Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

German Coral Narváez

202337164_6

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería - ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad Red Team y Blue Team

Diciembre 2024

Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

German Coral Narváez

202337164_6

Ever Luis Arroyo Barón

Director De Curso

Universidad Nacional Abierta y a Distancia – UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería - ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad Red Team y Blue Team

Diciembre 2024

Resumen

Este informe técnico es el compendio de las actividades propias de los equipos de seguridad Informática Red y Blue Team ejecutadas sobre un escenario simulado de una empresa de nombre CyberFort Technologies, compuesto por una maquina Kali Linux oficiando de recurso atacante y una máquina Windows 7 como maquina víctima, la cual tiene asociadas ciertas vulnerabilidades tales como la identificada con el nombre de EternalBlue, y una aplicación Web de nombre HFS (Http File Server) la cual presta el servicio de compartición de archivos entre equipos conectados, siendo esta aplicación el objetivo de explotación con el cual se logró el acceso no autorizado al sistema, el escalamiento de privilegios , la creación de una cuenta tipo Administrador y la exfiltración de datos. Y en respuesta a estas acciones del equipo Red Team, se mostrará también las medidas de respuesta, contención, mitigación, aseguramiento y recomendaciones específicas dadas por el equipo de Blue Team. Todo esto expuesto desde el marco legislativo que rige en Colombia relacionado con delitos informáticos y tratamiento de informacion personal vigentes.

Palabras clave: Blue Team, Exploit, Hardening, Red Team.

Tabla De Contenido

Glosario **7**

Introducción **13**

Objetivos **14**

Objetivo General **14**

Objetivos Específicos **14**

Informe Técnico **15**

Aspectos Legales y Éticos **15**

Procesos Ilegales Encontrados En El Escenario De Anexo 3 ..... **16**

Vulnerabilidades A La Ley 1273 De 2009 17

Artículo 269A - Acceso Abusivo A Un Sistema Informático 17

Artículo 269B - Obstaculización Ilegítima De Sistema Informático O Red De Telecomunicación 18

Artículo 269C - Interceptación De Datos Informáticos 18

Artículo 269D - Daño Informático 19

Artículo 269E - Uso De Software Malicioso 19

Artículo 269F - Violación De Datos Personales 20

Aspectos Técnicos **21**

Actividades Red Team 21

Fases De Pentesting **22**

Fase de Planeación y Reconocimiento 22

Fase De Análisis De Vulnerabilidades 23

Fase De Explotación 25

Fase De Post-Explotación 26

Fase De Reporte Y Mitigación 27

Actividades Blue Team 29

Desarrollo De Estrategias De Red Team Y Blue Team **32**

Estrategias Para Red Team 33

Estrategias Para Blue Team 34

Conclusiones **35**

Recomendaciones **38**

Mejoras De Seguridad Informática A Largo Plazo **38**

Implementación De Software De Seguridad 38

Segmentación De La Red 38

Medidas De Hardenizacion 39

A Nivel De Sistema Operativo (Windows 7) 40

A Nivel De Aplicación HFS 43

A Nivel De Red 43

Medidas Generales 44

Referencias Bibliográficas **45**

Apéndice **49**

Enlace Al Video De Sustentación **49**

Resultado De Prueba Anti Plagio **49**

Lista De Figuras

Figura 1 Configuración Del Entorno Para Pentestin..... 21

Figura 2 Proceso de Explotación de HFS en Windows 7 22

Figura 3 Vulnerabilidad Aplicación HFS 23

Figura 4 Búsqueda De Exploits HFS 25

Figura 5 Configuración Y Uso Del Exploit 26

Figura 6 Acciones De Post-Explotación 27

Figura 7 Estrategias De Ciberseguridad Blue Team 30

Figura 8 Acciones De Los Equipos Red Y Blue Team 32

Figura 9 Resultado De Prueba Anti Plagio 49

Glosario

“Amenaza: Es una circunstancia desfavorable que puede ocurrir y desencadenar consecuencias negativas sobre los activos provocando indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, accidentales o intencionadas.” (Incibe, 2021) p. 14

“Análisis de riesgos: Es el proceso donde se identifican los activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar controles adecuados para tratar el riesgo.” (Incibe, 2021) p. 14

“Análisis de Vulnerabilidades: Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas y lógicas, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.” (Incibe, 2021) p. 15

“Ataque Activo: Tipo de ataque detectable que se caracteriza por la modificación del contenido de la información, así como de los recursos o funcionamiento del sistema, pudiendo causar daños a dicho sistema. Este tipo de ataques pone en riesgo los principios de la seguridad de la información: confidencialidad; integridad y disponibilidad.” (Incibe, 2021) p. 15

“Autenticación: Acción mediante la cual se demuestra a otra persona o sistema que alguien es quien realmente dice que es, mediante un documento, una contraseña, rasgo biológico etc.” (Incibe, 2021) p. 18

“Backdoor: Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.” (Incibe, 2021) p. 20

“Brecha de Seguridad: Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos.” (Incibe, 2021) p. 23

“Blue Team: Es un equipo de individuos especializados en seguridad informática encargados de detener ataques de intrusión en redes y sistemas del ámbito corporativo por parte de atacantes reales. Su misión es corregir las vulnerabilidades o deficiencias detectadas por un equipo rojo, el cual realiza simulaciones de ataques controlados, así como detener posibles ataques reales.” (Incibe, 2021) p. 41

“CVE: Acrónimo del inglés en Common Vulnerabilities and Exposures; en español, listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad, así como un resumen de las características, efectos, las versiones del software afectadas, posibles soluciones o mitigaciones de dicha vulnerabilidad.” (Incibe, 2021) p. 35

“CVSS: Acrónimo en inglés de Common Vulnerability Scoring System; en español, sistema de puntuación de vulnerabilidad común, es un estándar cuya finalidad es cuantificar la gravedad y estimar el impacto que presentan las vulnerabilidades respecto a la seguridad de un sistema.” (Incibe, 2021) p. 35

“Doble factor de autenticación: Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple.” (Incibe, 2021) p. 40

“Escalada de privilegios: Situación que se produce cuando un ciber atacante explota una vulnerabilidad o fallo de una aplicación o sistema, logrando con ello permisos de acceso más amplios de los que inicialmente debería tener.” (Incibe, 2021) p. 41

“Escaneo de puertos: Técnica intrusiva en la que los atacantes buscan de manera activa los puertos y servicios que pudieran estar a la escucha, en busca de recopilar información de la víctima con la finalidad de intentar encontrar vulnerabilidades que explotar en la fase de ataque. Este tipo de técnica también es denominada fingerprinting.” (Incibe, 2021) p. 41

“Escaneo de vulnerabilidades: Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.” (Incibe, 2021) p. 42

“Exploit: Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de exploit se suele perseguir: el acceso a un sistema de forma ilegítima, obtención de permisos de administración en un sistema ya accedido y un ataque de denegación de servicio a un sistema.” (Incibe, 2021) p. 42

“Firewall: Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.” (Incibe, 2021) p. 32

“Firmware: Tipo de software que permite proporcionar un control a bajo nivel de un dispositivo o componente electrónico, siendo capaz de proveer un entorno de operación para las funciones más complejas del componente o comportándose como sistema operativo interno en armonía con otros dispositivos o componentes.” (Incibe, 2021) p. 44

“Fuga de información: Proceso por el cual se produce una fuga de la información almacenada en una red interna o en dispositivos físicos provocada por un atacante malintencionado y que es volcada o publicada en Internet para su libre consulta por parte de terceros sin autorización.” (Incibe, 2021) p. 45

“Hacker: Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.” (Incibe, 2021) p. 47

“Hardening: Proceso que trata de reducir las vulnerabilidades y agujeros de seguridad presentes en un sistema, creando un entorno lo más seguro posible siguiendo los principios de: mínima superficie de exposición, mínimos privilegios y defensa en profundidad.” (Incibe, 2021) p. 47

“HTTP: Son las siglas en inglés de Protocolo de Transferencia de Hipertexto. Se trata del protocolo más utilizado para la navegación web. Se trata de un protocolo que sigue un esquema petición-respuesta. La información enviada mediante HTTP se envía en texto claro, lo que quiere decir que cualquiera que intercepte el tráfico de red puede leer lo que se está enviando y recibiendo.” (Incibe, 2021) p. 48

“IDS: Sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusión Detection System) es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.” (Incibe, 2021) p. 49

“Incidente de Seguridad: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.” (Incibe, 2021) p. 50

“IPS: Siglas de Intrusion Prevention System (sistema de prevención de intrusiones). Es un software que se utiliza para proteger a los sistemas de ataques y abusos.” (Incibe, 2021) p. 53

“Malware: que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento.” (Incibe, 2021) p. 76

“Mitigación: Reducción o atenuación de los daños potenciales sobre los sistemas, aplicaciones y dispositivos causados por un evento, como una vulnerabilidad o ataque.” (Incibe, 2021) p. 58

“Pentesting: Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad.” (Incibe, 2021) p. 60

“Puerto: Es una interfaz o “puerta” a través de la cual se pueden enviar y recibir datos. Existen dos tipos de puertos: los físicos, que serían los conectores de un equipo que permiten la comunicación entre dispositivos, y que a su vez se dividen en varios tipos según el conector y su función; y los lógicos, generalmente implementados por software, que son aquellos que permiten

la comunicación entre dos máquinas en una red, mediante áreas de memoria reservadas en un sistema.” (Incibe, 2021) p. 65

“Red Team: Equipo de individuos especializados en realizar pruebas de intrusión en redes y sistemas del ámbito corporativo con el fin de evaluar la ciberseguridad de la empresa y detectar vulnerabilidades. Su objetivo es detectar las deficiencias antes de que sean explotadas por atacantes reales.” (Incibe, 2021) p. 41

“Segmentación de Red: Técnica que consiste en dividir una red informática en otras redes más pequeñas o segmentos. El objetivo es aumentar el rendimiento de la red mejorando el ancho de banda al reducir el número de integrantes que se comunican entre sí.” (Incibe, 2021) p. 69

“Virtualización: La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, o una red, en una máquina física, generalmente con el apoyo de un software que implementa una capa de abstracción para que la maquina física y la virtual puedan comunicarse y compartir recursos.” (Incibe, 2021) p. 76

“Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.” (Incibe, 2021) p. 77

Introducción

En este escenario virtual generado en base al propuesto por la empresa CyberFort Technologies, se ha conseguido simular un ejercicio de ciberseguridad que involucra a una máquina Kali Linux utilizada por el equipo de Red Team y una máquina Windows 7 la cual presenta dos vulnerabilidades evidentes, una de ellas conocida mayormente como 'EternalBlue' y otra vulnerabilidad generada por una aplicación web instalada la cual se ejecuta sobre el puerto 80.

El objetivo principal de este ejercicio es demostrar el proceso con el cual el equipo de Red Team, logra finalmente explotar la vulnerabilidad relacionada con la aplicación web, y los procesos siguientes referidos en la post-explotacion, accesos no autorizados, creación de usuarios y exfiltración de datos; de la misma manera esta práctica aborda todos las acciones de respuesta, mitigación y recomendaciones dadas por parte del equipo Blue Team, demostrando su papel protagónico en los planes de respuesta a incidentes, así como el monitoreo continuo de cara a la protección contra las innumerables amenazas cibernéticas actuales, tratando siempre de mantener la integridad, confidencialidad y disponibilidad de la información de acuerdo con los estándares legales y lineamientos éticos vigentes y regentes en Colombia.

Objetivos

Objetivo General

Diseñar técnicas de contención basadas en el análisis de riesgos y vulnerabilidades dentro de una infraestructura de Tecnología de la Información.

Objetivos Específicos

Documentar las vulnerabilidades críticas encontradas sobre la maquina victima Windows 7, por el equipo de Red Team, enfatizando y priorizando aquellas que podrían ser fácilmente explotadas, comprometiendo la confidencialidad, integridad o disponibilidad de la información.

Elaborar un informe técnico detallado acerca de las actividades realizadas en el Pentesting por parte de los integrantes del Red Team, así como las respuestas de su contraparte el Blue Team, registro de vulnerabilidades corregidas, siempre alineadas con los requisitos legales del Decreto 1377 de 2013 sobre violaciones de datos sensibles.

Apoyar la utilización de herramientas éticas y legales sobre los escenarios y acciones ejecutadas por el equipo de Red Team, asegurando siempre la trazabilidad y auditoría de dichas actividades cumpliendo con ello los principios de transparencia, profesionalismo y responsabilidad.

Crear un conjunto de recomendaciones adaptadas al entorno productivo real, teniendo como misión la implementación de políticas de seguridad que mitiguen riesgos similares en entornos corporativos del entorno cercano, respetando siempre la legislación colombiana vigente.

Informe Técnico

Aspectos Legales y Éticos

En Colombia, varias leyes y regulaciones rigen la ciberseguridad, la protección de datos y la conducta ética de las organizaciones. Estas leyes proporcionan un marco para prevenir, responder y remediar actos de ciber espionaje y otros incidentes de ciberseguridad.

Las siguientes son algunas leyes y regulaciones clave que se aplican para el desarrollo de esta actividad:

Ley 1273 de 2009 (Congreso de Colombia, 2009) (Ley sobre Tecnologías de la Información y las Comunicaciones - Ley TIC), Exige a los proveedores de servicios implementar medidas de seguridad para garantizar la integridad, confidencialidad y disponibilidad de la información. El incumplimiento conlleva sanciones.

Ley 1581 de 2012 (Congreso de Colombia, 2012) (Ley General de Protección de Datos) - Requiere que las organizaciones obtengan el consentimiento de las personas antes de tratar sus datos personales y ordena la implementación de medidas de seguridad para proteger dichos datos, con sanciones por incumplimiento.

Decreto 1078 de 2015 (Presidencia de la República de Colombia., 2015) (Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones) - Enfatiza la necesidad de que los proveedores de servicios implementen medidas de seguridad para proteger la información e impone sanciones por no cumplir con ellas.

Decreto 1377 de 2013 (Presidencia de la República de Colombia., 2013) (Reglamentación de la Ley 1581 de 2012) - Detalla las medidas de seguridad para proteger los datos personales e impone sanciones por violaciones.

Ley 1480 de 2011 (Congreso de Colombia., 2011b) (Ley de Protección al Consumidor) - Obliga a las organizaciones a proteger los datos personales de los consumidores y establece sanciones por no hacerlo.

Ley 1340 de 2009 (Congreso de Colombia., 2011a) (Ley Antimonopolio) - Exige a las empresas que aseguren los datos personales que poseen y las somete a sanciones en caso de incumplimiento.

Ley 104 de 1993 (Congreso de Colombia., 1993)(Código de Procedimiento Penal) - Las agencias de aplicación de la ley deben garantizar la protección de los datos durante las investigaciones penales y enfrentan sanciones por cualquier violación.

Ley 527 de 1999 (Congreso de Colombia, 1999) (Ley para la Promoción de la Sociedad de la Información) - Los proveedores de servicios deben implementar medidas de seguridad para proteger los datos personales de los usuarios, con sanciones por incumplimiento.

Procesos Ilegales Encontrados En El Escenario De Anexo 3

El escenario simulado para este informe parte de un contexto contractual para los aspirantes a formar parte de los equipos de Red y Blue Team, el cual presenta las siguientes irregularidades:

Vulnerabilidades A La Ley 1273 De 2009

El Acuerdo de Confidencialidad presentado incluye múltiples cláusulas que podrían contravenir varias disposiciones de la Ley 1273 de 2009, que busca proteger la información y los datos informáticos, así como los sistemas que los procesan. Esta ley modifica el Código Penal para garantizar la seguridad de los sistemas informáticos y la información, y sanciona acciones que atenten contra su integridad, confidencialidad y disponibilidad. Entre otros artículos que se estarían vulnerando están:

Artículo 269A - Acceso Abusivo A Un Sistema Informático

Texto de la ley: "El que sin autorización acceda en todo o en parte a un sistema informático protegido con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."(Congreso de Colombia, 2009)

Posible vulneración: En el contrato presentado, si se obliga al aspirante a no denunciar actividades sospechosas o ilícitas (como accesos abusivos a sistemas informáticos o espionaje), estaríamos ante un intento de encubrimiento de conductas que podrían constituir un acceso abusivo a sistemas informáticos por parte de la empresa. La omisión de denuncia en este contexto fomenta la continuación de prácticas ilícitas que vulneran los derechos de terceros, incluidas otras empresas y el Estado.

Artículo 269B - Obstaculización Ilegítima De Sistema Informático O Red De Telecomunicación

Texto de la ley: "El que sin estar facultado legalmente para ello impida, obstaculice o interfiera el funcionamiento o acceso a un sistema informático, red de telecomunicaciones o sus componentes, incurrirá en prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos legales mensuales vigentes." (Congreso de Colombia, 2009)

Posible vulneración: Las actividades de espionaje o interferencia con sistemas de telecomunicaciones, que no se pueden denunciar debido a las cláusulas contractuales, podrían constituir una violación a este artículo. Si la empresa, a través de accesos abusivos o la interrupción de redes, obstaculiza el funcionamiento de sistemas informáticos ajenos, esto sería una conducta ilícita. Obligar a un aspirante a guardar silencio sobre ello implicaría la complicidad y encubrimiento de estas acciones.

Artículo 269C - Interceptación De Datos Informáticos

Texto de la ley: "El que sin orden judicial intercepte datos informáticos en tránsito hacia un sistema informático, incurrirá en prisión de 36 a 72 meses y multa de 100 a 1.000 salarios mínimos legales mensuales vigentes." (Congreso de Colombia, 2009)

Posible vulneración: En el contrato, si se incluye la omisión de denuncia ante acciones como la interceptación de datos sin autorización judicial, se estaría favoreciendo la violación de este artículo. Las actividades de ciber espionaje o de interceptación ilegal de datos son prácticas prohibidas que, de llevarse a cabo por la empresa, pondrían en riesgo la seguridad de la información de terceros, y silenciar tales actos vulnera este precepto.

Artículo 269D - Daño Informático

Texto de la ley: "El que sin estar facultado para ello destruya, dañe, deteriore, altere o suprima sistemas informáticos, o sus partes o componentes lógicos (software) o físicos (hardware), incurrirá en prisión de 48 a 96 meses y multa de 200 a 1.000 salarios mínimos legales mensuales vigentes." (Congreso de Colombia, 2009)

Posible vulneración: Si en la empresa se realizan actividades ilegales que destruyen o dañan sistemas informáticos de otras entidades o personas, y se obliga al aspirante a no revelar estos hechos, se estaría promoviendo la impunidad ante delitos que generan un daño informático.

Este tipo de cláusula no solo contraviene la Ley 1273, sino que además podría agravar la responsabilidad penal de las personas involucradas por la destrucción o alteración de sistemas de terceros.

Artículo 269E - Uso De Software Malicioso

Texto de la ley: "El que sin estar facultado para ello y con el propósito de dañar, eliminar o destruir un sistema informático, transmita, introduzca, difunda o haga accesible un software malicioso, incurrirá en prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos legales mensuales vigentes." (Congreso de Colombia, 2009)

Posible vulneración: En caso de que dentro de la empresa se desarrolle, utilice o distribuya software malicioso, el contrato que impide denunciar o advertir sobre estas actividades es claramente contrario a la ley. Los pentesters, o cualquier profesional de ciberseguridad, tienen una responsabilidad ética y legal de reportar este tipo de acciones, y cualquier cláusula que limite esa obligación se consideraría una violación a los principios legales establecidos.

Artículo 269F - Violación De Datos Personales

Texto de la ley: "El que, sin estar facultado para ello, con provecho propio o de un tercero, o con daño del titular, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercambie, transmita o difunda datos personales contenidos en archivos, bases de datos o medios semejantes, incurrirá en prisión de 48 a 96 meses y multa de 200 a 1.500 salarios mínimos legales mensuales vigentes." (Congreso de Colombia, 2009)

Posible vulneración: Si el contrato implica la manipulación o acceso a datos personales y obliga al aspirante a no denunciar actos ilícitos, tales como el uso indebido o la venta de datos personales, esto estaría vulnerando este artículo. La confidencialidad no puede ser una excusa para encubrir actividades ilegales relacionadas con el tratamiento de datos personales. La Ley 1273 protege estos datos y castiga su manejo indebido sin la debida autorización.

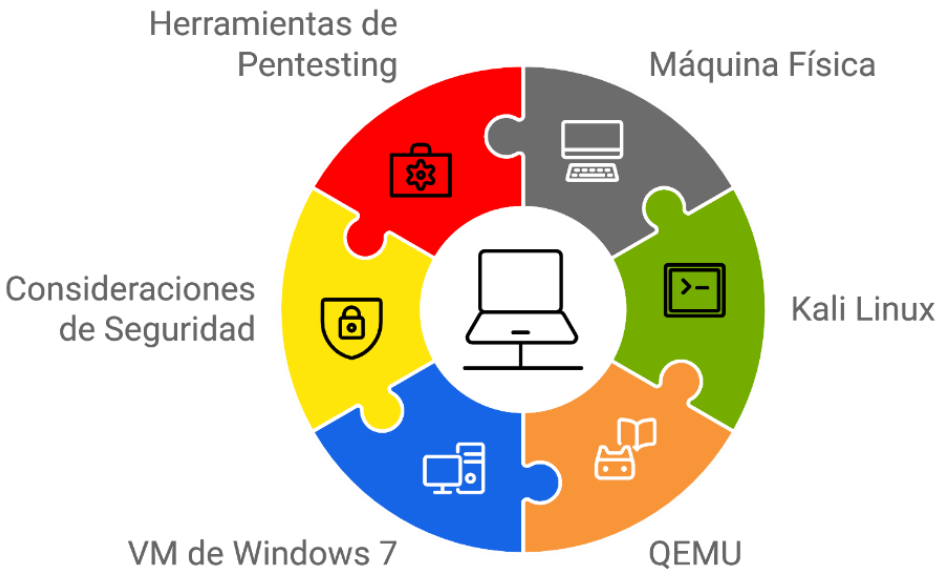
Las cláusulas del contrato de confidencialidad propuesto en el Anexo 3, plantean una serie de inconsistencias legales y éticas con respecto a la Ley 1273 de 2009. Obligar a un profesional a no denunciar actos ilegales como accesos abusivos a sistemas informáticos, espionaje, interceptación de datos sin orden judicial o el uso de software malicioso, no solo contraviene los principios éticos básicos en el campo de la ciberseguridad, sino que además infringe varios artículos de la ley mencionada. La confidencialidad debe proteger la información legítima de la empresa, pero no puede ser usada como una herramienta para encubrir actos ilícitos.

Aspectos Técnicos

Actividades Red Team

Entorno Simulado

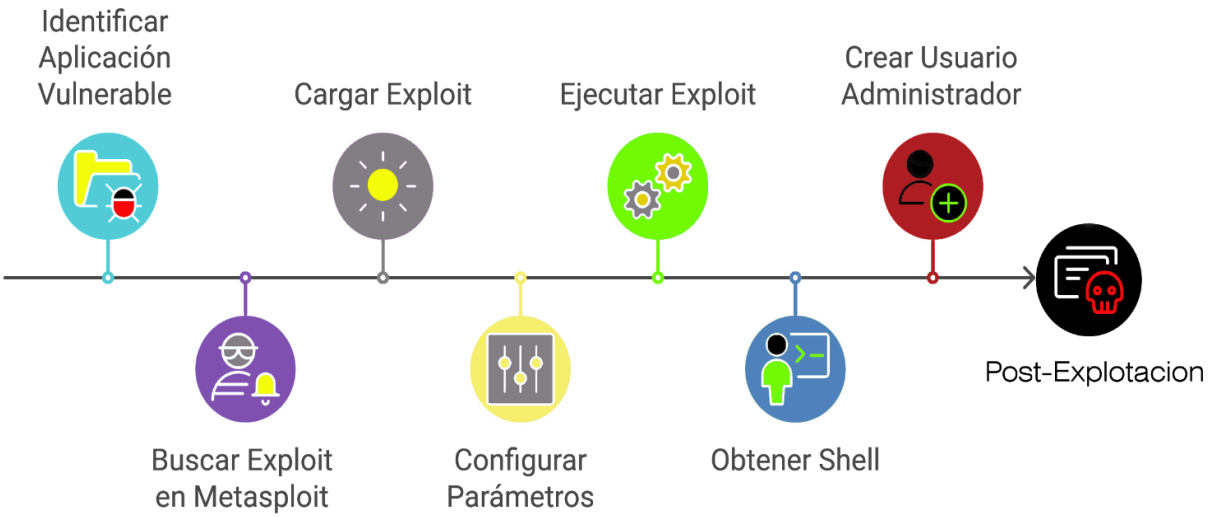
Figura 1 Configuración Del Entorno Para Pentestin



Fuente: Coral,G. (2024)

Proceso de Explotación a realizar por el equipo de Red Team (CYBERWARFARE, n.d.) sobre la vulnerabilidad presentada por la aplicación HFS en maquina Windows 7:

Figura 2 Proceso de Explotación de HFS en Windows 7



Fuente: Coral,G. (2024)

Para el logro del Proceso de explotación propuesto, el equipo de Red Team ejecuto los siguientes pasos relacionados con la prueba de penetración:

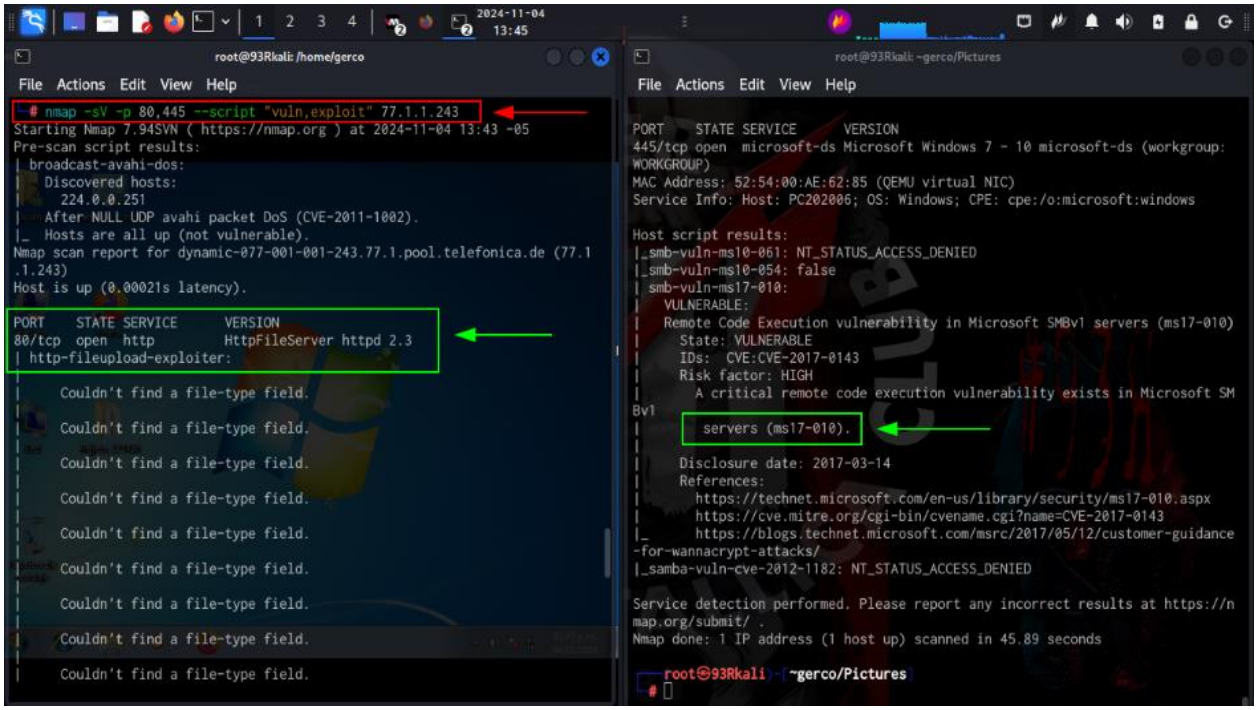
Fases De Pentesting

Fase de Planeación y Reconocimiento

En esta fase se recopilo información del objetivo identificando vulnerabilidades y vectores de ataque. En este escenario no se requirió del uso de herramientas OSINT ni búsquedas externas. Este proceso se enfocó exclusivamente en la gestión de información utilizando la herramienta Nmap desde la máquina Kali Linux (Práctica & Caballero Quezada, n.d.).

Alcance: En la definición del alcance, se delimitó el Pentesting al análisis de las vulnerabilidades y procesos de explotación asociados a la aplicación HFS (HTTP File Server) en el puerto 80 de la máquina Windows 7 objetivo. Aunque se identificó una vulnerabilidad crítica en el puerto 445, conocida como EternalBlue (MS17-010), este análisis se centrará exclusivamente en el puerto 80, según el documento del Anexo 4 - escenario 3.

Figura 3 Vulnerabilidad Aplicación HFS



Fuente: Coral,G. (2024)

Fase De Análisis De Vulnerabilidades

Se verifica que esta aplicación tiene asociada una vulnerabilidad reconocida con el CVE-2014-6287 (NIST, 2021), la cual explotada permite al atacante tener acceso al Shell y ejecutar código arbitrario sobre la maquina objetivo.

Clasificación: Se clasifica como una Vulnerabilidad del tipo Ejecución Remota de Código (RCE), con una puntuación de 9.8 o de nivel *Crítico*, según el CVSS (CVEDetails, 2021) (Common Vulnerability Scoring System), Sistema de Puntuación de Vulnerabilidades Comunes. La vulnerabilidad plantea un alto riesgo debido a su impacto crítico y su facilidad de explotación.

Documentación: Se adjunta la documentación (Packetstormsecurity, 2014) relacionada con el CVE-2014-6287

"Affected software: http://sourceforge.net/projects/hfs/

Version: 2.3x

 # Exploit Title: HttpFileServer 2.3.x Remote Command Execution

 # Google Dork: intext:"httpfileserver 2.3"

 # Date: 11-09-2014

 # Remote: Yes

 # Exploit Author: Daniele Linguaglossa

 # Vendor Homepage: http://rejetto.com/

 # Software Link: http://sourceforge.net/projects/hfs/

 # Version: 2.3.x

 # Tested on: Windows Server 2008, Windows 8, Windows 7

 # CVE : CVE-2014-6287

issue exists due to a poor regex in the file ParserLib.pas

function findMacroMarker(s:string; ofs:integer=1):integer;

begin result:=reMatch(s, '\{[.:]|[.:]\}|\|', 'm!', ofs) end;

it will not handle null byte so a request to

http://localhost:80/search=%00{.exec|cmd.}

will stop regex from parse macro, and macro will be executed and remote code injection happen."

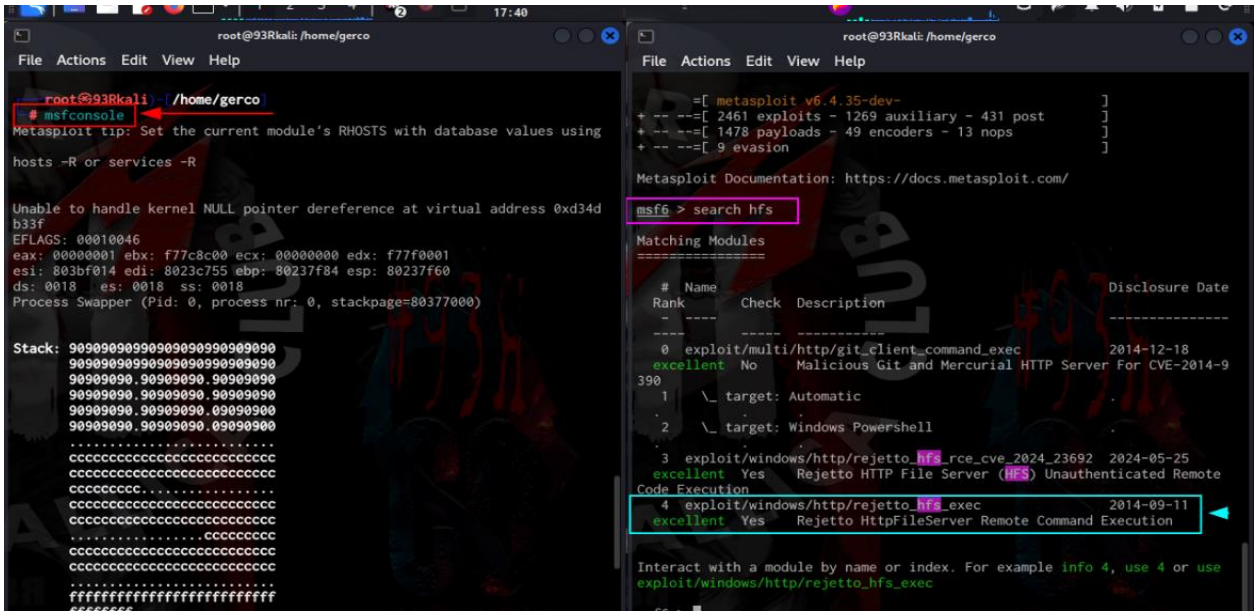
Fase De Explotación

En esta fase, se hace uso de la herramienta *Metasploit Framework (Metasploit, 2024),*para lo cual se ejecutó el comando *msfconsole*, sobre la terminal del usuario root de Kali Linux, una vez dentro de su entorno se buscó el *exploit* correspondiente a la aplicación rejeto HFS. Ver Figura 4.

Comando Metasploit: *search hfs*

Resultado: Muestra listado de exploits relacionados con esta aplicación.

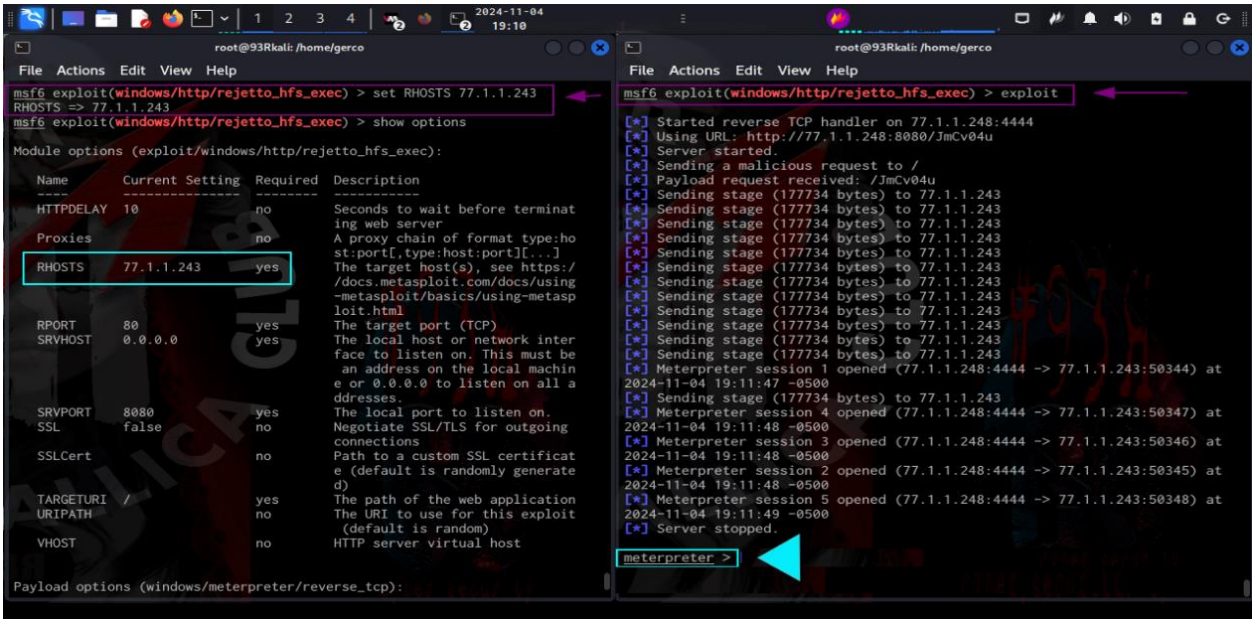
Figura 4 Búsqueda De Exploits HFS



Fuente: Coral, G. (2024)

Configuración del Exploit: El parámetro requerido para la correcta ejecución de este exploit, se denomina *RHOST*S, y corresponde a la dirección IP del host remoto, en este caso la dirección IP de la maquina Windows 7, que es 77.1.1.243. Para configurar este parámetro se hizo uso del comando de metasploit *set*. Seguidamente se ejecutó el exploit con el comando *exploit* o *run*, generando un shell "*meterpreter*" consecuencia de exitosa explotación de la vulnerabilidad.

Figura 5 Configuración Y Uso Del Exploit



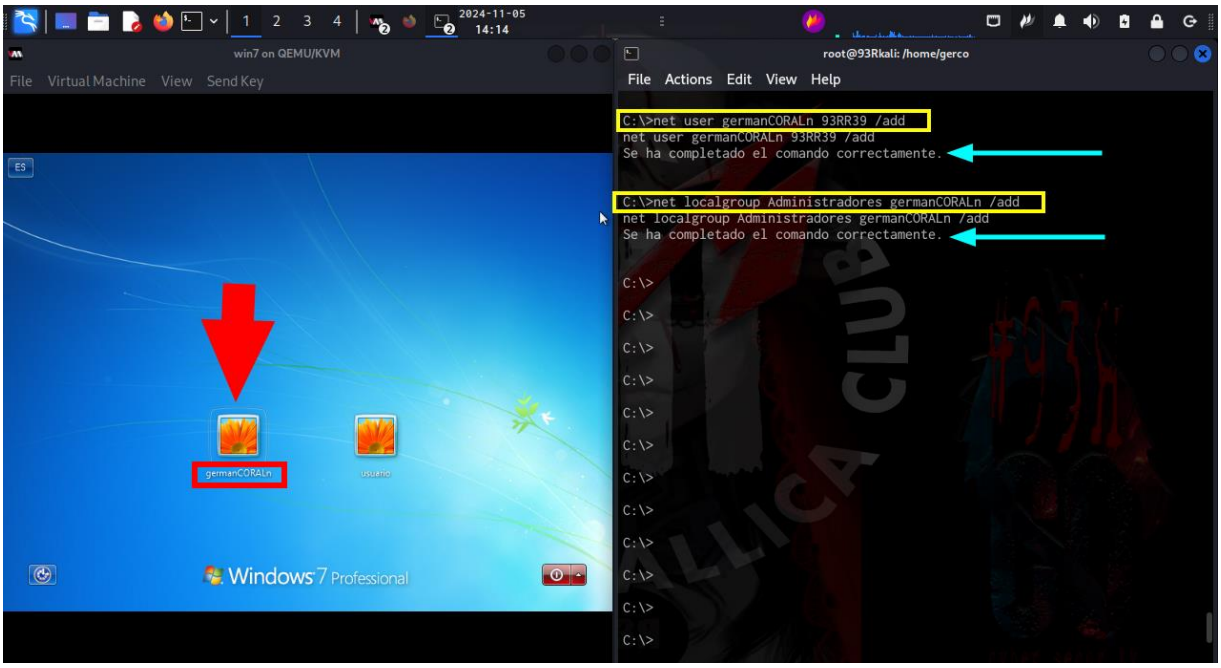
Fuente: Coral, G. (2024)

Fase De Post-Explotación

En este punto ya se logró un acceso no autorizado a la máquina Windows 7 mediante la explotación de la vulnerabilidad de la aplicación HFS, utilizando Metasploit Framework obteniendo un shell Meterpreter y un shell nativo del sistema. Esto permitió ejecutar procesos de para mantener un acceso persistente, se escaló privilegios, se exploró la red y se creó una cuenta

de usuario tipo Administrador, utilizando los comandos complementarios ofrecidos por ambos tipos de shell.

Figura 6 Acciones De Post-Explotación



Fuente: Coral, G. (2024)

Fase De Reporte Y Mitigación

Resumen Ejecutivo

Durante la prueba de penetración realizada a la máquina con Windows 7 sobre este escenario propuesto y controlado, esta se vio comprometida al explotar una vulnerabilidad en la aplicación del servidor de archivos HTTP (Http File Server) (Exploit-db, 2016), el cual se ejecuta en el puerto 80 de esta máquina. La explotación de esta vulnerabilidad y su posterior proceso de Post-Explotación, condujo a la creación de una cuenta de usuario no autorizada de

tipo administrador, con las consecuencias relacionadas a este acceso privilegiado y la consecuente filtración de datos sugerida. Este informe detalla el proceso de explotación, evalúa el impacto de las vulnerabilidades explotadas y proporciona recomendaciones para su solución.

Recomendaciones De Mitigación

Actualizar Versión De Aplicación HFS

Acción: Se requiere acción inmediata Actualización a la última versión de la aplicación HFS que incluye el parche de seguridad para CVE-2014-6287 (CVEDetails, 2021), o búsqueda de aplicación similar con características de seguridad más elevadas.

Razón: Corrige la vulnerabilidad de ejecución remota de código.

Segmentación De Red

Acción: Implementar la segmentación de la red para aislar el servidor HFS de otros sistemas críticos.

Razón: Limita la exposición del servidor HFS y reduce el riesgo de movimiento lateral dentro de la red.

Controles De Acceso

Acción: Aplicar controles de acceso estrictos para limitar el acceso a la aplicación HFS.

Razón: Reducir la superficie de ataque y minimiza el riesgo de acceso no autorizado.

Monitorización

Acción: Implementar monitoreo para detectar y responder a cualquier intento de explotar la vulnerabilidad.

Razón: permite la detección y respuesta proactiva a amenazas potenciales.

Parches Regulares

Acción: Establecer un cronograma periódico de parches para garantizar que todo el software y los sistemas estén actualizados.

Razón: Impedir la explotación de vulnerabilidades conocidas.

Actividades Blue Team

Las intervenciones del Blue Team (Murdoch. D., 2018) ante este ataque tuvieron en cuenta marcos de referencia actualizados y efectivos, como NIST CSF (NIST, 2024), MITRE ATT&CK (Mitre, 2015), CIS Controls (CIS Critical Security Controls® v8 CIS Critical Security Controls, n.d.), y otros. Para este caso en particular, se escogió a MITRE D3FEND Framework (Mitre, 2023) por su enfoque en técnicas defensivas específicas para mitigar vulnerabilidades. En este escenario planteado, donde una máquina Windows 7 fue vulnerada lo que permitió la creación de una cuenta de administrador no autorizada con posible exfiltración de datos, se subraya la necesidad de implementar las siguientes estrategias defensivas:

Figura 7 Estrategias De Ciberseguridad Blue Team

Fuente: Coral, G(2024)

Aislamiento Inmediato

Desconexión de la Red

Se Aísla la máquina comprometida para evitar la propagación del ataque. Desconectando de la red, bloqueando el tráfico con reglas de firewall, cambiando contraseñas comprometidas, y desactivando servicios no esenciales para limitar accesos y privilegios del atacante.

Contención

Deshabilitar Cuentas y/o Servicios no Autorizadas

Se remueve o deshabilita cualquier Cuenta de tipo Administrativo no Autorizada creada por el atacante.

Monitoreo por actividad: se utiliza herramientas de monitoreo de red para identificar cualquier actividad sospechosa, como conexiones inusuales o intentos de acceso a recursos críticos.

Bloqueo de direcciones IP: Identificando la dirección IP maliciosa, bloqueando desde el firewall para prevenir futuros ataques.

Implementación de medidas de control de acceso: Revisando y reforzando políticas de control de acceso para garantizar que solo usuarios autorizados puedan acceder a los sistemas y datos estos momentos críticos.

Bloqueo del puerto 80: Utilizando el firewall de Windows, bloquear el acceso al puerto 80 para evitar que el atacante pueda volver a explotar la vulnerabilidad.

Neutralización Inmediata

Parchar la Vulnerabilidad

Se gestiona la instalación de parches de seguridad y/o actualizaciones de la aplicación para mitigar la vulnerabilidad.

Se descarga e instala la versión más reciente de la aplicación HFS (Http Files Server), la cual incluye el parche de seguridad para la vulnerabilidad identificada como CVE-2014-6287.

Aplicar algunos otros parches de seguridad, como el correspondiente para la vulnerabilidad denominada EternalBlue que se observo estaba presente en el sistema, además de las actualizaciones de versión del sistema operativo.

Desarrollo De Estrategias De Red Team Y Blue Team

En este escenario virtual, simulamos un ejercicio de ciberseguridad que involucra dos máquinas: una máquina Kali Linux utilizada por el Red Team y una máquina Windows vulnerable. La máquina con Windows tiene dos vulnerabilidades mayormente conocidas: la vulnerabilidad 'EternalBlue' y otra vulnerabilidad ubicada en el puerto 80, conocida como 'HFS'.

El objetivo de este ejercicio es demostrar las acciones del Equipo Rojo al explotar esta última vulnerabilidad y la respuesta posterior y los esfuerzos de mitigación por parte del Equipo Azul. Es importante resaltar las acciones específicas que desarrolla cada equipo de seguridad,

Figura 8 Acciones De Los Equipos Red Y Blue Team

Fuente: (Global Technology, 2024)

Estrategias Para Red Team

Reconocimiento Inicial. Acerca del Escaneo de puertos: Es vital el identificar puertos abiertos, teniendo especial interés sobre el puerto 80 y demás vulnerabilidades mayormente conocidas en otros puertos.

Acerca del Escaneo de vulnerabilidades: El uso de herramientas como Nmap o Nessus ayuda la identificación de la mayoría de vulnerabilidades conocidas, incluidas las que para este ejercicio aplicaron para el puerto 80 determinado.

Acerca del Escaneo de aplicaciones web: El uso complementario de herramientas como Burp Suite u OWASP ZAP ayuda a identificar plenamente posibles vulnerabilidades en aplicaciones web que se ejecutan en el puerto 80.

Explotación. Tomando ventaja de la vulnerabilidad: El uso de herramientas o scripts diseñados puntualmente para la explotar la vulnerabilidad especifica implica un ahorro sustancial de tiempo y esfuerzos a todo nivel para el equipo de Red Team.

Realizar Escalada de privilegios: una vez alcanzado el acceso inicial no autorizado, es necesario escalar privilegios con el fin de obtener control total sobre el sistema, lo cual se logra con la creación o el acceso a cuentas administrativas.

Post-Explotación. Ejecutar Movimientos laterales: Se hace necesario identificar otros sistemas vulnerables instalados sobre la red, por lo cual es recomendable comprometerlos.

Acerca de la Exfiltración de datos: En este punto, es necesario recordar que el robar datos confidenciales, como contraseñas, información financiera o propiedad intelectual, son actos castigados por la legislación de cualquier país y en Colombia se tiene la suficiente legislatura para hacer cumplir la ley que sobre seguridad de la información se trata.

Persistencia: Sobre la Instalación de puertas traseras o Backdoors: El instalar un backdoor, permitirá el mantener el acceso persistente al sistema comprometido.

Acerca de la Implementación de Rootkits: Con lo cual se podrá ocultar la actividad maliciosa a fin de no ser detecta fácilmente por herramientas de seguridad.

Estrategias Para Blue Team

Detección. El Equipo Azul se caracteriza por la utilización de múltiples herramientas para el monitoreo y detección, en pos de identificar que actividades ha estado o está realizando el Equipo Rojo. Entre ellas están: IDS o Sistemas de detección de intrusiones (Intrusion Detection System), SIEM o sistemas de gestión de eventos e información de seguridad, así como herramientas para la monitorización de eventos sobre la red. La utilización de indicadores de compromiso (IoC), para la detección de tráfico inusual sobre la red, acceso a archivos sospechosos y demás eventos característicos de una intrusión son utilizados por este equipo.

Respuesta Al Incidente. Al detectar las actividades del Red Team, el Blue Team pone en marcha un plan de respuesta a incidentes, teniendo como acciones prioritarias, las siguientes:

Aislar la máquina Windows comprometida para evitar daños mayores.

Analizar las vulnerabilidades explotadas y el alcance del compromiso.

Recopilación de pruebas forenses para comprender las acciones del Equipo Rojo y los datos exfiltrados.

Mitigación. Acciones Inmediatas: Parchear la vulnerabilidad HFS actualizando dicha aplicación web, con la última versión segura distribuida por el fabricante.

Aplicar el parche MS17-010 de mitigación para la vulnerabilidad EternalBlue y reemplazar todas las credenciales comprometidas y reconfigurar controles de acceso.

Conclusiones

El ejercicio de ciberseguridad realizado sobre el entorno virtual que representaba al presentado por la empresa CyberFort Technologies involucro actividades tanto del equipo de seguridad Red Team como del Blue Team, tanto en la maquina Kali Linux que oficio de atacante como de la maquina Windows 7 en función de objetivo o víctima, proporciono mucha información valiosa como punto de partida para mejorar la seguridad informática en entornos computacionales. La toma de medidas de seguridad proactivas toma relieve en este contexto ya que son cruciales, así como el escaneo de vulnerabilidades, la aplicación de parches y la actualización de sistemas periódicos para evitar la explotación de estos fallos de seguridad propios de los sistemas operativos o las aplicaciones, tales EternalBlue y HFS.

Acciones como la implementación de sistemas de monitoreo continuo y detección de intrusiones (IDS), hace que la detección temprana de actividades sospechosas en conjunto con una respuesta eficaz a incidentes pase a configurarse como un plan de respuesta a incidentes bien definido para una rápida identificación y mitigación de amenazas, incluido el correspondiente análisis forense para comprender de mejor manera el alcance del compromiso y por supuesto mejorar las defensas actuales y futuras.

Dentro del concepto de acciones recomendadas hacia una mitigación de estos eventos, tiene un especial interés el enfoque de seguridad por capas, al combinar una segmentación de red, con controles de acceso y seguridad de terminales, mejorando sustancialmente la seguridad general, mientras que la implementación de la autenticación multifactorial (MFA) agrega una capa adicional de protección contra los accesos no autorizados a sistemas y/o aplicaciones.

Un factor supremamente importante que marcara la diferencia es la concientización y la capacitación de los usuarios, ya que estas características son esenciales, con capacitación regular se ayuda a los empleados a reconocer y responder a intentos de phishing y ataques de ingeniería social; al realizar una simulación de phishing, por ejemplo, se identifican áreas de mejora en la concientización de los empleados y la respuesta a las amenazas. El cumplimiento de directrices administrativas, así como el cumplimiento normativo garantizaran que se está actuando dentro de las leyes y regulaciones colombianas pertinentes, estando en libertad para la realización de auditorías de seguridad y controles de cumplimiento periódicos, sin prejuicio de la integridad de la información.

La gestión de riesgos generada por terceros implico el tener que evaluar la postura de seguridad de dichos proveedores para garantizar que si estén cumpliendo con la normatividad propia de los estándares de seguridad de la organización; El incluir requisitos de seguridad y Acuerdos a nivel de servicios en los contratos ayudan a reducir los riesgos de terceros de manera efectiva. La mejora continua definitivamente se logrará mediante revisiones y actualizaciones periódicas de las políticas, procedimientos y controles de seguridad para lograr adaptarse a las amenazas del día a día y estableciendo un circuito de retroalimentación para recopilar aportes de los usuarios y partes interesadas para identificar áreas de mejora y perfeccionar las prácticas de seguridad.

Habilidades y herramientas técnicas demostraron ser vitales, Kali Linux, Metasploit y Nmap, fueron esenciales para ejecutar acciones de seguridad ofensivas, y el conocimiento de herramientas como soluciones IDS, SIEM y EDR, por su parte fueron cruciales para la defensa eficaz y respuesta a incidentes. La colaboración y la comunicación entre los equipos Red y Blue

Team, así como con otros actores involucrados, fueron esenciales para crear una estrategia de seguridad integral junto con la toma de acciones de mitigación garantizaron que todas las partes interesadas hayan estado informadas y pudieran tomar las medidas adecuadas.

Finalmente, en relación con las lecciones aprendidas y el hecho de estar preparados para cualquier intervención futura implica la realización de análisis y evaluaciones exhaustivas posteriores al incidente, el uso de los conocimientos adquiridos en el ejercicio mejorara la postura general de seguridad del entorno a cualquier nivel. Con la realización de este ejercicio se destacó de forma concluyente la importancia de un enfoque holístico ante el tema de la ciberseguridad, que combine medidas proactivas, respuestas eficaces a eventos anómalos, seguridad dado en niveles, concienciación y capacitación de usuarios, y el cumplimiento normativo y legal junto con la mejora continua.

Con la creación de conocimiento generada a partir de estas bases fundamentales, las organizaciones e incluso los usuarios domésticos pueden construir un marco de seguridad sólido para sus infraestructuras informáticas que pueda actuar de un escudo real y efectivo contra una amplia gama de amenazas cibernéticas y garantice la integridad, confidencialidad y disponibilidad de sus sistemas y la información objetivos finales de este ejercicio.

Recomendaciones

Mejoras De Seguridad Informática A Largo Plazo

Implementación De Software De Seguridad

Finalidad: Implementar una solución integral de software de seguridad para proteger la infraestructura informática de la empresa de futuros ataques.

Acciones: Instalar y configurar soluciones de protección tipo Endpoint, incluyendo antivirus, antimalware, y herramientas EDR (Acronis, 2024)– EndPoint Detection and Response, como Acronis Security and EDR, CrowdStrike Falcon Insight, Trellix y también están las herramientas open source como: OSSEC, TheHive Project, osQuery, Nessus Vulnerability scanner, SNORT (Cisco, 2020), Ettercap Project, entre muchas otras más.

Habilitar las actualizaciones automáticas del sistema operative y aplicaciones instaladas sobre la(s) maquina(s).

Segmentación De La Red

Finalidad: Implementar la segmentación de la red para aislar sistemas críticos y su información relacionada.

Acciones: Configurar la segmentación de la red utilizando firewalls, VLANs, o cualquier otra técnica a nivel de hardware o software para realizar esta funcionalidad sobre la red.

Limitar el acceso a sistemas críticos, tanto para usuarios como para dispositivos no autorizados.

Finalmente, es importante resaltar que, bajo el escenario planteado para esta actividad, el sistema operativo de la maquina victima presenta una ausencia de protección a nivel de software,

por tanto, el accionar inmediato es crucial para mitigar la vulnerabilidad y prevenir que las acciones arbitrarias generadas por el atacante se propaguen. Siguiendo estos procesos técnicos, que incluyen el aislamiento inmediato, la contención, la evaluación inicial, la remediación inmediata, la implementación de protecciones temporales, la protección de datos, el análisis posterior al incidente y las mejoras de seguridad a largo plazo, las organizaciones pueden responder eficazmente al ataque y fortalecer su postura de seguridad.

Medidas De Hardenizacion

El hardening (BeyondTrust, 2024) consiste en una serie de herramientas y medidas técnicas, así como de mejores prácticas, destinadas a fortalecer la postura de seguridad de un sistema, a través de la optimización de su configuración. Este proceso implica la revisión y ajuste de parámetros de seguridad a nivel de sistema operativo, firmware, aplicaciones, servicios y otras áreas, con el objetivo de eliminar vulnerabilidades conocidas y prevenir la explotación de debilidades, enfocando todos los esfuerzos metódicos para auditar, identificar, cerrar y controlar dichas vulnerabilidades de seguridad sobre la infraestructura informática de una empresa o cliente individual.

Para el caso de estudio, las medidas de hardenizacion propuestas serían las siguientes, entre otras:

A Nivel De Sistema Operativo (Windows 7)

Actualizaciones De Seguridad. Instalar parches de Seguridad: Actualizar periódicamente Windows 7 con los últimos parches y revisiones para cerrar las vulnerabilidades de seguridad. Utilizar un servidor WSUS o soluciones de administración de parches de terceros para un control centralizado.

Configurar Windows Update: Automatizar las actualizaciones para garantizar que el sistema esté siempre protegido.

Configuración Del Firewall. Bloquear puertos innecesarios: Además del puerto 80, bloquear cualquier otro puerto que no sea estrictamente necesario para el funcionamiento de las aplicaciones.

Activar el firewall de Windows: Asegurando que el firewall de Windows esté activado y configurado correctamente.

Definir reglas de entrada y salida para restringir la comunicación innecesaria.

Gestión De Cuentas De Usuario. Eliminar cuentas innecesarias: Eliminar todas las cuentas de usuario que no sean necesarias y/o desconocidas para el Administrador real del sistema.

Restringir privilegios: Otorgar a los usuarios solo los privilegios necesarios para realizar sus tareas, basados en el concepto de Zero Trust (Kaelble. S., 2023).

Utilizar contraseñas fuertes: Implementar políticas de contraseñas robustas, exigiendo contraseñas largas y complejas.

Deshabilitar Servicios Innecesarios. Desactivar servicios: Deshabilitar todos los servicios que no sean esenciales para el funcionamiento del sistema.

Control de Cuentas de Usuario (UAC):

Habilitar y/o configurar UAC para evitar cambios no autorizados en el sistema.

Considerar configurar UAC en su nivel más alto para mayor seguridad.

Herramientas Antivirus Y Antimalware. Instalar y mantener soluciones antivirus y antimalware actualizadas, habilitando el análisis en tiempo real, permitiendo que se ejecuten de manera periódica sobre el sistema.

Configuración De Políticas De Seguridad De Grupos (GPO). Para generar funciones de complejidad en contraseñas, políticas de bloqueo de cuentas y restricciones en la instalación de software.

Escritorio Remoto Seguro (RDP). Deshabilitar el servicio y/o puerto RDP si no está siendo utilizado. De lo contrario, es necesario configurarlo, restringiendo el acceso a direcciones IP específicas que no sean reconocidas, aplicando además NLA o Autenticación a Nivel de Red.

Cambiar el puerto RDP predeterminado, a un puerto no estándar para ofuscarlo.

Lista Blanca De Aplicaciones. Utilizar AppLocker o Políticas de restricción de software para controlar qué aplicaciones se pueden ejecutar en el sistema.

Cifrado De Disco. Utilizar BitLocker u otras herramientas de cifrado para proteger los datos confidenciales en el disco duro.

Deshabilitar Servicios No Necesarios Y/O Obsoletos Sobre El Sistema. Esta acción incrementa el nivel de seguridad disminuyendo la superficie de ataque sobre el sistema (por ejemplo, Telnet, Registro remoto, Fax, etc.).

Habilitar Registros De Auditoría Y Monitoreo. Revisar frecuentemente eventos de seguridad con la ayuda de herramientas como Sysmon o soluciones de terceros para mejorar los detalles y el monitoreo de los registros.

Configuración De Arranque Seguro. Utilizar el entorno de configuración de BIOS o UEFI para habilitar el arranque seguro (si es compatible) para evitar cargas de firmware o sistema operativo no autorizados.

Restringir Protocolos Heredados. Deshabilitar protocolos como SMBv1, LLMNR y NetBIOS para reducir las superficies de ataque asociadas con protocolos más antiguos y/o deprecated.

Copia De Seguridad Y Recuperación. Implementar un plan periódico de copias de seguridad y prueba de procesos de recuperación. Almacenar copias de seguridad sin conexión para protegerse contra ataques de ransomware.

A Nivel De Aplicación HFS

Parches De Seguridad Para HFS - Http File Server. Aplicar parches: Si hay parches disponibles para la aplicación HFS, instalarlos inmediatamente para corregir la vulnerabilidad explotada, de lo contrario instale la versión más reciente de la aplicación la cual muy seguramente ya cuenta con el parche incluido.

Configuración Segura. Revisar la configuración: Revisar y ajustar la configuración de la aplicación HFS para minimizar la superficie de ataque, haciendo énfasis en accesos autorizados de usuarios.

Aislamiento. Aislar la aplicación: Si es posible, aislar la aplicación en una máquina virtual o contenedor para limitar el daño en caso de un nuevo compromiso.

A Nivel De Red

Intrusión Detection System (IDS). Implementar un IDS: Utilizar un IDS para monitorear el tráfico de red y detectar posibles intrusos. Aplicaciones open source como Snort, Suricata, OpenDLP entre otros, proporcionan altos niveles de calidad en la ejecución de estas tareas sobre la red.

Firewall De Hardware. Configurar reglas: Configurar el firewall de hardware para bloquear el tráfico no autorizado y permitir solo el tráfico necesario.

VPN. Utilizar VPN: Si se accede a la red de forma remota, obligar a los usuarios a conectarse a través de una VPN para proteger el tráfico. Aplicaciones como WireGuard y OpenVPN brindan máxima seguridad en este tipo de conexiones.

DLP. La implementación de un software DLP – permite detectar y prevenir las fugas de datos y las medidas adecuadas encaminadas a garantizar la protección de la información. Aplicación open source como KickIdler y MyDLP ofrecen características relevantes en este sentido de protección.

Medidas Generales

Realizar copias de seguridad regulares: Las copias de seguridad periódicas de los datos unidas a los correspondientes y correctos procesos de verificación de almacenamiento y restauración de dichas copias, son vitales en el restablecimiento del sistema en caso de un desastre.

Capacitación del personal: Capacitar a los usuarios sobre las mejores prácticas de seguridad para evitar que sean engañados por ataques de ingeniería social y/o acciones conscientes o inconscientes acerca del manejo de la tecnología .

Análisis de vulnerabilidades: Realizar análisis de vulnerabilidades periódicamente para identificar y corregir cualquier debilidad en el sistema y todo el entorno informático que posea la empresa o el usuario independiente.

Es importante recordar que la seguridad informática es un proceso continuo y el mantener una postura de defensa en profundidad, combinando múltiples capas de seguridad, será un mecanismo eficaz para proteger los sistemas y la información en particular.

Referencias Bibliográficas

Acronis. (2024). *The Best EDR Tools in 2024 - Acronis*. https://www.acronis.com/en-sg/blog/posts/enhance-threat-detection-with-advanced-edr-tools/

BeyondTrust. (2024). *What is Systems Hardening?* https://www.beyondtrust.com/resources/glossary/systems-hardening

CIS Critical Security Controls® v8 CIS Critical Security Controls. (n.d.). www.cisecurity.org/controls/

Cisco. (2020). *SNORT R Users Manual 2.9.16 The Snort Project*. https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMMOXGB2W5%2F20241202%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241202T165633Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=8b3b18d4caa58bdea8760a537a8e9b4eb23634edc6120ceb7e90b894353aafab

Congreso de Colombia. (1993). *Ley_104_de_1993* (Por la cual se dictan normas sobre mecanismos para la búsqueda de la convivencia la eficacia de la justicia y se disponen otras medidas. Diario Oficial No. 41.124. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=5091, Trans.).

Congreso de Colombia. (1999). *Ley_527_de_1999* (define y reglamenta el acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación. Diario Oficial No. 43.673., Trans.).

Congreso de Colombia. (2009). *Ley_1273_de_2009* (se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (TIC). Diario Oficial No. 47.223., Trans.).

Congreso de Colombia. (2011a). *Ley_1450_de_2011* (Plan Nacional de Desarrollo 2010-2014. Diario Oficial No. 48.102. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=41258, Trans.).

Congreso de Colombia. (2011b). *Ley_1480_de_2011* (Estatuto del Consumidor. Diario Oficial No. 48.220. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=41263, Trans.).

Congreso de Colombia. (2012). *Ley_1581_de_2012* (se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587., Trans.).

CVEDetails. (2021). *CVE-2014-6287 : The findMacroMarker function in parserLib.pas in Rejetto HTTP File Server (aks H*. https://www.cvedetails.com/cve/CVE-2014-6287/

CYBERWARFARE. (n.d.). *RED TEAM FOR BEGINEERS*. Retrieved December 1, 2024, from https://elhacker.info/Cursos/Certified%20Red%20Team%20Analyst%20-%20CRTA/PDF/Red%20Team%20Analyst%20Course.pdf

Exploit-db. (2016). *Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) - Windows remote Exploit*. https://www.exploit-db.com/exploits/39161

Global Technology. (2024). *Red Team y Blue Team en las organizaciones*. https://globalt4e.com/infografia-blue-team-red-team-organizaciones/

Incibe. (2021). *Glosario de términos de ciberseguridad*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Kaelble. S. (2023). *Zero-Trust-Segmentation-for-Dummies*. https://cdn.prod.website-files.com/63e25fb5e66132e6387676dc/641b76470c4b1b9caa3c986c_Zero-Trust-Segmentation-for-Dummies.pdf

Metasploit. (2024). *Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit*. https://www.metasploit.com/

Mitre. (2015). *MITRE ATT&CK®*. https://attack.mitre.org/

Mitre. (2023). *D3FEND Matrix | MITRE D3FEND™*. https://d3fend.mitre.org/

Murdoch. D. (2018). *Blue-team-handbook*. https://dokumen.pub/blue-team-handbook-soc-siem-amp-threats-hunting-use-cases-notes-from-fields-v102-9781021493896.html

NIST. (2021). *NVD - CVE-2014-6287*. https://nvd.nist.gov/vuln/detail/CVE-2014-6287

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Packetstormsecurity. (2014, September 12). *HttpFileServer 2.3.x Remote Command Execution ≈ Packet Storm*. https://packetstormsecurity.com/files/128243/HttpFileServer-2.3.x-Remote-Command-Execution.html

Práctica, U. P., & Caballero Quezada, A. E. (n.d.). *Hacking con Kali Linux*. Retrieved May 21, 2024, from www.ReYDeS.com

Presidencia de la República de Colombia. (2013). *Decreto_1377_de_2013* (Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial No. 48.807., Trans.).

Presidencia de la República de Colombia. (2015). *Decreto_1074_de_2015* (Decreto Único Reglamentario del Sector Comercio Industria y Turismo Diario Oficial No. 49.523. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=76608, Trans.).

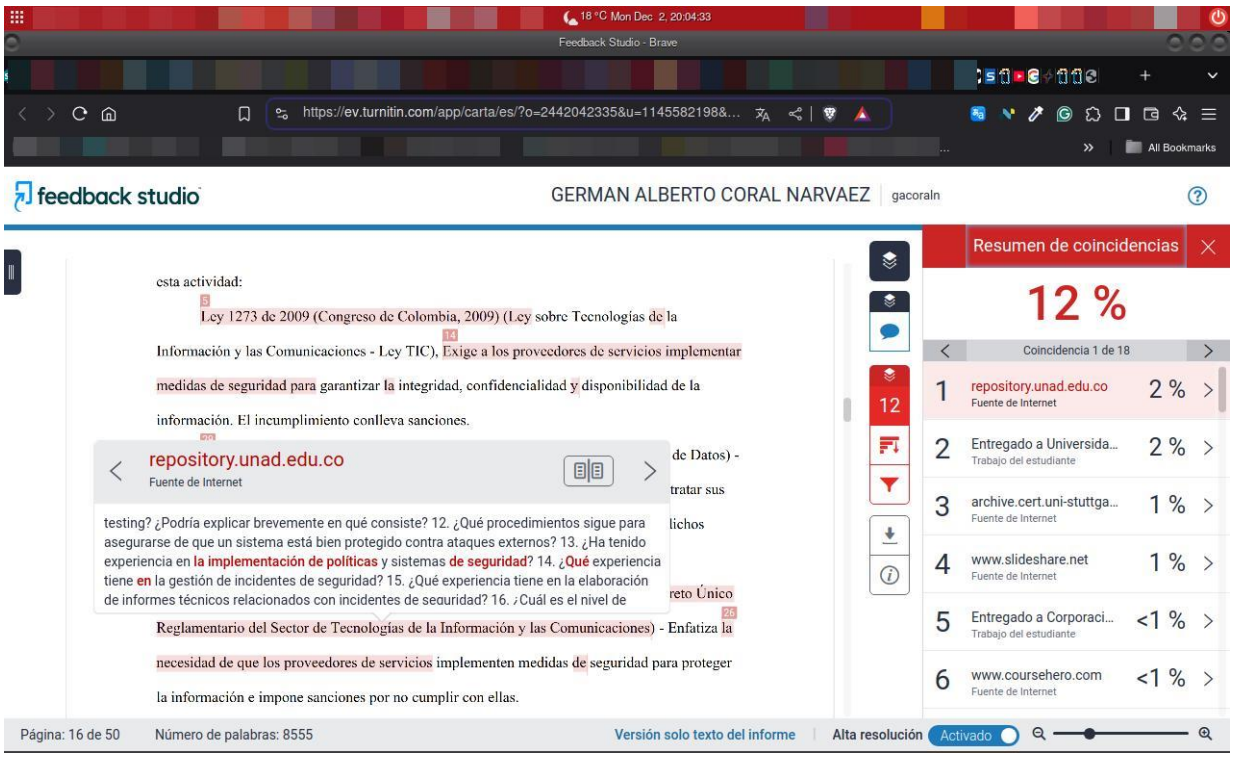
Apéndice

Enlace Al Video De Sustentación

Link del video **https://youtu.be/zRiyntlK3yQ**

Resultado De Prueba Anti Plagio

Figura 9 Resultado De Prueba Anti Plagio



Fuente: Coral, G. (2024)