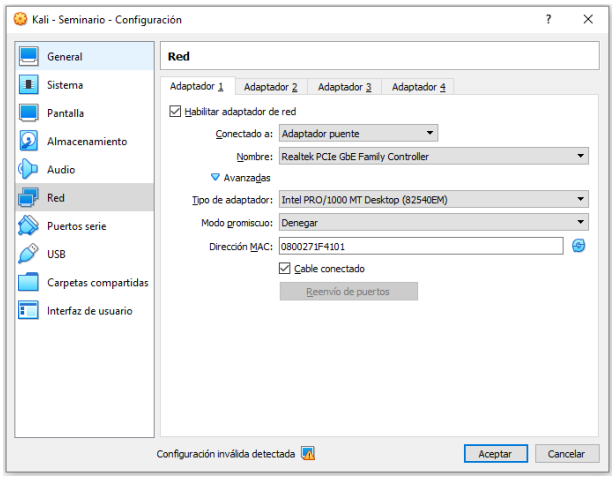


Fuente: elaboración propia.

Red:

Configuración de red – Adaptador Puente.

Figura 9. Kali Linux - Red.



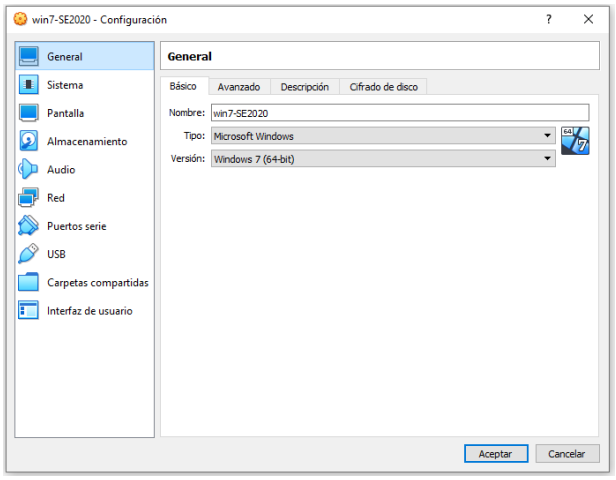
Fuente: elaboración propia.

Las máquinas virtuales de Windows 7 de 32 y 64 bits tienen las siguientes características de configuración:

Sistema Operativo:

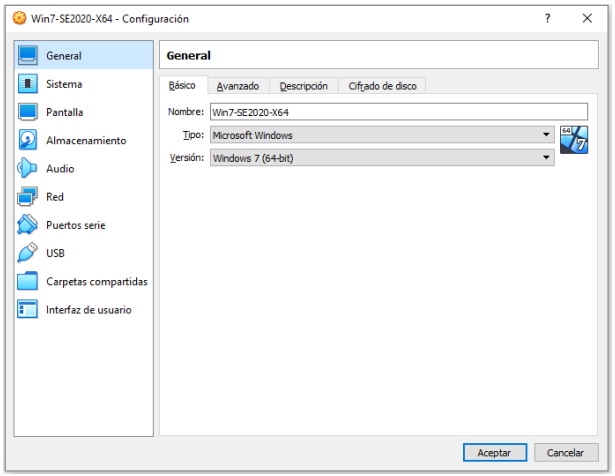
Windows 7 de 32 y 64 Bits.

Figura 10. Windows 7 - 32 Bits.



Fuente: elaboración propia.

Figura 11. Windows 7 - 64 Bits.

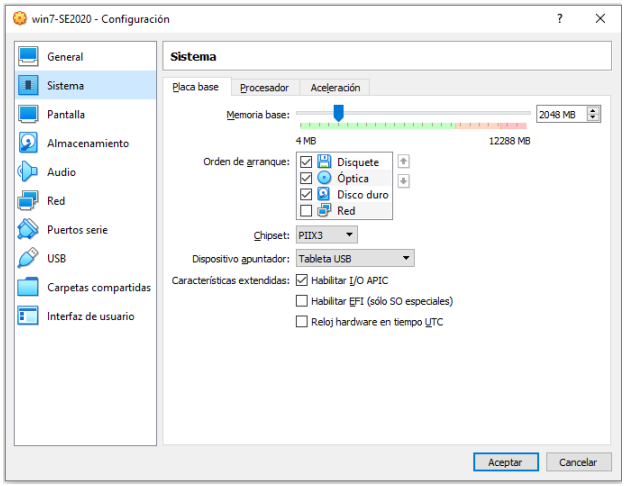


Fuente: elaboración propia.

Memoria:

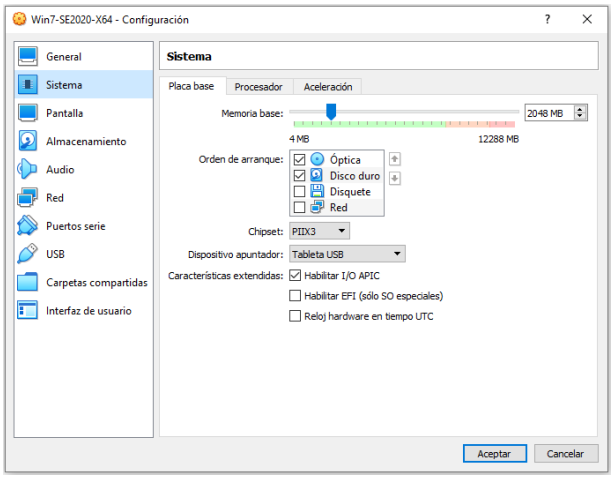
Configuración de memoria de 2048 MB

Figura 12. Windows 7 - 32 Bits - Memoria.



Fuente: elaboración propia.

Figura 13. Windows 7 - 64 Bits - Memoria.

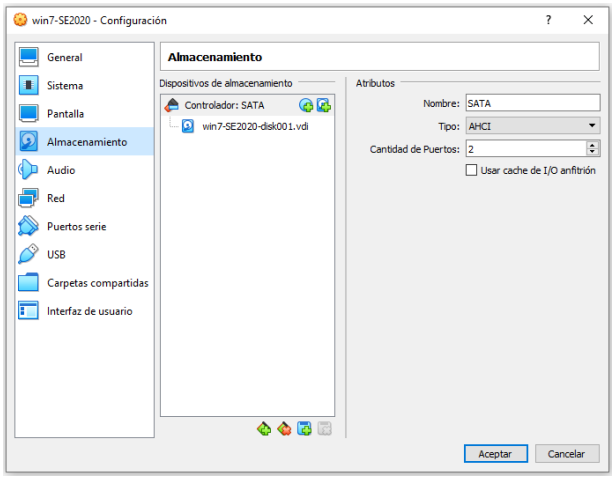


Fuente: elaboración propia.

Almacenamiento:

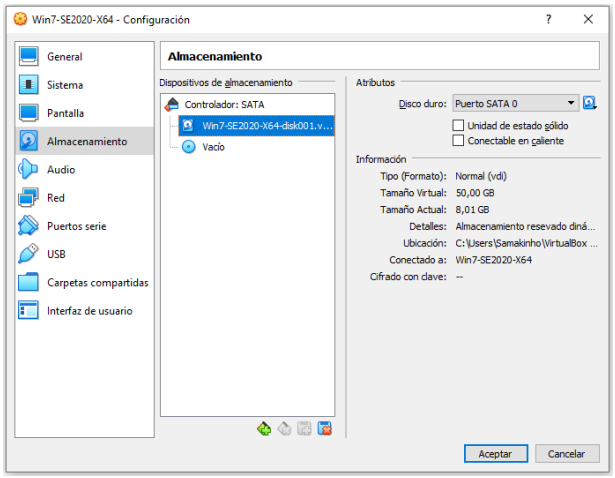
Configuración de disco duro de 50 GB.

Figura 14. Windows 7 - 32 Bits – Disco Duro.



Fuente: elaboración propia.

Figura 15. Windows 7 - 64 Bits – Disco Duro.

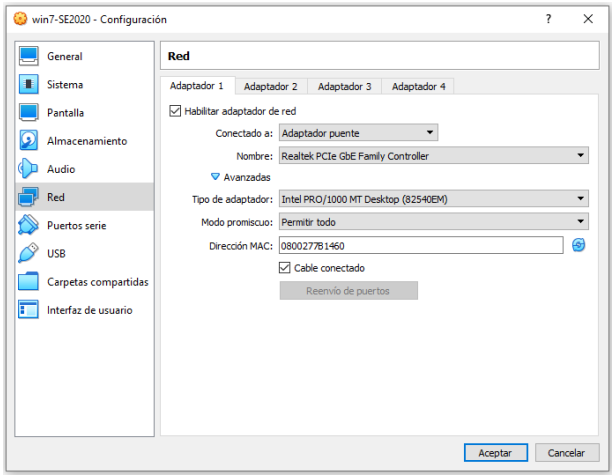


Fuente: elaboración propia.

Red:

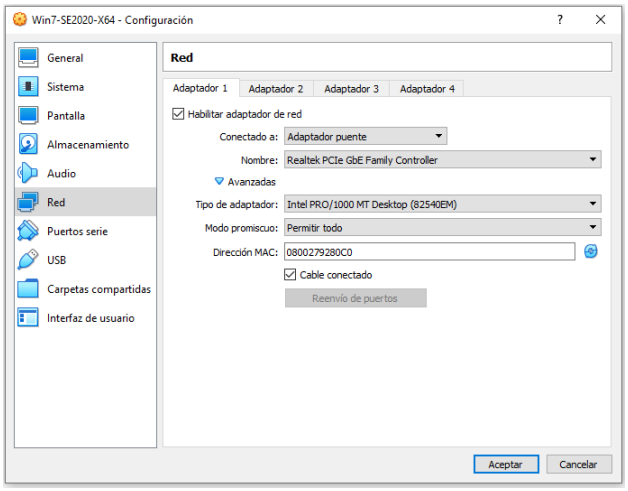
Configuración de red – Adaptador Puente.

Figura 16. Windows 7 - 32 Bits – Adaptador de red - Puente.



Fuente: elaboración propia.

Figura 17. Windows 7 - 64 Bits – Adaptador de red - Puente.

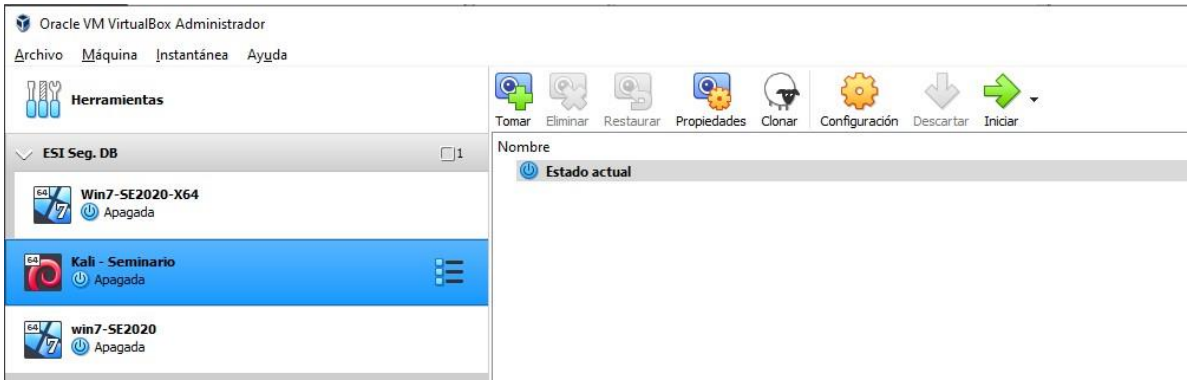


Fuente: elaboración propia.

Esquema completo del banco de trabajo:

Se resume en VirtualBox la configuración del banco de trabajo con los equipos requeridos y con conectividad para los laboratorios a desarrollar.

Figura 18. Esquema de Banco de Trabajo.



Fuente: elaboración propia.

5.2 EVALUAR LAS ACCIONES DE LOS EQUIPOS RED TEAM & BLUE TEAM DE THE WHITEHOUSE SECURITY EN EL MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES.

1. Análisis de los anexos Escenario 2 y Acuerdo desde el punto de vista legal y no ético.

En el Anexo 3 – Acuerdo, se encuentran procesos ilegales y no éticos los cuales son irregulares y deja en evidencia que la organización Whitehouse Security realiza actividades sospechosas que vulneran algunos artículos de la ley 1273 de 2009.

Se relacionan clausulas y fragmentos que presentan irregularidades:

Primera Clausula: Objeto:

Sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

(En este fragmento especifican que los procesos ilegales que maneja la organización no podrán ser divulgados).

Segunda Clausula: Definición de información confidencial:

Punto 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”.

(Especifican chuzadas e interceptación y accesos abusivos a sistemas).

Cuarta. Obligaciones de la parte receptora:

Punto 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

(Informan no reportar a las autoridades actividades sospechosas).

Punto 4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

(No generar ningún tipo de denuncia con respecto a la información ilegal que se maneje en las reuniones).

Punto 7. Responder por el mal uso que le den sus representantes a la información confidencial.

(Asumir responsabilidades por el mal uso que brinden a la información confidencial los representantes que también puede ser la misma organización).

Punto 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.

(Asumir responsabilidades legales de la información que se encuentre en el poder del responsable).

Punto 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.

(No divulgar información ilegal sin previo aviso por escrito a la organización).

Octava. Solución de controversias:

En caso de que la información ilegal o confidencial 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.

(La organización no brinda las garantías de responsabilidad de la información o procesos ilegales que pueden llegar a manejar).

2. **Análisis de los anexos, en relación con la vulneración de la ley 1273 argumentando cualquier proceso ilegal.**

De acuerdo con los procesos ilegales encontrados en el Anexo 3 - acuerdo, se mencionan los artículos de la ley 1273 de 2009[20] los cuales podrían ser vulnerados:

Artículo 269A: Acceso abusivo a un sistema informático. prisión de 48 meses a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: Interceptación de datos informáticos, penas de prisión de 36 a 72 meses.

Como se menciona en el Anexo 3 – acuerdo, en la segunda Clausula: Definición de información confidencial datos, habla de datos secretos como chuzadas, interceptación de información y acceso abusivo a lo cual requiere de una orden judicial que al ser estos vulnerados genera penas de prisión que son mencionadas en los artículos anteriormente informados.

3. **Análisis de la propuesta laboral, teniendo presente en cuenta la revisión desde el punto de vista legal y ético.**

Aunque la oferta laboral ofrece un gran salario y un contrato atractivo, después de analizado el Anexo 3 – Acuerdo, se presentan procesos irregulares los cuales no son óptimos para aplicar al trabajo, dado que bajo el código de ética para ingenieros se encuentran deberes generales que como lo menciona COPNIA[21] en sus artículos 30 y 32 el profesional debe denunciar los delitos, contravenciones con ocasión del ejercicio de su profesión aportando todo tipo de información y pruebas, adicional a ello, recibir gratificaciones en razón del ejercicio de la profesión que como se evidencia en la oferta laboral están siendo representadas en el salario y tipo de contrato.

4. **Análisis del caso “OPERACIÓN ANDROMEDA BUGGLY” desde su posición teniendo en cuenta los aspectos legales y éticos.**

[20] SIC, “LEY 1273 DE 2009”. {En línea}. {07 octubre de 2021} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

[21] COPNIA, “Código de Ética”. {En línea}. {07 octubre de 2021} disponible en: (https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf).

De acuerdo con lo mencionado por Enter.co[22] en su artículo, en la fachada Andrómeda se realizaron actividades ilícitas las cuales no tenían ningún tipo de orden judicial como interceptación de comunicaciones y uso de software malicioso para obtener información de personas, lo cual es una falta grave que sanciona la ley 1273 de 2009 en sus artículos 269A, 269C, 269D, 269F y 269H. A pesar de que eran actividades patrocinadas por fuerzas militares, no se tenía un control legitimo sobre todo lo que se realizaba en dicha fachada afectando el código de ética tanto militares como hacia la ciudadanía y el estado.

5.3 DEMOSTRAR VULNERABILIDADES EN UN SISTEMA INFORMÁTICO A PARTIR TÉCNICAS DE INTRUSIÓN.

Fase 1:

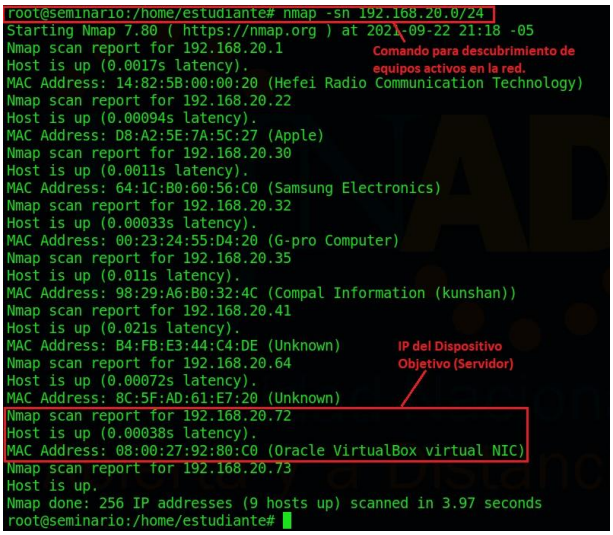
Dentro de la recopilación de la información, se tiene en cuenta las observaciones que se encuentran en el Anexo 4 – Escenario 3 donde se identifica un sistema operativo obsoleto y la versión del software rejetto v. 2.3 que presenta la vulnerabilidad.

Fase 2:

Haciendo uso de KaliLinux, se realiza el descubrimiento de los dispositivos activos en la red con la herramienta **NMAP**, que mediante el escaneo con el comando **nmap -sn 192.168.20.0/24** muestra todos los dispositivos conectados a la red y con el comando **nmap -sV -O -v** se identifica el sistema operativo, software instalado con la versión y puertos abiertos del objetivo. Con ello se identifican las vulnerabilidades y posibles ventores de ataque. Ver figura1, figura 2 y figura 3.

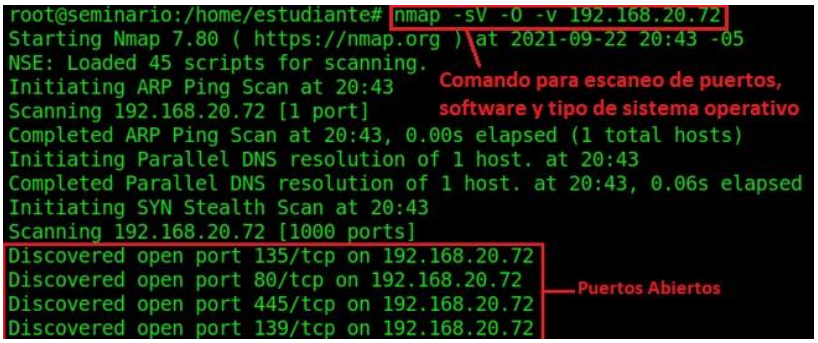
[22] ENTER.CO, “Detrás de Buggly: la historia de la fachada Andrómeda”. {En línea}. {08 octubre de 2021} disponible en: (https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/).

Figura 19. Escaneo red local.



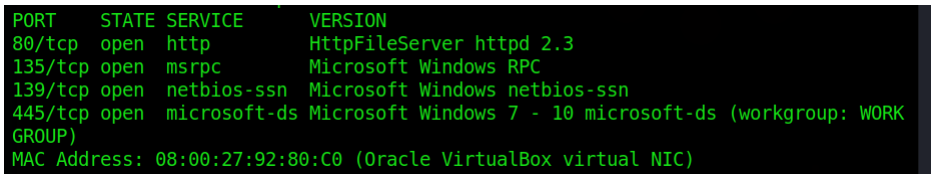
Fuente: elaboración propia.

Figura 20. Escaneo software y versiones.



Fuente: elaboración propia.

Figura 21. Puertos y Versiones.



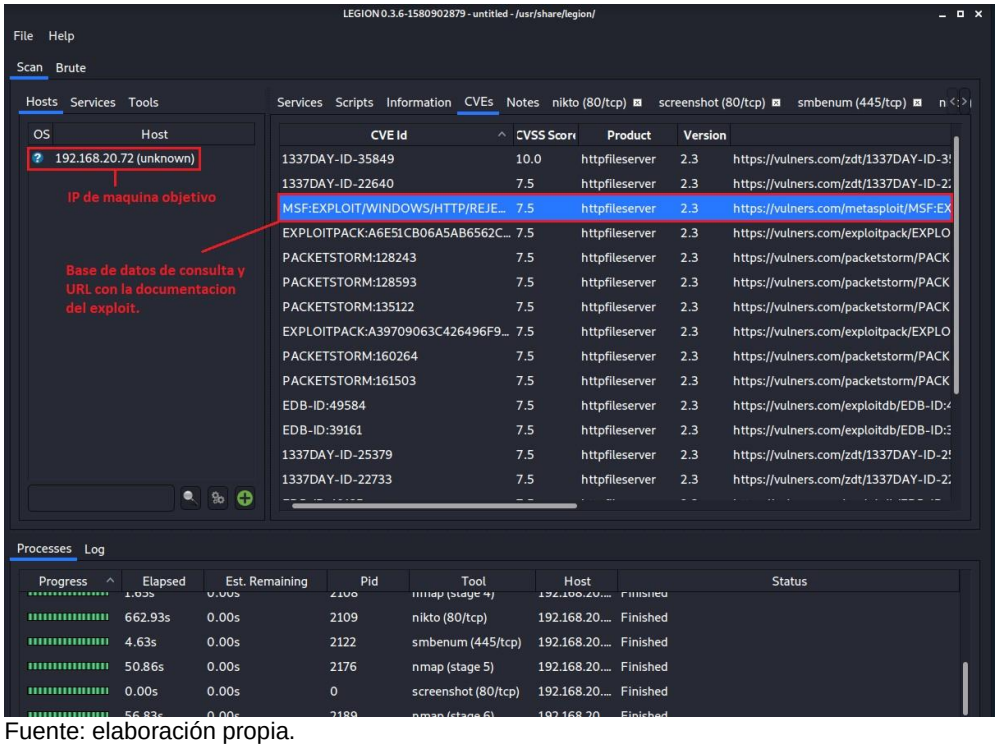
Fuente: elaboración propia.

A continuación, se relacionan los datos e información la cual ayudó a identificar el fallo de seguridad:

- Software rejetto v. 2.3 dado que tiene asociado un exploit el cual se encuentra publicado y donde se encuentra el procedimiento de como explotar esta vulnerabilidad.
- Fuga de información, esto relaciona a que existe perdida de información por conexiones externas.
- Escalamiento de privilegios lo cual indica que existe un usuario con privilegios suficientes para realizar modificaciones o ajustes sobre el sistema.
- Sistema operativo Windows 7 el cual es obsoleto y presenta múltiples vulnerabilidades.

Se hace uso de la herramienta LEGION y NAMP las cuales se encuentran en Kali Linux y se realiza el análisis de vulnerabilidades de la maquina objetivo, donde se evidencia la falla de seguridad y exploit que tiene el software rejetto v. 2.3.

Figura 22. Legion.



Fuente: elaboración propia.

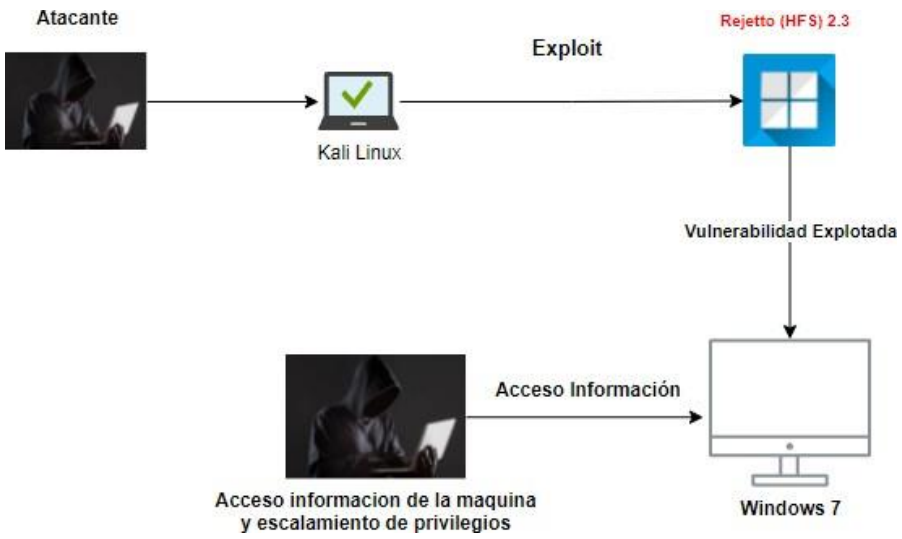
La aplicación rejetto v. 2.3 hace uso del puerto 80.

Mediante el escaneo de puertos y vulnerabilidades con NMAP y LEGION, se encuentran exploits disponibles en la maquina Windows 7 como lo evidencia

en la figura 4, con las cuales se procede a realizar su explotación con Metasploit Framework haciendo uso de los payloads disponibles, esto genera que la maquina quede expuesta por estas vulnerabilidades y pueda existir un escalamiento de privilegios donde se puede presentar secuestro de información, instalación de keylogger o malware.

En la figura 23, se explica el ataque a la vulnerabilidad identificada en la maquina Windows 7 de 64 bits.

Figura 23. Ataque.



Fuente: elaboración propia.

Paso 1.

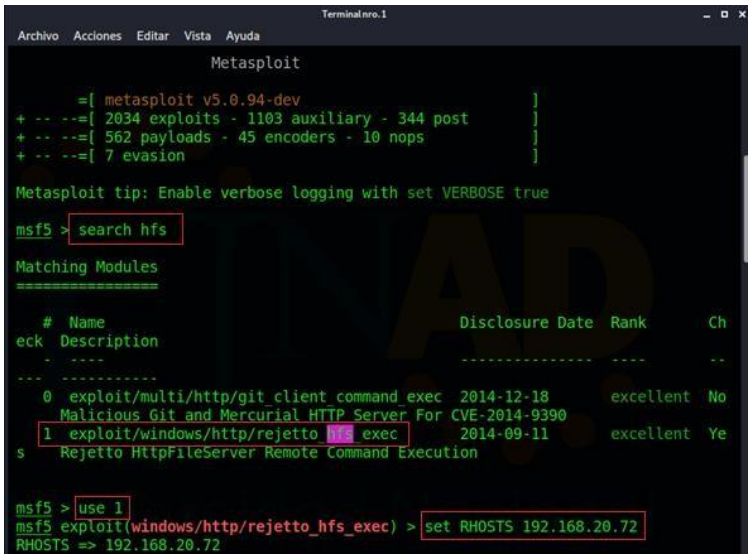
Se ejecuta la aplicación Metasploit Framework la cual se encuentra integrada en Kali Linux para iniciar la explotación de la vulnerabilidad identificada.

Paso 2.

Como se muestra en la figura 6, se ejecuta el comando **search hfs** para la identificación del exploit.

Después de identificado el exploit, se hace uso de este ejecutando el comando **use 1** y se carga el IP del objetivo con el comando **set RHOST 192.168.20.72**.

Figura 24. Search hfs.

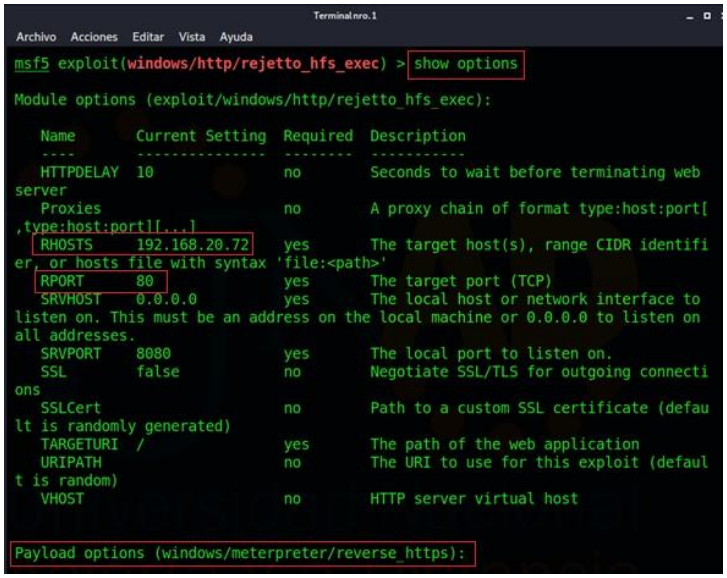


Fuente: elaboración propia.

Paso 3.

Al cargar el IP objetivo, con el comando **show options** se muestran las opciones del exploit (ver figura 7).

Figura 25. Opciones exploit.



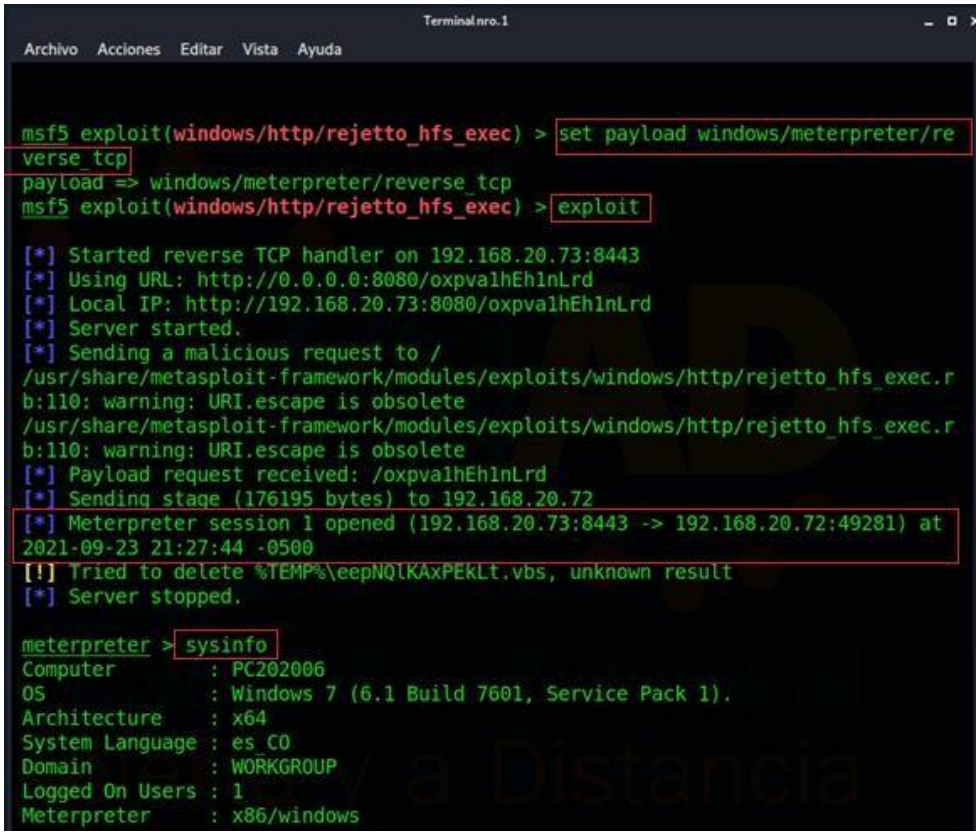
Fuente: elaboración propia.

Paso 4.

Se carga el payload con el comando **set payload Windows/emterpreter/reverse_tcp** y se ejecuta el comando **exploit** con el cual se inicia la explotación de la vulnerabilidad que en el proceso hace apertura de una Shell meterpreter y brinda el acceso a la maquina objetivo. (ver figura 7).

Al iniciar la Shell meterpreter y ejecutar el comando **sysinfo**, se puede identificar que brinda información de la máquina que está siendo explotada como el tipo de sistema operativo, arquitectura y dominio. (ver figura 7).

Figura 26. Payload y shell.



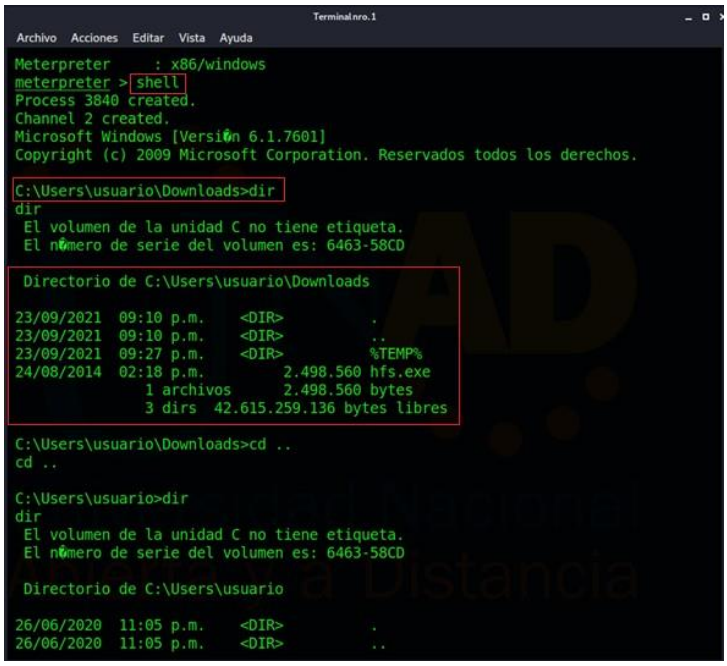
Fuente: elaboración propia.

Paso 5.

Al ejecutar el comando **Shell** en meterpreter, accede a la consola de comandos CMD de la maquina objetivo en la cual se puede realizar cualquier tipo de proceso

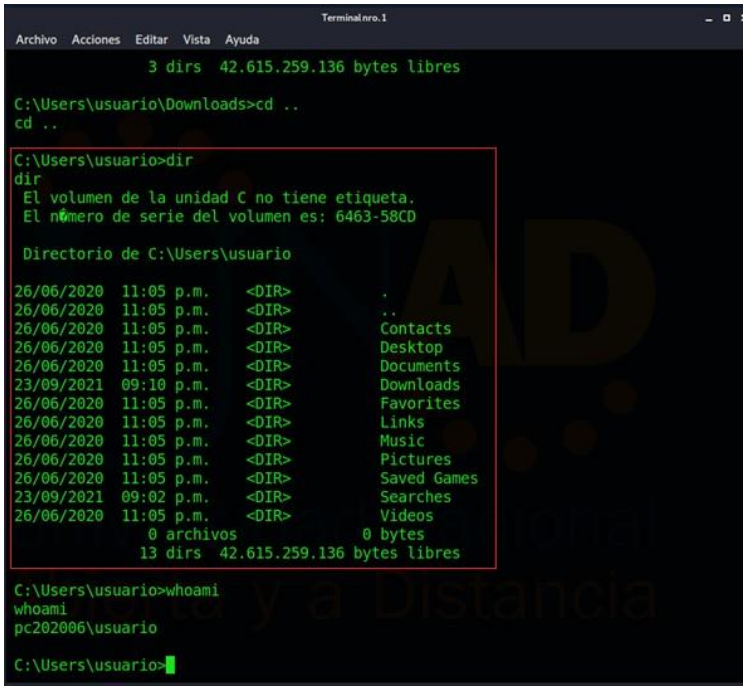
en el sistema o sobre la información que la maquina pueda tener lo que facilita fuga de información. (ver figuras 8 y 9).

Figura 27. Shell consola.



Fuente: elaboración propia.

Figura 28. CMD objetivo.



Fuente: elaboración propia.

Paso 6.

Con el comando **getsystem** en meterpreter, se realiza el proceso de escalamiento de privilegios donde se accede con el usuario **NT AUTHORITY\SYSTEM** y se crea el usuario **luissamaca** con privilegios de administrador. (ver figura 10).

Figura 29. Escalamiento de privilegios.

Fuente: elaboración propia

Se evidencia la creación de un usuario administrador con el escalamiento de privilegios. (ver figura 11).

Figura 30. User admin.

Fuente: elaboración propia

5.4 FORMULAR ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN THE WHITEHOUSE SECURITY.

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

   - Contener el ataque de manera rápida realizando escaneo, análisis y monitoreo de dispositivos y red interna identificando las posibles vulnerabilidades que fueron explotadas.

   - Determinar el alcance que tuvo el ataque teniendo presente dispositivos, equipos y software que pudieron estar involucrados aislándolos de la red.

   - Corregir las vulnerabilidades que hayan sido identificadas.

   - Restablecer el servicio en dado caso que haya sido afectada la continuidad del negocio.

   - Denunciar ante las autoridades competentes de delitos informáticos.

   - Proponer mejoras continuas para reforzar la seguridad de la infraestructura.

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

   Las medidas a proponer para evitar que este tipo de ataques se repitan son las siguientes:

   - Actualizar y parchar el sistema operativo hasta una versión la cual brinde las garantías de seguridad necesarias, para este caso, Windows 7 es un sistema operativo obsoleto el cual no cuenta con actualizaciones recientes lo cual convierte al sistema operativo vulnerable a la explotación.

   - Actualizar el software rejetto v. 2.3 a la versión más resiente que brinde las garantías de seguridad para su uso o en su defecto utilizar un software que cumpla con las mismas funcionalidades y posea un esquema de seguridad eficiente en cuanto actualizaciones, esto teniendo presente que se haya realizado una investigación minuciosa del software verificando que no tenga ningún tipo de vulnerabilidad.

- Monitoreo de trafico de la red con el fin de identificar aumento de tráfico lo cual puede evidenciar fuga de información.

- Evitar que los usuarios tengan privilegios para la instalación de software, esto garantiza que se instale software de manera controlada y con supervisión de los responsables del área de tecnología.

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

   Los equipos BlueTeam son encargados de brindar seguridad de manera proactiva, analizando y monitoreando constantemente patrones anormales, brindando mejoras continuas en seguridad a la infraestructura tecnológica con el fin de detectar y responder a cualquier tipo de ataque.
   A comparación con un equipo de respuesta a incidentes informáticos (CSIRT) los cuales brindan respuesta de manera urgente a posibles ataques que se puedan estar presentando, generando acciones reactivas y proactivas para contenerlos y acompañar en el proceso de recuperación y restablecimiento del servicio sobre el incidente presentado.

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

   Para la aplicación de controles básicos como son:

   - Identificación de actividades anormales o maliciosas en la red.
   - Análisis y auditoria de logs para detección y respuesta a posibles ataques.
   - Controlar e inventariar el software instalado en lo equipos de la red con el fin de identificar posibles instalaciones no autorizadas por la organización.
   - Para pruebas de penetración y ejercicios de RedTeam.
   - Aplicación de mejores prácticas para defensa en ciberseguridad.
   - Gestión continua de vulnerabilidades.

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

Como lo menciona nsit[23], es una solución realizada para detectar, responder y neutralizar amenazas cibernéticas donde su objetivo principal es tener una visión general de todo el entorno de red permitiendo la recopilación de datos en tiempo real de toda actividad que pueda presentar un riesgo para la empresa.

Sus características principales son las siguientes:

- Monitorear de manera centralizada las amenazas potenciales.
- Identificar entre falsos incidentes y amenazas reales.
- Capacidad de respuesta en tiempo real.
- Documenta el proceso de detección, resolución y actuación.
- Crea base de conocimientos.
- Escalamiento de casos o incidentes a los analistas de seguridad correspondientes.

6. 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.

1. ModSecurity (WAF):

Como lo menciona GEEKFLARE[24] Es un firewall de aplicaciones web de código abierto el cual brinda protección contra los siguientes tipos de ataques:

- Inyección SQL
- Cross-site scripting
- Ataques web comunes
- Actividad maliciosa
- Trojan
- Fuga de información

2. Snort:

Es un software de código abierto para la contención y detección de intrusos, tiene la capacidad de detener y generar alertas de gusanos,

[23] LogRhythm. (2021). Gestión de eventos e información de seguridad (SIEM). Recuperado de https://logrhythm.com/solutions/security/siem/.

[24] GEEKFLARE. (2021). 4 Firewall de aplicaciones web de código abierto para una mejor seguridad. Recuperado de https://geekflare.com/es/open-source-web-application-firewall/.

troyanos e intentos de vulneración de firewall, adicional a ello, avisos sobre posibles escaneos de puertos en la red o comportamientos irregulares.

3. Firewall Endian:

Es un firewall basado en Linux[25] el cual brinda una solución para la prevención, contención y gestión de amenazas el cual contiene funcionalidades como antivirus, VPN y filtrado de contenido, adicional a ello, brinda monitoreo, registro e informes en tiempo real sobre el comportamiento y actividades de la red contando con un sistema de prevención de intrusos (IPS).

[25] Ibid.

6 CONCLUSIONES

- Con el desarrollo del informe técnico sobre las fases del seminario de equipos de Red Team y Blue Team basado en escenarios, se encuentran todos los procesos que se deben llevar a cabo para el análisis a una infraestructura tecnológica y todos aquellos puntos importantes a tener en cuenta.

- De acuerdo con los conocimientos adquiridos sobre el funcionamiento de los Equipos de respuesta Red y Blue Team, se identifica la importancia de contar con los servicios que brindan, dado que mide la seguridad de la infraestructura tecnológica de una organización y las vulnerabilidades que se pueden encontrar en ella.

- En el transcurso del desarrollo de las actividades, se encuentra que las metodologías y técnicas utilizadas por los Equipo Red Team y Blue Team brindan un gran aporte en la detección y prevención de ataques cibernéticos para las organizaciones, dado que permiten establecer el aseguramiento de la información siguiendo las diferentes fases y procesos que se ejecutan.

7 RECOMENDACIONES

- Se recomienda que las organizaciones cuenten con equipos de ciberseguridad preparados para mitigar cualquier tipo de amenaza a la infraestructura tecnológica, realizando constantemente monitoreo sobre sus redes y aplicaciones.

- Mantener los sistemas operativos actualizados con los últimos parches de seguridad, actualizar dispositivos obsoletos que no posean soporte y realizar pruebas periódicas de pentesting con el fin de identificar vulnerabilidades de manera proactiva.

- Las organizaciones deben garantizar a su equipo de tecnología el apoyo necesario para blindar la seguridad de su infraestructura, esto incluye la adquisición de nueva tecnología, contratación de personal capacitado y brindar entrenamientos basados en seguridad al personal de la organización con el fin de mitigar amenazas de ingeniería social.

- Es importante establecer políticas de seguridad sobre los recursos y servicios informáticos de las organizaciones, este proceso involucra el personal y activos de la compañía que mediante normas y directrices permiten garantizar la confidencialidad, integridad y disponibilidad de la información, minimizando los riegos y vulnerabilidades que afecten la continuidad del negocio.

8 BIBLIOGRAFÍA

Catoira, Fernando, “PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: EXPLOTANDO UNA VULNERABILIDAD CON METASPLOIT FRAMEWORK”. {En línea}. {07 octubre de 2021} disponible en: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html).

Chaparro, Maria. “Legislación informática y protección de datos en Colombia, comparada con otros países”. {En línea} {07 octubre de 2021} disponible en: (file:///C:/Users/Samakinho/Downloads/1014-Texto%20del%20art%C3%ADculo-2757-1-10-20150430.pdf).

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. [Guía No 10]. (12 octubre de 2021). Seguridad y Privacidad de la Información. Guía para la preparación de las TIC para la continuidad del negocio. Bogotá, Colombia: MINTIC.p.3.

COPNIA, “Código de Ética”. {En línea}. {07 octubre de 2021} disponible en: (https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf).

CVE “CVE”. {En línea}. {06 octubre de 2021} disponible en: (https://cve.mitre.org/).

DESTINONEGOCIO “¿Cómo evitar un ciberataque en las empresas?”. {En línea}. {07 octubre de 2021} disponible en: (https://destinonegocio.com/co/gestion-co/recursos-materiales-co-co/ciberataque/).

EC-COUNCIL, Blog “RED TEAM VS BLUE TEAM”. {En línea}. {06 octubre de 2021} disponible en: (https://blog.eccouncil.org/red-team-vs-blue-team/).

ENTER.CO, “Detrás de Buggly: la historia de la fachada Andrómeda”. {En línea}. {08 octubre de 2021} disponible en: (https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/).

GEEKFLARE. (2021). 4 Firewall de aplicaciones web de código abierto para una mejor seguridad. Recuperado de https://geekflare.com/es/open-source-web-application-firewall/.

INCIBE_ “Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?”. {En línea}. {07 octubre de 2021} disponible en: (https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian).

INFOSEC, Industries. “OpenVAS / Greenbone Community Edition”. {En línea}. {07 octubre de 2021} disponible en: (https://infosecindustries.com/vendors/greenbone/openvas-greenbone-community-edition.html).

LogRhythm. (2021). Gestión de eventos e información de seguridad (SIEM). Recuperado de https://logrhythm.com/solutions/security/siem/.

MINTIC, “Ley 1273 de 2009”. {En línea} {07 octubre de 2021} disponible en: (https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf).

NMAP, “Escáner de seguridad de Nmap”. {En línea}. {07 octubre de 2021} disponible en: (https://nmap.org/).

Revista HackingEtico, “FASES DEL PENTESTING Aprende Como Hacer Auditoria De HACKING A Empresas”. {En línea}. {07 octubre de 2021} disponible en: (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html).

SIC, “LEY 1273 DE 2009”. {En línea}. {07 octubre de 2021} disponible en: (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf).

SGSI “ISO 27001: Vulnerabilidades de la organización”. {En línea}. {07 octubre de 2021} disponible en: (https://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/#:~:text=Las%20vulnerabilidades%20pueden%20encontrase%20asociadas,%2C%20equipos%2C%20software%20o%20informaci%C3%B3n.&text=Falta%20de%20aplicaci%C3%B3n%20de%20procedimientos,Fallos%20del%20control%20interno.).

SITEL “Gestión de la seguridad Blue Team”. {En línea}. {06 octubre de 2021} disponible en: (https://www.sistel.es/business-information-security/gestion-seguridad).

Tarazona, Cesar “AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN”. {En línea}. {06 octubre de 2021} disponible en: (https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/.).

UNITEL “Seguridad Informática en las empresas. Consejos básicos”. {En línea}. {06 octubre de 2021} disponible en: (https://unitel-tc.com/seguridad-informatica-en-las-empresas-consejos/).

UNIR, universidad en internet “Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?”. {En línea}. {06 octubre de 2021} disponible en: (https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/).

9 ANEXOS

ANEXO 1. ENLACE VIDEO DE SUSTENTACIÓN

https://youtu.be/_O2lIRvECls