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

DANIEL RUBIO SIERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA - CUNDINAMARCA
2022

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

DANIEL RUBIO SIERRA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

LUIS FERNANDO ZAMBRANO
Tutor de Curso.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA – CUNDINAMARCA
2022

CONTENIDO

pág.

INTRODUCCIÓN *9*

1 OBJETIVOS *10*

1.1 OBJETIVOS GENERAL 10

1.2 OBJETIVOS ESPECÍFICOS 10

2 DESARROLLO DE LOS OBJETIVOS *11*

2.1 DESARROLLO DE OBJETIVO 1 11

2.2 DESARROLLO DE OBJETIVO 2 19

2.3 DESARROLLO DE OBJETIVO 3 34

2.4 DESARROLLO DE OBJETIVO 4 43

2.5 DESARROLLO DE OBJETIVO 5 48

3 CONCLUSIONES *65*

4 RECOMENDACIONES *66*

BIBLIOGRAFÍA *67*

ANEXO *72*

LISTA DE CUADROS

Cuadro 1 Vulnerabilidad N° 1 - OpenVas 49
Cuadro 2 Vulnerabilidad N° 2 - OpenVas 50
Cuadro 3 Vulnerabilidad N° 3 - OpenVas 51
Cuadro 4 Vulnerabilidad N° 4 - OpenVas 52
Cuadro 5 Vulnerabilidad N° 5 - OpenVas 53
Cuadro 6 Vulnerabilidad N° 6 - OpenVas 54
Cuadro 7 Vulnerabilidad N° 7 - OpenVas 55
Cuadro 8 Vulnerabilidad N° 1 - Nessus 56
Cuadro 9 Vulnerabilidad N° 2 - Nessus 57
Cuadro 10 Vulnerabilidad N° 3 - Nessus 58
Cuadro 11 Vulnerabilidad N° 4 - Nessus 59
Cuadro 12 Vulnerabilidad N° 5 - Nessus 60
Cuadro 13 Hardening OpenVas.....62
Cuadro 14 Hardening Nessus.....63

LISTA DE ILUSTRACIONES

Ilustración 1 Fases de Pentesting 20
Ilustración 2 Topología Maquina Objetivo N° 1 21
Ilustración 3 Maquina Objetivo - App rejetto v. 2.3 22
Ilustración 4 Nmap - Descubrimiento de Equipos 23
Ilustración 5 Escaneo – Detección Vr Puertos Maquina Objetivo N° 1 24
Ilustración 6 Montaje OpenVas 25
Ilustración 7 Analisis Vulnerabilidades Maquina Objetivo 25
Ilustración 8 Severidad General 26
Ilustración 9 Vulnerabilidades Identificadas 26
Ilustración 10 Severidad de Vulnerabilidades 26
Ilustración 11 Aplicaciones de la Maquina Objetivo 30
Ilustración 12 Analisis de Vulnerabilidades Nessus 31
Ilustración 13 Vulnerabilidades a Detalle - Nessus 31
Ilustración 14 Nessus - Puerto 8080 33
Ilustración 15 Aplicación rejetto v. 2.3 34
Ilustración 16 Escaneo – Detección Vr Puertos Maquina Objetivo N° 1 35
Ilustración 17 Vulnerabilidades Identificadas 35
Ilustración 18 Información Exploit Rejetto 37
Ilustración 19 Ejecución Exploit Vs Log HFS 37
Ilustración 20 Ejecución Metasploit 38
Ilustración 21 Search Exploit HFS 39
Ilustración 22 Options Exploit HFS 39
Ilustración 23 Ejecución Exploit 40
Ilustración 24 Creación de Usuario 41
Ilustración 25 Configuración Usuario Administrador 41
Ilustración 26 Validación Creación Usuario 41
Ilustración 27 Validación Privilegios Usuario 42
Ilustración 28 Actualización de Rejjeto 45
Ilustración 29 SO - No Activo 46
Ilustración 30 SO Activo 46
Ilustración 31 Actualizaciones Instaladas SO 46
Ilustración 32 Instalación de Google Drive 47
Ilustración 33 Contenido Almacenado en Google Drive 47
Ilustración 34 OpenVas Resultados. 61
Ilustración 35 Nessus Resultados 61
Ilustración 36 Hardening - OpenVas Before Vs Later 62
Ilustración 37 Hardening - Nessus Before Vs Later 63

GLOSARIO

Nmap (Network Mapper): Es un Software gratuito, permite hallar las Vulnerabilidades y brechas de Seguridad en un sistema informático determinado, su código de programación puede ser configurado de manera libre (open source); suele ser usado de manera correcta, pero a la vez de manera maligna; permite hallar en grandes y pequeñas redes las diferentes terminales que componen dicha red; a la vez permite conocer el estado y actividad de cada puerto de dicho host a analizar (o atacar), también permite conocer el tipo y versión de sistema operativo que contiene la terminal.

Caja Blanca: Dentro de las Auditorias de Caja Blanca se encuentra las Auditorias de Caja Negra; en este tipo de Auditoria el Pentester obtiene el "Rol de Empleado o Usuario" de dicho Sistema, por ende, contiene ciertos privilegios sobre los roles que asume el Auditor en las Auditorias de Tipo Caja Negra y Caja Gris. El Pentester analiza y ataca las brechas de seguridad del sistema informático por medio de los medios y privilegios que tiene como el Rol de Empleado, a la vez de conocer que acciones puede realizar un usuario determinado con los privilegios que se le establecieron.

Caja Gris: Es uno de los Proceso de Auditoria más usados, junto con el Proceso de Auditoria de Caja Blanca; en este caso el Auditor obtiene el Rol de "Cliente o Proveedor" de dicho sistema informático a analizar; el cual contiene más privilegios que el Rol que asume el Auditor en el Proceso de Auditoria de Caja Negra, pero menos privilegios que el Rol que asume el Auditor en el de Caja Blanca; además de poca información sobre dicho sistema informático. Donde el Pentester analiza y ataca las brechas de seguridad teniendo en cuentas lo privilegios otorgados como el Rol de "Cliente o Proveedor".

Caja Negra: Es el Proceso de Auditoria más Costoso a Implementar; el Pentester requiere de grandes conocimientos y habilidad de análisis; obtiene el "Rol de un Tercero" que no contiene ninguna información pública característica y relevante sobre el sistema informático a analizar, por ende, debe realizar una investigación exhaustiva para poder hallar y explotar las vulnerabilidades de dicho sistema; por último, este tipo de auditoria requiere de mucho tiempo para su implementación.

CSIRT (Computer Security Incident Response Team): Son equipos de respuesta de incidentes de seguridad, los cuales actúan con gran rapidez ante ataques de seguridad informática; sus principales funciones mitigar y controlar al máximo estos riesgos, minimizar el impacto y consecuencia de estos riesgos; a la vez de obtener y contener las evidencias sobre dicho ataque para poner analizar las posible consecuencias y origen de dicho ataque.

Kali Linux 2.0: Es un Software gratuito y su codigo de programación puede ser configurado de manera libre (open source), se compone de una interfaz gráfica amigable con el usuario; su principal función y aplicación es realizar pruebas de penetración y conocer el nivel de seguridad de un sistema informático o un Hardware en específico; a la vez es usados en los procesos de los diferentes tipos de Auditorias (Caja Negra, Blanca y Gris). Kali Linux 2.0 se desarrolló con base al Software Backtrack y Kali Linux 1.0.

Malware: Este se refiere en general a cualquier tipo de Software Malicioso, diseñado para realizar ataques de manera visible (Ransomware) u oculta (Gusano y Troyanos) aun sistema informático, afectado principalmente los pilares de la seguridad informática (integridad, confidencialidad y disponibilidad).

Pentesting: También conocido como “Test de Penetración” (“prentration” y “testing”) es una técnica o procedimiento compacto que permite atacar a un determinado sistema informático para hallar y prevenir brechas de seguridad en dicho sistema, a la vez de conocer el nivel de seguridad que contiene dicha compañía, infraestructura o sistema. Es un Tipo de Hacking, pero legal.

Ransomware (Secuestro de Datos): Software con propósitos maliciosos ante sistemas informáticos, su ataque se basa en el secuestro de datos, por medio de cifrados complejos de datos importantes, bloquear por completo una terminal y anuncios sobre realizar pagos para obtener de nuevo los datos secuestrados “Rescate”.

Spear Phishing: Es un Tipo de ataque dirigido a correos y mensajería electrónicos por medio de la implementación de mensaje falsos que solicitan y redirigen a páginas Web Fraudulentas a ventanas de inicio de Sesión; donde la victima ingresa sus credenciales confidenciales y los Ciber Delincuentes captan esta información y realiza acciones malignan como hacerse pasar con la identidad de una persona de manera no autorizada en un página de compras, y realizar compras con la credenciales e identidad de la víctima.

OpenVas (Open Vulnerability Assessment Scanner): Software dirigido al hallazgo de vulnerabilidades (Scanner) a un sistema informático determinado, contiene un gran rango de Test y Vulnerabilidades de bajo, medio y alto riesgo de diferentes sistemas informáticos (Actualización a menudo de nuevas vulnerabilidades y Exploit). Permite realizar Pruebas (Autenticadas y no Autenticadas) y personalización de explotación de vulnerabilidades, a su vez su principal cualidad es su interfaz gráfica, la cual permite obtener una mejor interacción e interpretación del estado de seguridad de dicho sistema informático.

RESUMEN

Hoy en día las Infraestructuras Tecnológicas a nivel mundial, van creciendo aceleradamente y brindando más servicios digitales; teniendo en cuenta lo expuesto por el Periódico el Tiempo (2018) en su artículo Web “Este es uno de los vehículos que más contribuye en la reducción del uso del efectivo y de los costos de las transacciones, pero sobre su control en el mercado es poco lo que se conoce”[1], a de aclarar que en la venta y compra de producto, como el pago de servicios ya no se evidencia el intercambio de dinero físico; ya que por medio de las Plataformas de pago se ejecuta el canjeo de dinero pero de manera virtual; concediendo los trasmites de compra y venta de una manera más rápido y segura respecto a la manera presencial.

Las Infraestructuras Tecnológicas, un claro ejemplo son las Pasarelas de Pago, que generan las herramientas de utilidad como lo son pagos o servicios hacia los comerciantes, entidades financieras y usuarios finales, pero estas plataformas, sistemas tecnológicos y digitales presentan algunas falencias relevantes sobre el tema en general de Seguridad; ya que cuentan con vulnerabilidades y brechas de seguridad que pueden ser explotados por amenazas dirigidas por ciberdelincuentes.

Para poder optimizar y mejorar la seguridad de las Infraestructuras Tecnológicas, se requiere de la implementación de las estrategias basadas en metodologías de ciberseguridad Red Team y Blue Team ; para poder lograr una seguridad compacta e indescifrable, por medio de las herramientas y cualidades que ofrece Red Team, localizando cada brecha de seguridad en estas Infraestructuras Tecnológicas, que no pudiesen ser identificadas sin la implementación de las herramientas y procesos que componen Red Team. A la vez del planteamiento e implementación de salvaguardas por parte de Blue Team sobre las vulnerabilidades identificadas por Red Team.

[1] EL TIEMPO. Intermediario de pagos en internet, negocio que crece con poco control [en línea]. [Consulta: 20 de marzo del 2022]. Recuperado de: https://www.eltiempo.com/economia/sector-financiero/intermediarios-de-pagos-por-internet-en-colombia-no-estan-muy-controlados-175320

INTRODUCCIÓN

El siguiente documento hace referencia al análisis a fondo de las vulnerabilidades, brechas de seguridad y bajo nivel de seguridad de las principales Infraestructuras Tecnológicas, todo este análisis es realizado por medio de la ejecución de las funciones y herramientas de Red Team, además del estudio de sus posteriores resultados; teniendo en cuenta los antecedentes de los diferentes ataques que se han realizado a la Infraestructuras Tecnológicas.

Teniendo en cuenta los resultados arrojados de la implementación de las herramientas y funciones de Red Team, Blue Team diseña y ejecuta procedimientos, políticas de seguridad, controles de acceso y certificaciones de seguridad para solventar las vulnerabilidades y brechas de seguridad presentes en las Infraestructuras Tecnológicas, a la vez de aumentar el nivel de seguridad en dichas Infraestructuras Tecnológicas, por ultimo pero importante aumentar la confianza de los usuarios al depositar sus credenciales y datos sensibles en los diferentes servicios que ofrecen las Infraestructuras Tecnológicas.

1 OBJETIVOS

1.1 OBJETIVOS GENERAL

- Planificar estrategias basadas en metodologías de ciberseguridad ofensivas y defensivas (Red Team y Blue Team) ante incidentes de seguridad presentes en una infraestructura tecnología determinada.

1.2 OBJETIVOS ESPECÍFICOS

- Evaluar acciones y criterios de Red Team y Blue Team dentro de una Organización en base al Marco Ético y Legal.

- Identificar vulnerabilidades y brechas de seguridad en un sistema informático a partir del uso de metodologías y técnicas de intrusión – Red Team.

- Explotar la vulnerabilidad que contiene mayor impacto en un sistema informático a partir del uso de metodologías y técnicas de intrusión, generar un PoC ante los altos directivos de la compañía – Red Team.

- Formular e implementar estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI – Blue Team.

- Evaluar el nivel de seguridad de una Infraestructura Tecnológica luego de la implementación de las estrategias basadas en metodologías de ciberseguridad Red Team y Blue Team, para conocer su impacto en el aumento del nivel de seguridad final en base al nivel inicial.

2 DESARROLLO DE LOS OBJETIVOS

2.1 DESARROLLO DE OBJETIVO 1

- Evaluar acciones y criterios de Red Team y Blue Team dentro de una Organización en base al Marco Ético y Legal.

Luego de la lectura del Anexo N° 2 – Escenario 2 y el Anexo N° 3 – Acuerdo a detalle, se evidencia una serie fragmentos ilegales en dichos documentos.

Dentro del Anexo N° 2 – Escenario 2 se observa el siguiente fragmento a analizar:

Fragmento N° 1 – Anexo N° 2: Según el Anexo N° 2 – Escenario 2 "Para dar inicio, la organización WhiteHouse Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna."[2]

Analisis Fragmento N° 1 – Anexo N° 2: Se observa que dicho contrato de reclutamiento de integrantes de Red Team y Blue Team dentro de la compañía WhiteHouse Security, contiene procesos ilegales adjuntos por el abogado que ya no pertenece a la compañía. Otro factor importante la compañía WhiteHouse Security luego de evidenciar estos procesos ilegales dentro del contrato de reclutamiento, no reviso y elimino dichos procesos ilícitos antes de ser entregados a estos Equipos de Seguridad Informática.

Cabe aclarar que el Anexo N° 3 – Acuerdo destaca el Acuerdo de Confidencialidad entre partes.

Dentro del Anexo N° 3 – Acuerdo se observa los siguientes fragmentos a analizar:

Fragmento N° 1 – Anexo N° 3: De acuerdo al Anexo N° 3 – Acuerdo **"**Primera. Objeto: En virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales,

[2] UNAD**.** Anexo 2 – Escenario 2**.** [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://campus107.unad.edu.co/ecbti99/mod/folder/view.php?id=2937

asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados."[3]

Analisis Fragmento N° 1 – Anexo N° 3: Se aprecia claramente en dicho fragmento la no divulgación de procesos ilegales ejecutados dentro la compañía WhiteHouse Security por parte de los integrantes de Red Team y Blue Team, un item clave que dicha compañía realiza actos ilegales para beneficio propio.

Fragmento N° 2 – Anexo N° 3: Según al Anexo N° 3 – Acuerdo **"**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"."[4]

Analisis Fragmento N° 2 – Anexo N° 3: La compañía WhiteHouse Security da a conocer a los integrantes de Red Team y Blue Team que se entiende como información confidencial actos ilegales como son "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"[5], un item clave que dicha compañía realiza actos ilegales para beneficio propio.

Fragmento N° 3 – Anexo N° 3: De acuerdo al Anexo N° 3 – Acuerdo.

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

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

3. Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

4. Mantener la información confidencial en reserva hasta tanto adquiera el carácter de pública.

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

[3] UNAD**.** Anexo 3 – Acuerdo**.** [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://campus107.unad.edu.co/ecbti99/mod/folder/view.php?id=2937

[4] Idem.

[5] Idem.

6. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

7. 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."[6]

Analisis Fragmento N° 3 – Anexo N° 3: La compañía WhiteHouse Security da a conocer a los integrantes de Red Team y Blue Team las obligaciones que tienen sobre la información confidencial, en donde se observa claramente la no denuncia y divulgación (total o parcial) de los procesos y actos ilegales que se ejecutan dentro de la compañía WhiteHouse Security hacia las autoridades, competencia, terceros y entre otros.

Si llegase a caer estos datos confidenciales ilegales a las autoridades competentes, el responsable de la ejecución de dichos procesos y actos ilegales serán los integrantes de Red Team y Blue Team, sin recaer en responsabilidades legales y penales a la compañía WhiteHouse Security.

Fragmento N° 4 – Anexo N° 3: Según al Anexo N° 3 – Acuerdo **"**Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas."[7]

Analisis Fragmento N° 4 – Anexo N° 3: Se evidencia si los integrantes de Red Team y Blue Team incumplan con algunas de las obligaciones expuestas en el Acuerdo, como la denuncia y divulgación de procesos y actos ilegales dentro de la compañía, debe responder ante la compañía WhiteHouse Security.

Fragmento N° 5 – Anexo N° 3: De acuerdo al Anexo N° 3 – Acuerdo "Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada

[6] Idem.
[7] Idem.

en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security."[8]

Analisis Fragmento N° 5 – Anexo N° 3: Si llegase a caer estos datos confidenciales ilegales a las autoridades competentes, el responsable de la ejecución de dichos procesos y actos ilegales serán los integrantes de Red Team y Blue Team, sin recaer en responsabilidades legales y penales a la compañía WhiteHouse Security. Los integrantes de Red Team y Blue Team debe acudir a abogado privado.

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

Por medio de la Pagina Web de la Alcaldía Mayor de Bogotá DC (2009) da a conocer la Ley 1273 del 2009 expedida el 5 de enero del 2009 "De la Protección de la Información y de los Datos"[9] y sus respectivos Capítulos ($I\ y\ II$) y artículos ($269A\ al\ 269J$) que la componen.

Capitulo I:

Artículo $269A$ (Acceso Abusivo a un Sistema Informático): Cualquier persona que obtenga por ingresar a un sistema informático determinado (Blindado o no) de manera no autorizada, contemplara entre 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigentes.

Artículo $269B$ (Obstaculización Ilegitima de Sistema Informático o Red de Telecomunicación): El que obstaculice la disponibilidad del funcionamiento normal de un sistema de seguridad determinado, contemplara entre 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigentes.

Artículo $269C$ (Interceptación de Datos Informáticos): Cualquier persona que sin autorización legal obtenga acceso a datos entre un sistema de comunicación determinado, contemplara entre 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigente.

Artículo $269D$ (Daño Informático): Cualquier persona que manipule de manera maligna la integridad de datos informáticos, contemplara entre 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigente.

[8] Idem.

[9] ALCALDIA MAYOR DE BOGOTA DC**.** Ley 1273 del 2009. [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Artículo $269E$ (Uso de Software Malicioso): El que opte por diseñar, distribuir y usar un Software Malicioso ante un sistema informatice determinado, contemplara entre 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigente.

Artículo $269F$ (Violación de Datos Personales): Cualquier persona que obtenga y manipule datos personales de manera no autorizada y de forma maligna, contemplara entre 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigente.

Artículo $269G$ (Suplantación de Sitios Web para Capturar Datos Personales): El que opte por diseñar páginas Web o manipular el servicio DNS para llevar a las víctimas a páginas Web falsas para obtener datos personales o aplicar cualquier tipo de Malware a los PCs de las víctimas, contemplara entre 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigente.

Artículo $269H$ (Circunstancias de Agravación Punitiva): Teniendo en cuentas los artículos mencionados anteriormente, obtendrán un aumento de la mitad y tres cuartas partes de los castigos como lo son más años de prisión y multas más elevadas, cuando se somete estos delitos ante determinado servicio (8 Items) lo Items son:

- Item N° 1: El Ataque fue realizado sobre un una red o un sistema informático de una ente estatal u oficial (nacional o extranjero).
- Item N° 2: Servidor Público infringe la ley en ejercicio de sus funciones.
- Item N° 3: Abuso de Confianza al ser portador de información sensible.
- Item N° 4: Despojando la confidencialidad de información sensible, para causar daño a otro.
- Item N° 5: Generando provecho para sí mismo o un tercero.
- Item N° 6: El Ataque se realizó con fines terroristas o poner en riesgo la seguridad y defensa nacional.

Capitulo II:

Artículo $269I$ (Hurto por Medios Informáticos y Semejantes): La persona que suplante la identidad de otra persona para ingresar de manera no autorizada a un sistema informático determinado, obtendrá las sanciones del artículo 240.

Artículo $269J$ (Transferencia no Consentida de Activos): El que realice de manera no autorizada la transferencia de activos a terceros, contemplara entre 4 a 10 años de cárcel; y posterior una multa de 200 a 1.500 salarios mínimos legales vigente.

Artículos de la Ley 1273 vulnerados en el Anexo N° 3 – Acuerdo:

Los artículos de la Ley 1273 vulnerados en el Anexo N° 3 – Acuerdo[10] son:

- Artículo $269A$ (Acceso Abusivo a un Sistema Informático): Se evidencia en la compañía WhiteHouse Security acceso abusivo a un Sistema Informático "Accesos abusivos a sistemas informáticos"[11].

  Al infringir el Artículo 269A se obtendrán una sanción de 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigentes.

- Artículo $269C$ (Interceptación de Datos Informáticos): Se observa en la compañía WhiteHouse Security actividades de espionaje y "interceptación de información"[12].

  Al infringir el Artículo 269C se obtendrán una sanción de 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigentes.

- Artículo $269F$ (Violación de Datos Personales): Se evidencia en la compañía WhiteHouse Security "datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"[13].

[10] UNAD. Anexo 3 – Acuerdo. [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://campus107.unad.edu.co/ecbti99/mod/folder/view.php?id=2937

[11] Idem.

[12] Idem.

[13] Idem.

Al infringir el Artículo 269C se obtendrán una sanción de 4 a 8 años de cárcel; y posterior una multa de 100 a 1.000 salarios mínimos legales vigentes.

- Artículo $269H$ (Circunstancias de Agravación Punitiva): Luego del analisis de las actividades y procesos ilegales del Anexo N° 3 – Acuerdo de la compañía WhiteHouse Security para el "Item N° 5: Generando provecho para sí mismo o un tercero" se obtendrá un aumento de la mitad y tres cuartas partes de los castigos como lo son más años de prisión y multas más elevadas teniendo como base los años de prisión y multas estipuladas en los artículos $269A, 269C\ y\ 269F$.

Dado a la lectura minuciosa del Anexo N° 3 – Acuerdo de la compañía WhiteHouse Security, dirigido hacia reclutamiento de integrantes de Red Team y Blue, se evidencia una serie de fragmentos dudosos, dado a las actividades y procesos ilegales dentro de la compañía para beneficio propio.

Teniendo en cuenta lo anteriormente mencionado, como Especialista de Seguridad informática y con base al Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares - COPNIA[14], no aplicaría al trabajo en la compañía WhiteHouse Security teniendo en cuenta lo estipulado en el Codigo de Ética – COPNIA.

- Artículo 31. Deberes Generales de los Profesionales.

  f) "Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder"[15], en el Anexo N° 3 – Acuerdo, informa a los integrantes de Red Team y Blue la prohibición de denunciar las actividades ilegales a las entidades correspondientes.

- Artículo 34. Prohibiciones Especiales a los Profesionales Respecto de la Sociedad.

  a) "Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su

[14] COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica
[15] Idem.

propia preparación”[16], en dicho Anexo N° 3 – Acuerdo se observa actividades y procesos ilegales ejecutados dentro de la compañía WhiteHouse Security.

- Artículo 36. Prohibiciones a los Profesionales Respecto de la Dignidad de sus Profesiones.

  a) “Recibir o conceder comisiones, participaciones u otros beneficios ilegales o injustificados con el objeto de gestionar, obtener o acordar designaciones de índole profesional o la encomienda de trabajo profesional”[17], la compañía contiene un sueldo compacto y bonificaciones a la persona que acepte las actividades y procesos ilegales del Anexo N° 3 – Acuerdo.

- Artículo 38. Prohibiciones a los Profesionales Respecto de sus Colegas y demás Profesionales.

  a) “Utilizar sin autorización de sus legítimos autores y para su aplicación en trabajos profesionales propios, los estudios, cálculos, planos, diseños y software y demás documentación perteneciente a aquellos, salvo que la tarea profesional lo requiera, caso en el cual se deberá dar aviso al autor de tal utilización”[18], se observa dentro de la compañía WhiteHouse Security acciones ilegales sin el consentimiento del autor, como lo son: interceptación de información, accesos abusivos a sistemas informáticos.

  c)” Usar métodos de competencia desleal con los colegas”[19], la compañía WhiteHouse Security da a conocer en el Anexo N° 3 – Acuerdo realizar actividades en contra de la competencia para beneficio propio.

[16] Idem.
[17] Idem.
[18] Idem.
[19] Idem.

2.2 DESARROLLO DE OBJETIVO 2

- Identificar vulnerabilidades y brechas de seguridad en un sistema informático a partir del uso de metodologías y técnicas de intrusión – Red Team.

¿Qué es Pentesting?

Según la Página Web Ciberseguridad[20], Pentesting también conocido como "Test de Penetración" ("penetration" y "testing") es una técnica o procedimiento compacto y controlado que permite atacar a un determinado sistema informático para hallar y prevenir brechas de seguridad en dicho sistema, a la vez de conocer el nivel de seguridad que contiene dicha compañía, infraestructura o sistema. Es un Tipo de Hacking, pero legal. Hoy en día las compañías cada vez más requieren de un Pentester para conocer las amenazas y peligroso que se encuentra expuesta la compañía, y la vez analizar el nivel de defensa que contiene la compañía con respecto a ataques de seguridad informática.

Existen tres tipos de Pentesting entre los cuales son: Caja Blanca (Rol de Empleado o Usuario), Caja Negra (Rol de tercero o Ciber Delincuente) y Caja Gris (Rol de Cliente o Proveedor).

La Técnica de Pentesting se compone de 4 Fases, que también se pueden observar en la **Ilustración 1 Fases de Pentesting.**

- Fase N° 1 Pentesting - Determinar Tipo de Auditoria: La compañía informa el Pentesting a realizar teniendo en cuenta los tipos de Pentesting que existes: Caja Blanca (Rol de Empleado o Usuario), Caja Negra (Rol de tercero o Ciber Delincuente) y Caja Gris (Rol de Cliente o Proveedor).

- Fase N° 2 Pentesting - Recolección de Información: El Auditor investiga y obtiene las vulnerabilidades y brechas de seguridad de dicho sistema informático.

- Fase N° 3 Pentesting - Acceso al Sistema: Selección de objetivos a atacar y método de ataque a realizar.

- Fase N° 4 Pentesting - Elaboración de Informe: Se abordan el análisis de los resultados obtenidos dando a conocer el alcance e impacto de cada una de las brechas de seguridad de dicho sistema informático.

[20] CIBERSEGURIDAD. (2019). ¿Qué es el Pentesting? [en línea]. [Consulta: 20 de marzo 2022]. Recuperado de: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

Ilustración 1 Fases de Pentesting

Fuente: EXEVI**.** Servicio Pentesting de Webs, Apps y Sistemas [Imagen]. [Consultado: 20 de marzo de 2022]. Disponible en: https://www.exevi.com/soluciones/servicio-pentesting-de-webs-apps-y-sistemas/

Se determina la estructura de cada una de las Fases de Pentesting con base a los requerimientos de la compañía WhiteHouse Security.

- Fase N° 1 Pentesting - Determinar Tipo de Auditoria: Luego del analisis detallado del Anexo 4 – Escenario 3[21], se observa que tipo de auditoria va en base a la estructura Gray Box.

  Gray Box: Es uno de los Proceso de Auditoria más usados, junto con el Proceso de Auditoria de Caja Blanca; en este caso el Auditor obtiene el Rol de “Cliente o Proveedor” de dicho sistema informático a analizar; el cual contiene más privilegios que el Rol que asume el Auditor en el Proceso de Auditoria de Caja Negra, pero menos privilegios que el Rol que asume el Auditor en el de Caja Blanca; además de poca información sobre dicho sistema informático. Donde el Pentester analiza y ataca las brechas de seguridad teniendo en cuentas lo privilegios otorgados como el Rol de “Cliente o Proveedor”.

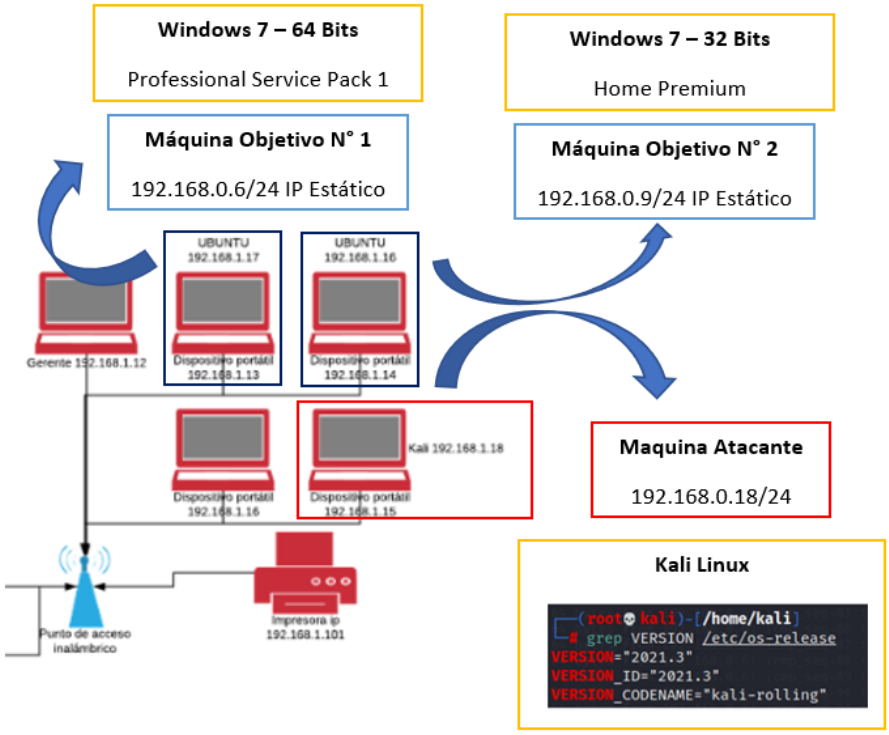
[21] UNAD**.** Anexo 4 – Escenario 3 [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://campus107.unad.edu.co/ecbti99/mod/folder/view.php?id=2939

- Fase N° 2 Pentesting - Recolección de Información:

Como primer paso se debe conocer el nivel de seguridad de la Maquina Objetivo (Windows 7 64 Bits) por medio de la ejecución de analisis de vulnerabilidades con las herramientas OpenVas y Nessus.

El Banco de Trabajo se conforma de 3 máquinas Virtuales, en donde hay una MV Atacante (Kali Linux), una Maquina Objetivo N° 1 (Windows 7 – 64 Bits) y una Maquina Objetivo N° 2 (Windows 7 – 32 Bits), en la **Ilustración 2 Topología Maquina Objetivo N° 1**, se observa el esquema del Banco de Trabajo solicitado (Whitehouse Security).

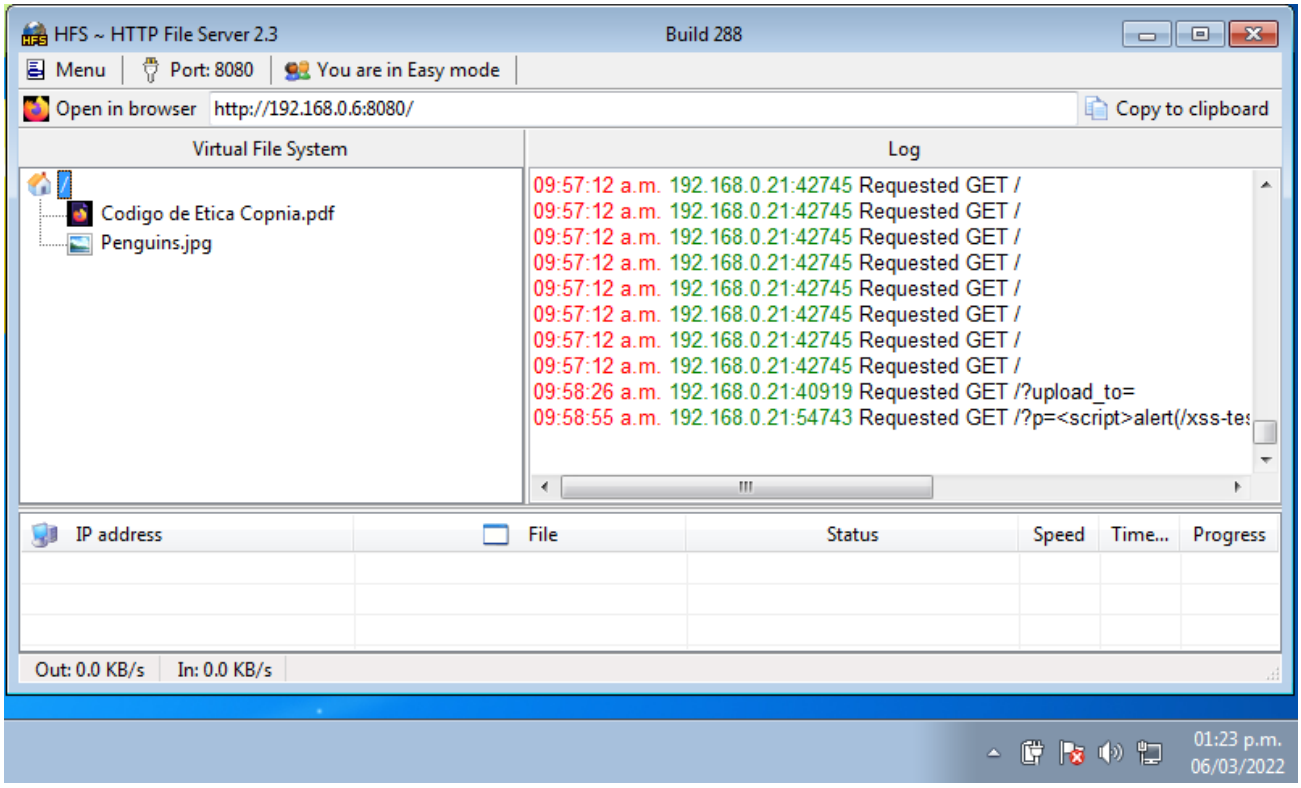
Ilustración 2 Topología Maquina Objetivo N° 1



Fuente: Elaboración Propia

Se observa la Maquina Objetivo Windows 7 64 Bits contiene la aplicación rejetto v. 2.3 (Puerto 8080/TCP) en ejecución.

Ilustración 3 Maquina Objetivo - App rejetto v. 2.3



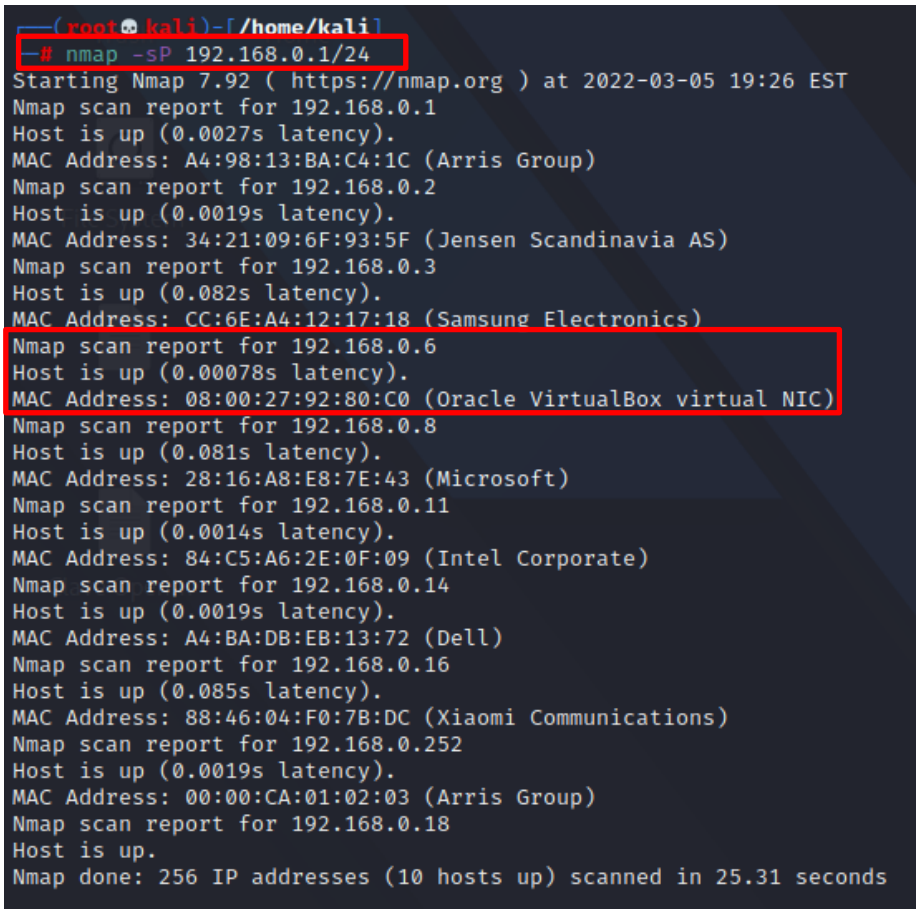
Fuente: Elaboración Propia

Recolección de Informacion – Nmap:

Se realiza un analisis de vulnerabilidades de primer nivel a la maquina Objetivo N° 1 Windows 7 64 Bits la cual contiene instalada la aplicación llamada rejetto v. 2.3 por medio del Software Kali Linux y la herramienta “Nmap”.

Se ejecuta comando para descubrimiento de dispositivos conectados a la Red 192.168.0.1/24.

Ilustración 4 Nmap - Descubrimiento de Equipos



Fuente: Elaboración Propia

Se realiza Escaneo de Puertos – Detección de Versiones a cada uno de los dispositivos conectados a la Red 192.168.0.1/24. Donde se evidencia la dirección IP 192.168.0.6 que corresponde a la maquina Objetivo N° 1 Windows 7 64 Bits, a la vez se evidencia una serie de datos importantes como lo son:

- Maquina Objetivo N° 1 encendida.
- MAC Maquina Objetivo N° 1 – 80:00:27:92:80:C0
- Nombre de la Maquina: PC202006.
- Sistema Operativo: Windows.
- Puertos abiertos (Servicios y Versión de la aplicación que usa dicho puerto).
- Puerto 8080/TCP – Open – Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Ilustración 5 Escaneo – Detección Vr Puertos Maquina Objetivo N° 1

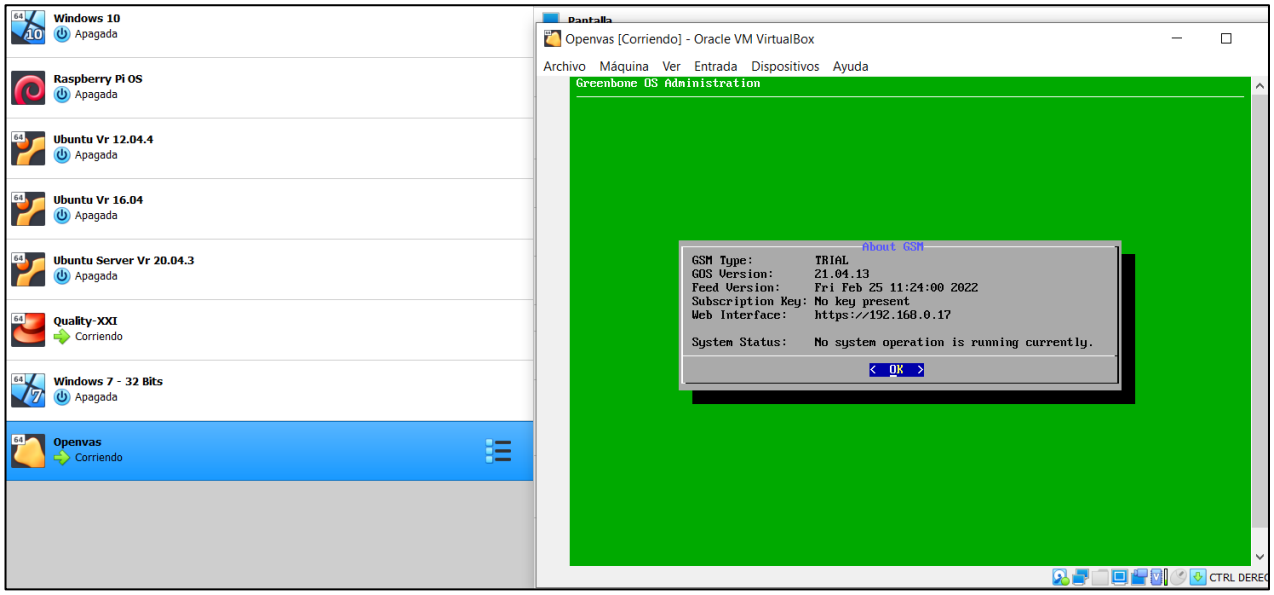
```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV 192.168.0.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-05 20:28 EST
Nmap scan report for 192.168.0.6
Host is up (0.00021s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open  http         HttpFileServer httpd 2.3
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 144.57 seconds
```

Fuente: Elaboración Propia

Analisis de Vulnerabilidades – OpenVas:

Se realiza montaje de la herramienta OpenVas:

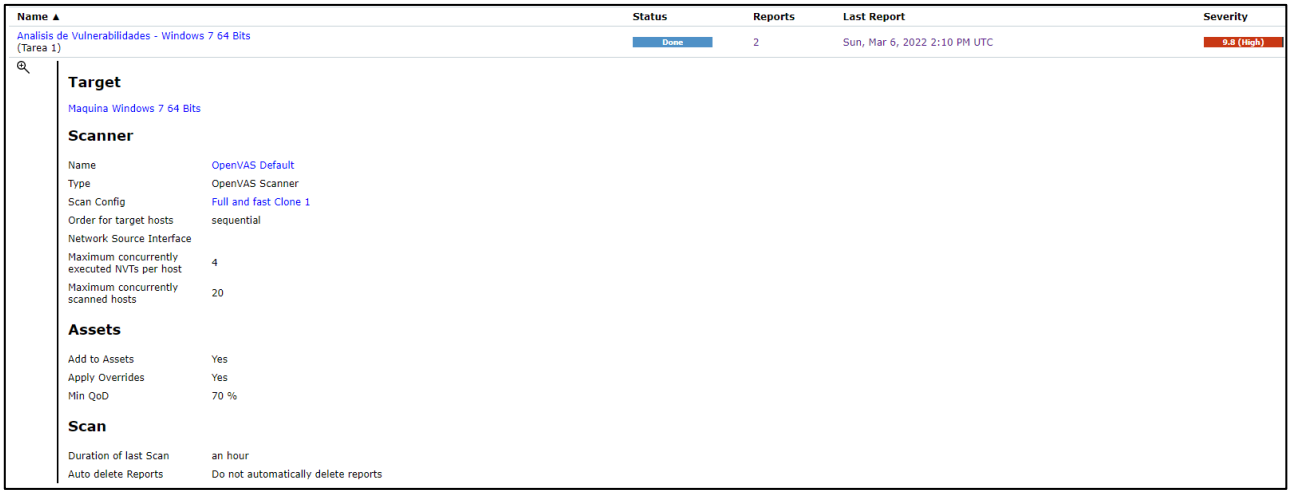
Ilustración 6 Montaje OpenVas



Fuente: Elaboración Propia

Se realiza configuración de Tarea 1 “Analisis de Vulnerabilidades - Windows 7 64 Bits” para el Objetivo “Maquina Objetivo N° 1 Windows 7 64 Bits”.

Ilustración 7 Analisis Vulnerabilidades Maquina Objetivo

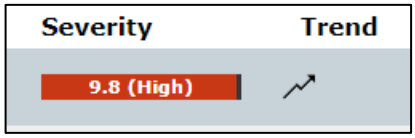


Fuente: Elaboración Propia.

Vulnerabilidades identificadas y Severidad de la vulnerabilidad.

Luego de la ejecución de la Tarea 1 “Analisis de Vulnerabilidades - Windows 7 64 Bits” hacia el Objetivo, la herramienta OpenVas da un rango de Severidad General Alta (9.8) con la tendencia de ir incrementado este score.

Ilustración 8 Severidad General



Fuente: Elaboración Propia.

A la vez identifica 7 Vulnerabilidades en la “Maquina Objetivo N° 1 Windows 7 64 Bits”.

Ilustración 9 Vulnerabilidades Identificadas

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location
HTTP File Server Remote Command Execution Vulnerability-02 Jan16	9.8 (High)	80 %	192.168.0.6		8080/tcp
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	8.1 (High)	95 %	192.168.0.6		445/tcp
HTTP File Server Remote Command Execution Vulnerability-01 Jan16	7.5 (High)	80 %	192.168.0.6		8080/tcp
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.0.6		135/tcp
Missing `httpOnly` Cookie Attribute	5.0 (Medium)	80 %	192.168.0.6		8080/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.0.6		8080/tcp
TCP timestamps	2.6 (Low)	80 %	192.168.0.6		general/tcp

Fuente: Elaboración Propia.

Dentro de las 7 Vulnerabilidades halladas en la “Maquina Objetivo N° 1 Windows 7 64 Bits”, se evidencia lo siguiente:

Ilustración 10 Severidad de Vulnerabilidades

Vulnerability	Severity ▼
HTTP File Server Remote Command Execution Vulnerability-02 Jan16	9.8 (High)
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	8.1 (High)
HTTP File Server Remote Command Execution Vulnerability-01 Jan16	7.5 (High)
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)
Missing `httpOnly` Cookie Attribute	5.0 (Medium)
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)
TCP timestamps	2.6 (Low)

Fuente: Elaboración Propia.

- **Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-02 Jan16.**

  Severidad: Alta (9.8)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: El servidor de archivos HTTP esta propenso a una vulnerabilidad de ejecución remota de comandos (RCE).

  Impacto: La explotación exitosa permitirá una atacante para ejecutar código arbitrario cargando un archivo con ciertos datos no válidos.

  Secuencias de bytes UTF-8 que se interpretan como símbolos de macro ejecutables.

- **Vulnerabilidad – Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)**

  Severidad: Alta (8.1)

  Puerto Afectado: 455/TCP (Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)).

  Descripción: El host le falta una seguridad crítica actualización según Microsoft Bulletin MS17-010.

  Impacto: La explotación exitosa permitirá remotamente obtener la capacidad de ejecutar código en el servidor de destino, también podría dar lugar a la divulgación de información del servidor.

- **Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-01 Jan16.**

  Severidad: Alta (7.5)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: El servidor de archivos HTTP esta propenso a una vulnerabilidad de ejecución remota de comandos (RCE).

Impacto: La explotación exitosa permitirá una atacante para ejecutar código arbitrario cargando un archivo con ciertos datos no válidos.

Secuencias de bytes UTF-8 que se interpretan como símbolos de macro ejecutables.

- **Vulnerabilidad - DCE/RPC and MSRPC Services Enumeration Reporting.**

  Severidad: Medio (5.0)

  Puerto Afectado: 135/TCP (epmap).

  Descripción: Entorno informático distribuido/llamadas a procedimientos remotos (DCE/RPC) o servicios MSRPC en ejecución en el host remoto se puede enumerar conectándose al puerto 135 y realizando las consultas correspondientes.

  Impacto: Un atacante puede usar este hecho para obtener más conocimiento.
  sobre el host remoto.

- **Vulnerabilidad - Missing `httpOnly` Cookie Attribute.**

  Severidad: Medio (5.0)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: A la aplicación le falta el atributo de cookie 'httpOnly'.

  Impacto: Application with session handling in cookies.

- **Vulnerabilidad - Cleartext Transmission of Sensitive Information via HTTP**

  Severidad: Medio (4.8)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: El host / aplicación transmite información sensible (usuarios/Password) en texto claro a través de HTTP (Sin encriptación).

  Impacto: Un atacante podría usar esta situación para comprometer o espiar el Comunicación HTTP entre el cliente y el servidor usando un ataque man-in-the-middle para obtener acceso a datos confidenciales como nombres de usuario o contraseñas.

- **Vulnerabilidad - TCP timestamps.**

  Severidad: Low (2.6)

  Puerto Afectado: General/TCP

  Descripción: El host remoto implementa marcas de tiempo TCP, por lo tanto, permite calcular el tiempo de actividad.

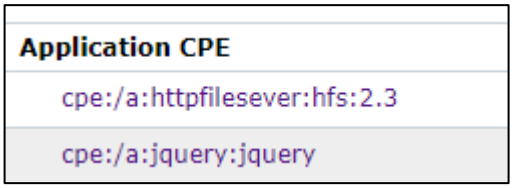
  Impacto: Un lado del efecto de esta característica es que el tiempo de actividad del host remoto pueda ser calculado por el atacante.

Componente o servicio que se puede ver afectado.

Se evidencia en el resultado del analisis de vulnerabilidades de la “Maquina Objetivo N° 1 Windows 7 64 Bits”, los servicios o aplicaciones afectadas son:

- Httpfilesever:hfs:2.3 (Aplicación rejetto v. 2.3).
- Jquery.

Ilustración 11 Aplicaciones de la Maquina Objetivo



Fuente: Elaboración Propia.

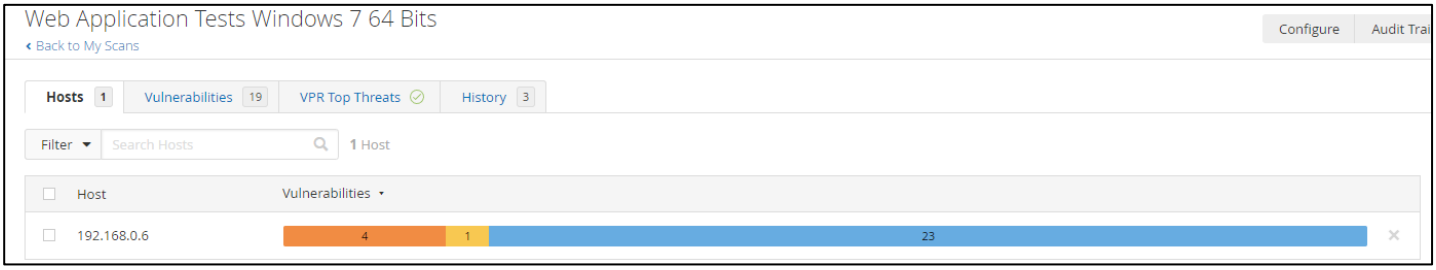
Los puertos de la “Maquina Objetivo N° 1 Windows 7 64 Bits” con vulnerabilidades son:

- Puerto 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3) Severidad Alta (9.8).
- Puerto 455/TCP (Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)).) Severidad Alta (8.1).
- Puerto 135/TCP (epmap) Severidad Media (5.0).

Analisis de Vulnerabilidades – Nessus:

Luego de la ejecución de la Tarea 1 “Web Application Tests Windows 7 64 Bits” hacia el Objetivo”, la herramienta Nessus identifica 5 Vulnerabilidades.

Ilustración 12 Analisis de Vulnerabilidades Nessus

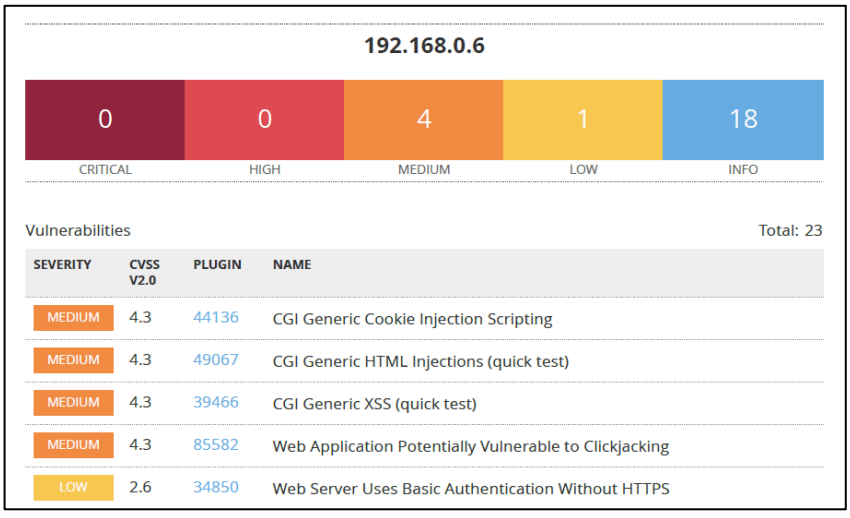


Fuente: Elaboración Propia.

Dentro de las 5 Vulnerabilidades halladas en la “Maquina Objetivo N° 1 Windows 7 64 Bits”, se evidencia lo siguiente:

- 4 vulnerabilidades con Severidad Media (4.3).
- 1 vulnerabilidad con Severidad Baja (2.6).

Ilustración 13 Vulnerabilidades a Detalle - Nessus



Fuente: Elaboración Propia.

- **Vulnerabilidad - CGI Generic Cookie Injection Scripting.**

  Severidad: Media (4.3)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: El servidor Web remoto contiene un script CGI que no desinfecta adecuadamente las cadenas de solicitud con JavaScript malicioso.

  Impacto: Un atacante inyecta cookies arbitrarias, obteniendo un ataque “fijación de sensación”.

- **Vulnerabilidad - CGI Generic HTML Injection (quick test).**

  Severidad: Media (4.3)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: El servidor Web remoto contiene un script CGI que no desinfecta adecuadamente las cadenas de solicitud con JavaScript malicioso.

  Impacto: Un atacante ejecuta HTML arbitrario, generando que el servidor pueda ser vulnerable ante inyecciones de “IFRAME”.

- **Vulnerabilidad - CGI Generic XSS (quick test).**

  Severidad: Media (4.3)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: El servidor Web remoto contiene un script CGI que no desinfecta adecuadamente las cadenas de solicitud con JavaScript malicioso.

  Impacto: Un atacante ejecuta codigo script y HTML arbitrario, generando que el servidor pueda ser vulnerable en secuencias de comandos entre sitios.

- **Vulnerabilidad - Web Application Potentially Vulnerable to Clickjacking.**

  Severidad: Media (4.3)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: Un encabezado de respuesta X-Frame-Options o un encabezado de respuesta Content-Security-Policy 'frame-ancestors' en todas las respuestas de contenido.

  Impacto: Exposición a ataques de secuestro de “clics”, generando que la víctima realice transacciones fráudenlas o acciones maliciosas sin su consentimiento.

- **Vulnerabilidad - Web Server Uses Basic Authentication Without HTTPS.**

  Severidad: Media (4.3)

  Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

  Descripción: El servidor Web remoto contiene varias páginas Web con protocolo Http, texto no cifrado.

  Impacto: Un ataque puede acceder al tráfico entre el servidor y el usuario, obteniendo usuarios y Password en texto claro.

Los puertos de la “Maquina Objetivo N° 1 Windows 7 64 Bits” con vulnerabilidades son:

- Puerto 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3) Severidad Alta (9.8).

Ilustración 14 Nessus - Puerto 8080

Port ▲	Hosts
8080 / tcp / www	192.168.0.6

Fuente: Elaboración Propia.

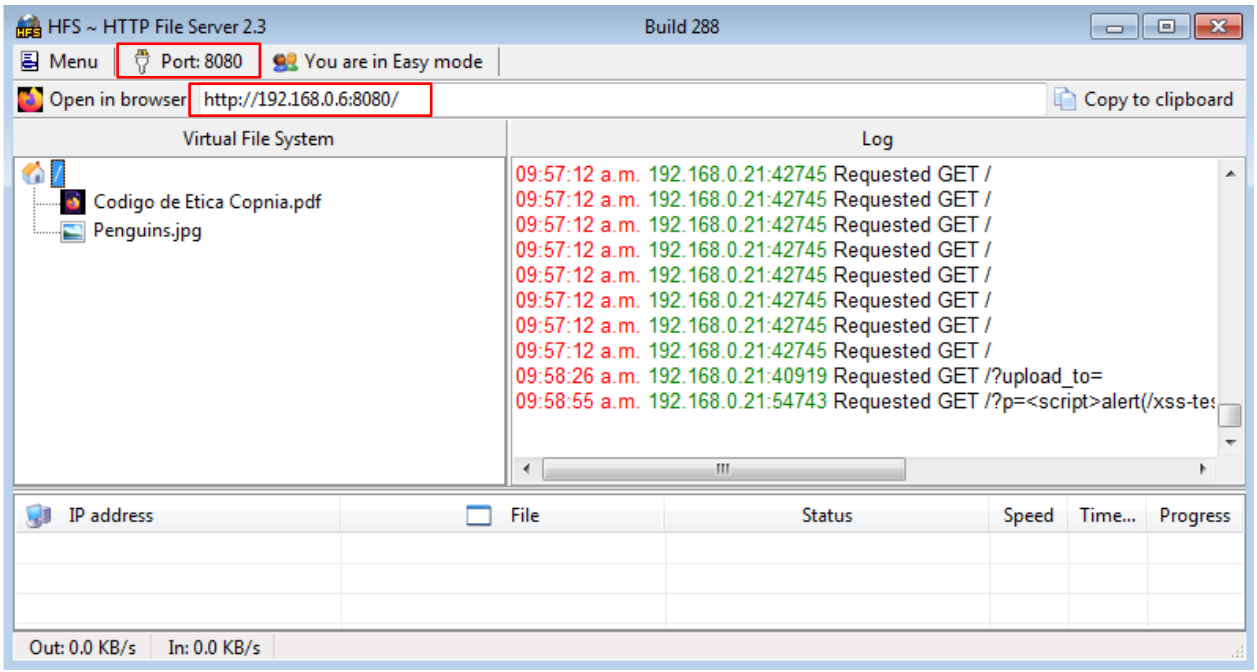
2.3 DESARROLLO DE OBJETIVO 3

- Explotar la vulnerabilidad que contiene mayor impacto en un sistema informático a partir del uso de metodologías y técnicas de intrusión, generar un PoC ante los altos directivos de la compañía – Red Team.

En primera instancia se observa desde la aplicación rejetto v. 2.3 que se encuentra en ejecución desde la “Maquina Objetivo N° 1 Windows 7 64 Bits”, el puerto de comunicación de dicha App es:

- Puerto 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3)

Ilustración 15 Aplicación rejetto v. 2.3



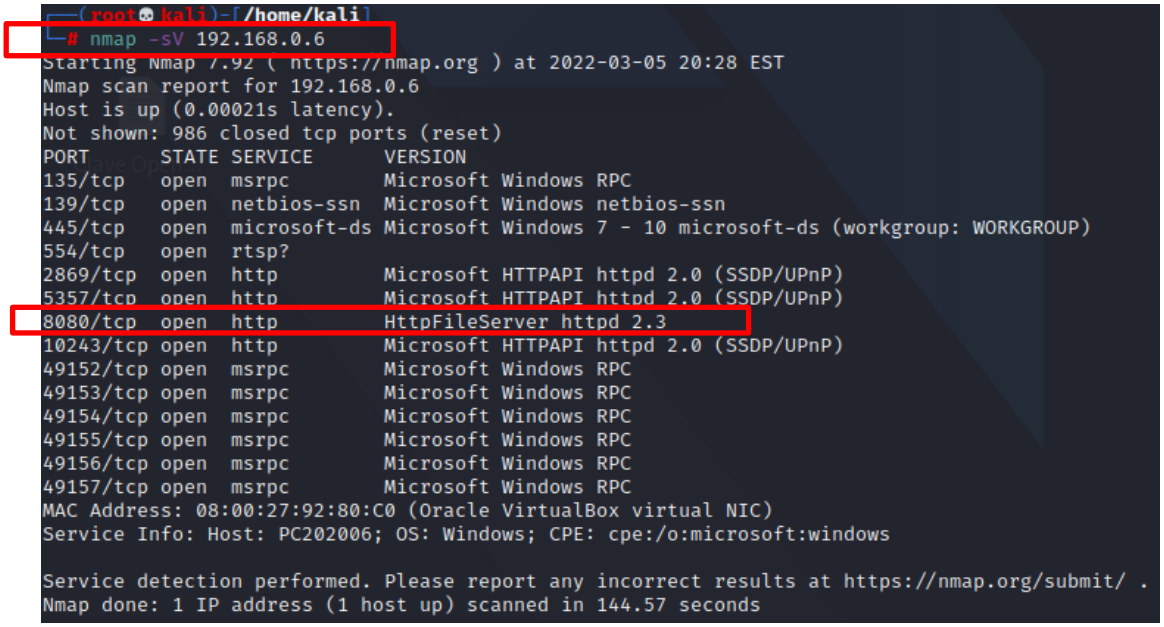
Fuente: Elaboración Propia.

El puerto 8080/TCP que es usado Aplicación rejetto v. 2.3 contiene un rango de Severidad Alta (9.8) dada a la gran cantidad de vulnerabilidades críticas que contiene este puerto / protocoló (Http).

Se realiza Escaneo de Puertos – Detección de Versiones a cada uno de los dispositivos conectados a la Red 192.168.0.1/24 por medio de Nmap. Donde se evidencia la dirección IP 192.168.0.6 que corresponde a la maquina Objetivo N° 1 Windows 7 64 Bits, a la vez se evidencia una serie de datos importantes como lo son:

- Puerto 8080/TCP – Open – Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Ilustración 16 Escaneo – Detección Vr Puertos Maquina Objetivo N° 1



Elaboración Propia

Por medio de OpenVas, se identifica 4 vulnerabilidades importantes sobre el puerto 8080/TCP.

Ilustración 17 Vulnerabilidades Identificadas

Vulnerability	Severity ▾	QoD	Host IP	Host Name	Location
HTTP File Server Remote Command Execution Vulnerability-02 Jan16	9.8 (High)	80 %	192.168.0.6		8080/tcp
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	8.1 (High)	95 %	192.168.0.6		445/tcp
HTTP File Server Remote Command Execution Vulnerability-01 Jan16	7.5 (High)	80 %	192.168.0.6		8080/tcp
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.0.6		135/tcp
Missing `httpOnly` Cookie Attribute	5.0 (Medium)	80 %	192.168.0.6		8080/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.0.6		8080/tcp
TCP timestamps	2.6 (Low)	80 %	192.168.0.6		general/tcp

Fuente: Elaboración Propia.

Entre estas vulnerabilidades del puerto 8080/TCP están:

- Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-02 Jan16.
- Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-01 Jan16.
- Vulnerabilidad - Missing `httpOnly` Cookie Attribute.
- Vulnerabilidad - Cleartext Transmission of Sensitive Information via HTTP.

- Fase N° 3 Pentesting - Acceso al Sistema:

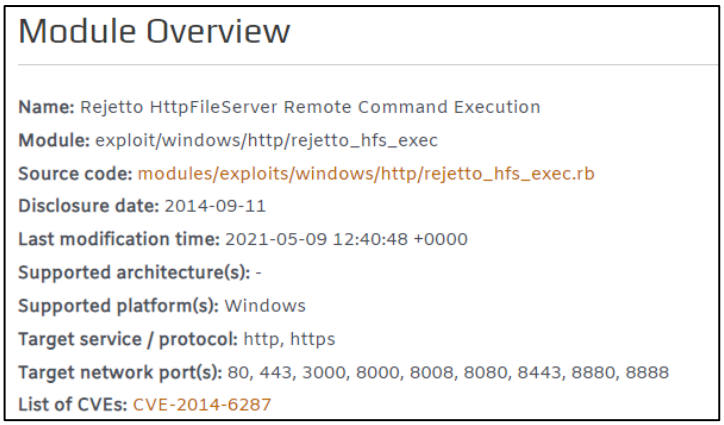
El objetivo a atacar es la “Maquina Objetivo N° 1 Windows 7 64 Bits” por medio de las vulnerabilidades halladas en el puerto 8080/TCP que es usado Aplicación rejetto v. 2.3, contiene un rango de Severidad Alta (9.8) dada a la gran cantidad de vulnerabilidades críticas (4) que contiene este puerto / protocoló (Http).

Por medio de la página Web InfosecMatter da a conocer a detalle de que se compone el Exploit “Rejetto HttpFileServer Remote Command Execution – Metasploit - exploit/windows/http/rejetto_hfs_exec” en donde da a conocer un item importante como lo es:

“Rejetto HttpFileServer (HFS) es vulnerable a un ataque de ejecución remota de comandos debido a una mala expresión regular en el archivo ParserLib.pas. Este módulo explota los comandos de secuencias de comandos HFS mediante el uso de '%00' para omitir el filtrado. Este módulo ha sido probado con éxito en HFS 2.3b sobre Windows XP SP3, Windows 7 SP1 y Windows 8”[22], por medio del puerto 8080/TCP Http (80/TCP Http), obteniendo acceso remoto a la maquina objetivo.

[22] INFOSECMATTER. Rejetto HttpFileServer Ejecución remota de comandos - Metasploit**.** [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/http/rejetto_hfs_exec

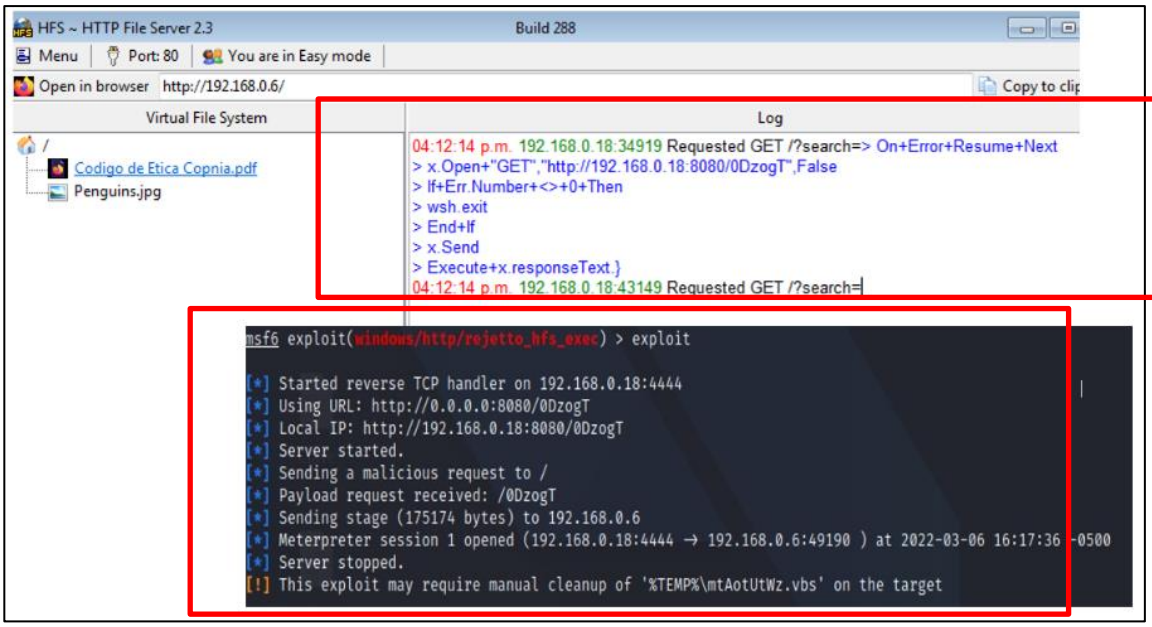
Ilustración 18 Información Exploit Rejetto



Fuente: INFOSECMATTER. Rejetto HttpFileServer Ejecución remota de comandos - Metasploit**.** [imagen]. [Consulta: 20 de marzo 2022]. Disponible en: https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/windows/http/rejetto_hfs_exec

Por medio de la **Ilustración 19 Ejecución Exploit Vs Log HFS**, se observa el script del exploit que se ejecuta dentro de la aplicación HFS (Rejetto v. 2.3) y así explotar las vulnerabilidades de dicha y obtener acceso remoto a la maquina objetivo “Windows 7 64 Bits”.

Ilustración 19 Ejecución Exploit Vs Log HFS



Fuente: Elaboración Propia.

Por medio del Software Kali Linux, se ejecuta la herramienta Metasploit atraves del comando “msfconsole”.

Ilustración 20 Ejecución Metasploit

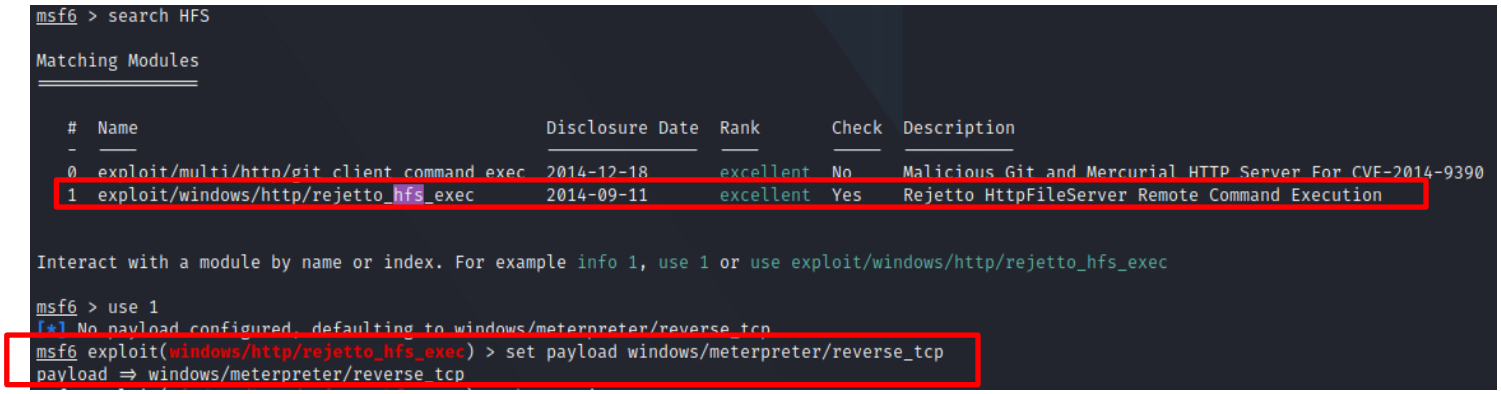
Fuente: Elaboración Propia.

Se realiza la búsqueda de exploit sobre la aplicación HFS (Rejetto HttpFileServer) en donde se encuentra y se selecciona el exploit:

- exploit/windows/http/rejetto_hfs_exec - Rejetto HttpFileServer Remote Command Execution”

Se configura el payload “windows/meterpreter/reverse_tcp”.

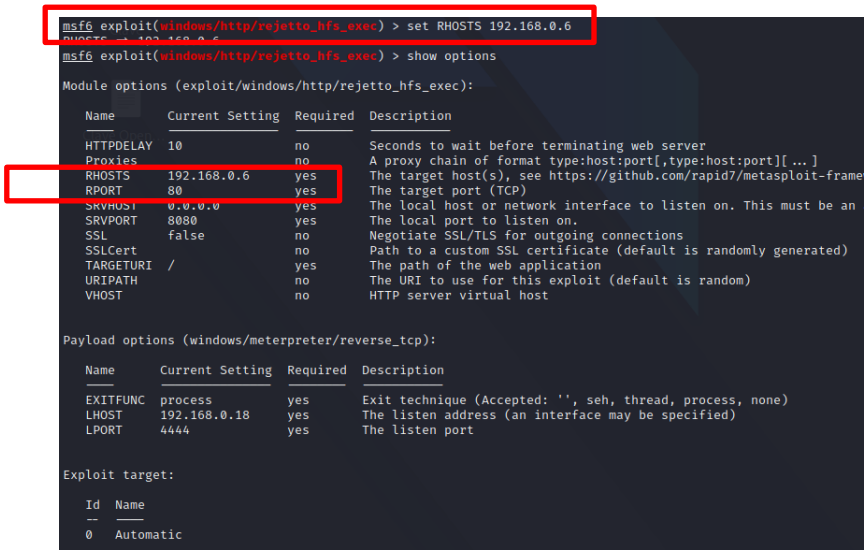
Ilustración 21 Search Exploit HFS



Fuente: Elaboración Propia.

Se realiza configuración del RHOSTS, que corresponde a la IP de la maquina objetivo, en este caso la dirección IP 192.168.0.6.

Ilustración 22 Options Exploit HFS

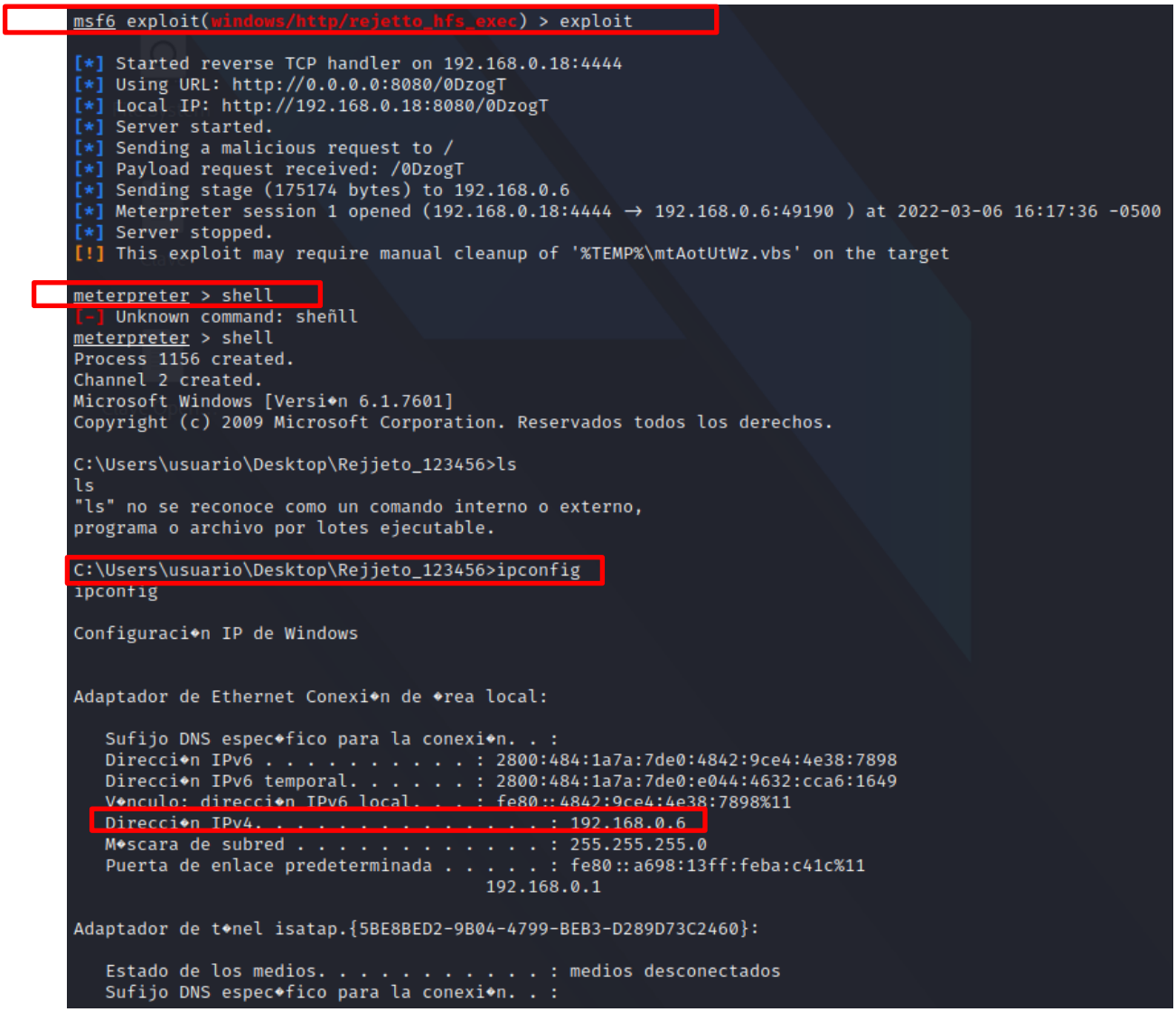


Fuente: Elaboración Propia.

Se realiza la ejecución del exploit “exploit/windows/http/rejetto_hfs_exec” hacia la maquina objetivo “Windows 7 64 Bits – 192.168.0.6” la cual contiene en ejecución la aplicación HFS - Aplicación rejetto v. 2.3.

Por medio del comando “Shell”, obtenemos una sesión hacia la maquina objetivo, por medio del comando “ipconfig”, observamos la dirección IP de la maquina objetivo “192.168.0.6

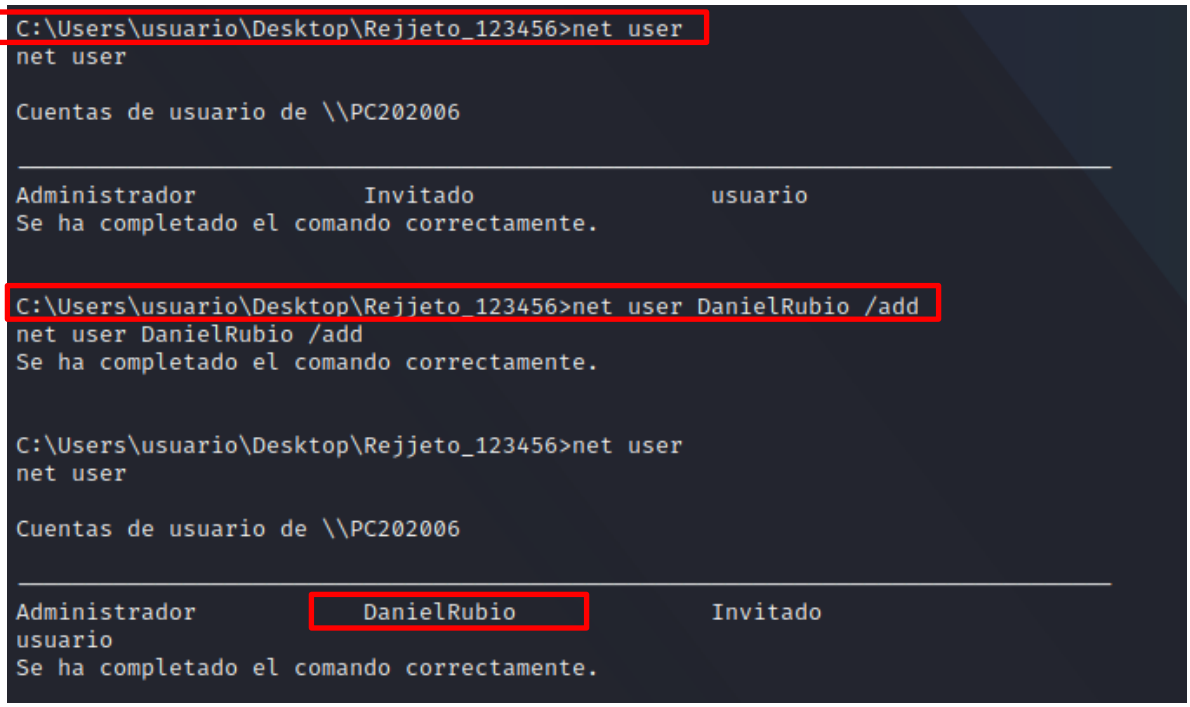
Ilustración 23 Ejecución Exploit



Fuente: Elaboración Propia.

Se realiza la creación de usuario “DanielRubio” en la maquina objetivo “Windows 7 64 Bits – 192.168.0.6” desde la maquina atacante “Kali Linux – 192.168.0.18”, como PoC ante los altos directivos de la compañía.

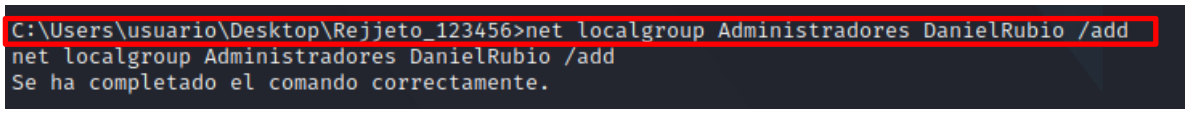
Ilustración 24 Creación de Usuario



Fuente: Elaboración Propia.

Se configura usuario “DanielRubio” como administrador

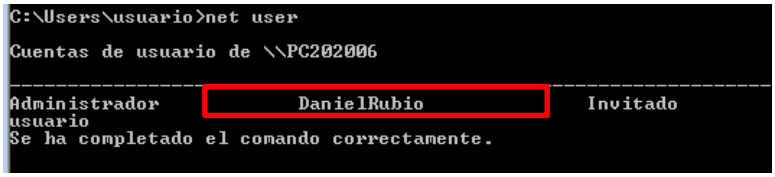
Ilustración 25 Configuración Usuario Administrador



Fuente: Elaboración Propia.

Desde CMD de la maquina objetivo “Windows 7 64 Bits – 192.168.0.6”, se valida creación de usuario “DanielRubio”.

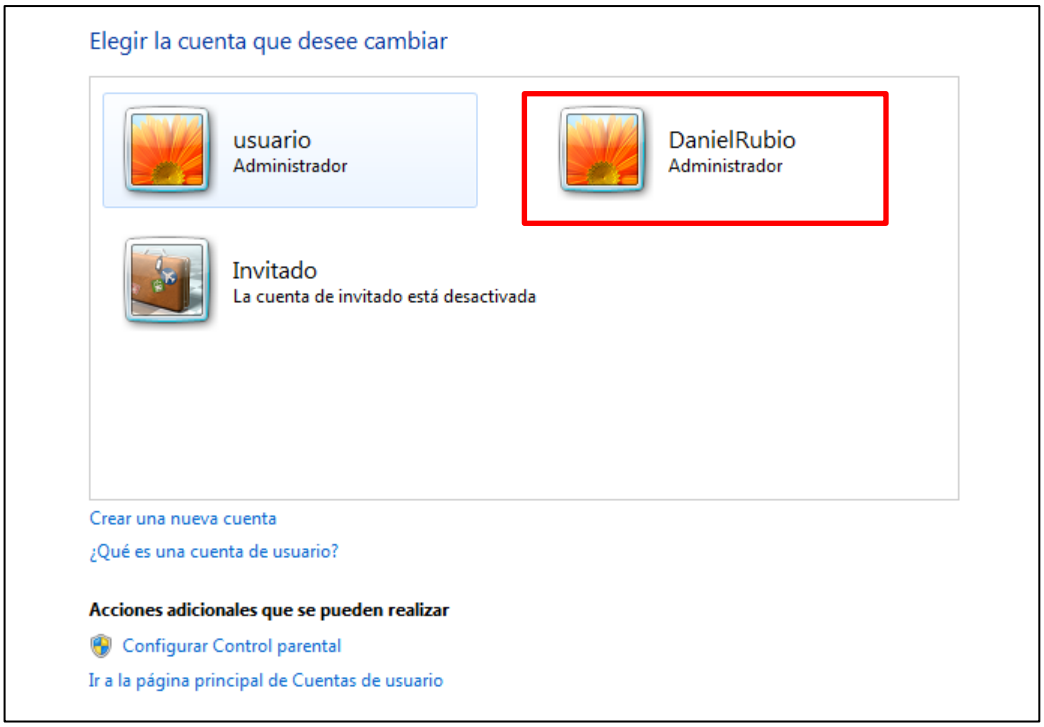
Ilustración 26 Validación Creación Usuario



Fuente: Elaboración Propia.

Por medio del panel de control de la de la maquina objetivo “Windows 7 64 Bits – 192.168.0.6”, se valida que el usuario “DanielRubio” contiene los privilegios de administrador.

Ilustración 27 Validación Privilegios Usuario



Fuente: Elaboración Propia.

2.4 DESARROLLO DE OBJETIVO 4

- Formular e implementar estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI – Blue Team

Analisis de Hardening – Blue Team.

Teniendo en cuenta las diferentes vulnerabilidades identificadas en la Maquina Objetivo (Windows 7 64 Bits) por medio de las herramientas OpenVas y Nessus; se investiga las posibles soluciones ante la mitigación de cada una de estas vulnerabilidades y ejecutar el proceso de Hardening para aumentar el nivel de seguridad de la maquina objetivo.

Remediación Vulnerabilidades OpenVas:

- **Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-02 Jan16.**

  Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

- **Vulnerabilidad – Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)**

  Remediación – Actualización: Actualizar Sistema operativo con la última versión de Security Updates.

- **Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-01 Jan16.**

  Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

- **Vulnerabilidad - DCE/RPC and MSRPC Services Enumeration Reporting.**

  Remediación – Mitigación: Filtre el tráfico entrante a estos puertos (135, 49152, 49153, 49154, 49155, 49156 y 49157).

- **Vulnerabilidad - Missing `httpOnly` Cookie Attribute.**

  Remediación – Mitigación: Establezca el atributo 'httpOnly' para cualquier cookie de sesión.

- **Vulnerabilidad - Cleartext Transmission of Sensitive Information via HTTP**

  Remediación – Solución Alterna: Detener el uso del protocolo Http y usar el protocolo seguro Https (SSL/TLS).

- **Vulnerabilidad - TCP timestamps.**

  Remediación – Mitigación: Deshabilitar el tiempo de actividad en el host remoto, mediante los siguientes comandos.

  Linux: add the line 'net.ipv4.tcp_timestamps = 0' to/etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

  Windows: execute 'netsh int tcp set global timestamps=disabled'

  Por defecto en el puerto TCP/IP en el Host esta deshabilitada la opción “Tiempo de Actividad” cuando se inicia las conexiones TCP.

Remediación Vulnerabilidades Nessus:

- **Vulnerabilidad - CGI Generic Cookie Injection Scripting.**

  Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

- **Vulnerabilidad - CGI Generic HTML Injection (quick test).**

  Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

- **Vulnerabilidad - CGI Generic XSS (quick test).**

  Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

- **Vulnerabilidad - Web Application Potentially Vulnerable to Clickjacking.**

  Remediación – Mitigación: Devuelve el encabezado HTTP X-Frame-Options o Content-Security-Policy (con la directiva 'frame-ancestors') con la respuesta de la página. Esto evita que otro sitio represente el contenido de la página cuando se usan las etiquetas HTML de marco o IFRAME.

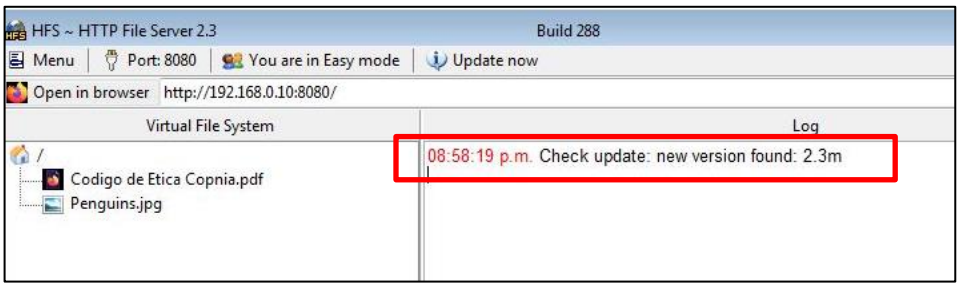
- **Vulnerabilidad - Web Server Uses Basic Authentication Without HTTPS.**

  Remediación – Solución Alterna: Detener el uso del protocolo Http y usar el protocolo seguro Https (SSL/TLS).

Implementación de Hardening – Blue Team.

Primera Acción: Descargar e instalación de la última versión disponible de la aplicación Rejjeto (En este caso no permite la descargar de la actualización por error en la plataforma).

Ilustración 28 Actualización de Rejjeto



Fuente: Elaboración Propia.

Segunda Acción: Activación del Sistema Operativo, para acceder a las actualizaciones del sistema operativo.

Ilustración 29 SO - No Activo

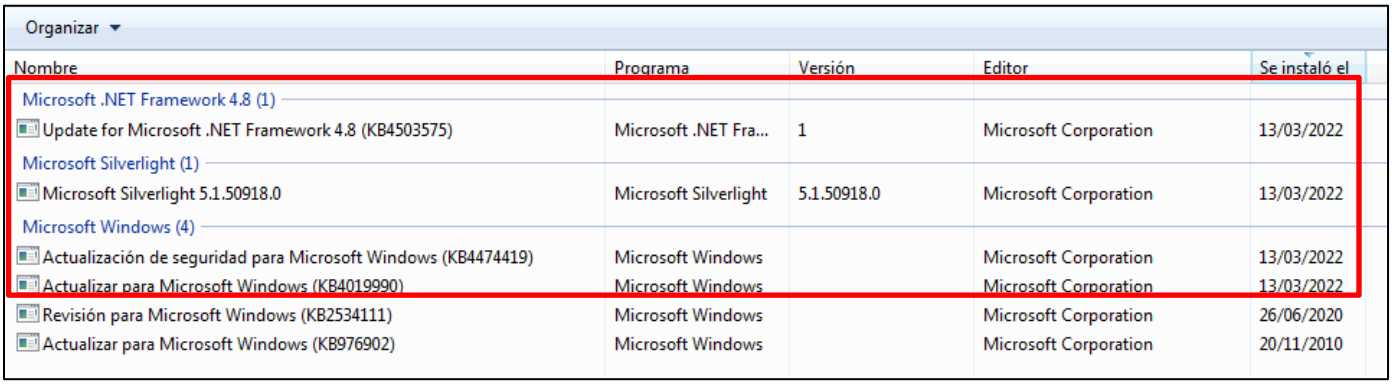
Fuente: Elaboración Propia.

Ilustración 30 SO Activo

Fuente: Elaboración Propia.

Tercera Acción: Actualización de Sistema Operativo (Security Updates).

Ilustración 31 Actualizaciones Instaladas SO



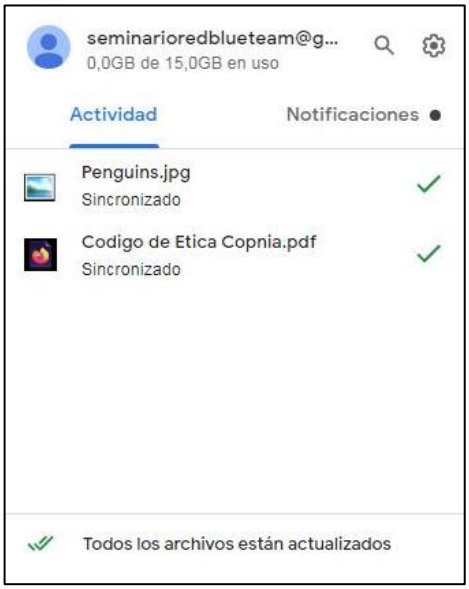
Fuente: Elaboración Propia.

Cuarta Acción: Uso de Almacenamiento en la Nube Google Drive, en sustitución a la aplicación rejetto v. 2.3. Se accede a los recursos almacenados de manera segura desde el equipo o desde la página oficial de Google Drive.

Ilustración 32 Instalación de Google Drive

Fuente: Elaboración Propia.

Ilustración 33 Contenido Almacenado en Google Drive



Fuente: Elaboración Propia.

2.5 DESARROLLO DE OBJETIVO 5

- Evaluar el nivel de seguridad de una Infraestructura Tecnológica luego de la implementación de las estrategias basadas en metodologías de ciberseguridad Red Team y Blue Team, para conocer su impacto en el aumento del nivel de seguridad final en base al nivel inicial.

Se aborda la última Fase de Pentesting:

- Fase N° 4 Pestenting - Elaboración de Informe: Se abordan el análisis de los resultados obtenidos dando a conocer el alcance e impacto de cada una de las brechas de seguridad de dicho sistema informático.

Durante esta etapa, se propone realizar la presentación ejecutiva y técnica de los resultados de las pruebas de Pentesting realizadas en las diferentes entidades y activos tecnológicos designados, además es la Etapa más importante de las Penetration Testing acorde al Framework "ADALID Corp" dado que en dicho informe se encuentra todo el trabajo realizado de Penetration Testing sobre la evaluación del estado de seguridad de la Infraestructura Tecnológica de la compañía WhiteHouse Security.

En el informe de resultados se detalla minuciosamente cada vulnerabilidad identificada en la Maquina Objetivo, se clasifican por calificación del Riego según Offensive Security "De acuerdo con NIST SP 800-30, las vulnerabilidades explotadas se clasifican según la probabilidad y el impacto para determinar el riesgo general"[23], además se da a conocer la descripción e impacto de la vulnerabilidad, y mitigación de ella.

Se usa el formato de Detalle de vulnerabilidades y mitigación del documento Offensive Security[24], para dar a conocer los resultados de la evaluación del estado de seguridad de la Infraestructura Tecnológica de la compañía WhiteHouse Security a los dirigentes de ella, para sus posteriores diseños e implementación de salvaguardas que eliminen o mitiguen el porcentaje de probabilidad de materialización de la vulnerabilidad hallada en dichas Penetration Testing.

Escala de Calificación de Riesgo: De acuerdo con NIST SP 800-30, las vulnerabilidades explotadas se clasifican según la probabilidad y el impacto para determinar el riesgo general.

[23] OFFENSIVE SECURITY. Penetration Test Report. [en línea]. [Consulta: 20 de noviembre 2022]. Recuperado de https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

[24] Idem.

Vulnerabilidades Identificadas – OpenVas:

Cuadro 1 Vulnerabilidad N° 1 - OpenVas

Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-02 Jan16 Severidad: Alto (9.8) Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3). Descripción: El servidor de archivos HTTP esta propenso a una vulnerabilidad de ejecución remota de comandos (RCE). Impacto: La explotación exitosa permitirá una atacante para ejecutar código arbitrario cargando un archivo con ciertos datos no válidos. Secuencias de bytes UTF-8 que se interpretan como símbolos de macro ejecutables. Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

Fuente: Elaboración Propia

Cuadro 2 Vulnerabilidad N° 2 - OpenVas

Vulnerabilidad – Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Severidad: Alta (8.1)

Puerto Afectado: 455/TCP (Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)).

Descripción: El host le falta una seguridad crítica actualización según Microsoft Bulletin MS17-010.

Impacto: La explotación exitosa permitirá remotamente obtener la capacidad de ejecutar código en el servidor de destino, también podría dar lugar a la divulgación de información del servidor

Remediación – Actualización: Actualizar Sistema operativo con la última versión de Security Updates.

Fuente: Elaboración Propia

Cuadro 3 Vulnerabilidad N° 3 - OpenVas

Vulnerabilidad - HTTP File Server Remote Command Execution Vulnerability-01 Jan16.

Severidad: Alta (7.5)

Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: El servidor de archivos HTTP esta propenso a una vulnerabilidad de ejecución remota de comandos (RCE).

Impacto: La explotación exitosa permitirá una atacante para ejecutar código arbitrario cargando un archivo con ciertos datos no válidos.

Secuencias de bytes UTF-8 que se interpretan como símbolos de macro ejecutables.

Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

Fuente: Elaboración Propia

Cuadro 4 Vulnerabilidad N° 4 - OpenVas

Vulnerabilidad - DCE/RPC and MSRPC Services Enumeration Reporting.

Severidad: Medio (5.0)

Puerto Afectado: 135/TCP (epmap).

Descripción: Entorno informático distribuido/llamadas a procedimientos remotos (DCE/RPC) o servicios MSRPC en ejecución en el host remoto se puede enumerar conectándose al puerto 135 y realizando las consultas correspondientes.

Impacto: Un atacante puede usar este hecho para obtener más conocimiento sobre el host remoto.

Remediación – Mitigación: Filtre el tráfico entrante a estos puertos (135, 49152, 49153, 49154, 49155, 49156 y 49157).

Fuente: Elaboración Propia

Cuadro 5 Vulnerabilidad N° 5 - OpenVas

Vulnerabilidad - Missing `httpOnly` Cookie Attribute.

Severidad: Medio (5.0)

Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: A la aplicación le falta el atributo de cookie 'httpOnly'.

Impacto: Application with session handling in cookies.

Remediación – Mitigación: Establezca el atributo 'httpOnly' para cualquier cookie de sesión.

Fuente: Elaboración Propia

Cuadro 6 Vulnerabilidad N° 6 - OpenVas

Vulnerabilidad - Cleartext Transmission of Sensitive Information via HTTP

Severidad: Medio (4.8)

Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: El host / aplicación transmite información sensible (usuarios/Password) en texto claro a través de HTTP (Sin encriptación).

Impacto: Un atacante podría usar esta situación para comprometer o espiar el Comunicación HTTP entre el cliente y el servidor usando un ataque man-in-the-middle para obtener acceso a datos confidenciales como nombres de usuario o contraseñas.

Remediación – Solución Alterna: Detener el uso del protocolo Http y usar el protocolo seguro Https (SSL/TLS).

Fuente: Elaboración Propia

Cuadro 7 Vulnerabilidad N° 7 - OpenVas

Vulnerabilidad - TCP timestamps.

Severidad: Low (2.6)

Puerto Afectado: General/TCP

Descripción: El host remoto implementa marcas de tiempo TCP, por lo tanto, permite calcular el tiempo de actividad.

Impacto: Un lado del efecto de esta característica es que el tiempo de actividad del host remoto pueda ser calculado por el atacante.

Remediación – Mitigación: Deshabilitar el tiempo de actividad en el host remoto, mediante los siguientes comandos.

Linux: add the line 'net.ipv4.tcp_timestamps = 0' to/etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

Windows: execute 'netsh int tcp set global timestamps=disabled'

Por defecto en el puerto TCP/IP en el Host esta deshabilitada la opción “Tiempo de Actividad” cuando se inicia las conexiones TCP.

Fuente: Elaboración Propia

Vulnerabilidades Identificadas – Nessus:

Cuadro 8 Vulnerabilidad N° 1 - Nessus

Vulnerabilidad - CGI Generic Cookie Injection Scripting. Severidad: Media (4.3) Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3). Descripción: El servidor Web remoto contiene un script CGI que no desinfecta adecuadamente las cadenas de solicitud con JavaScript malicioso. Impacto: Un atacante inyecta cookies arbitrarias, obteniendo un ataque “fijación de sensación”. Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

Fuente: Elaboración Propia

Cuadro 9 Vulnerabilidad N° 2 - Nessus

Vulnerabilidad - CGI Generic HTML Injection (quick test).

Severidad: Media (4.3)

Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: El servidor Web remoto contiene un script CGI que no desinfecta adecuadamente las cadenas de solicitud con JavaScript malicioso.

Impacto: Un atacante ejecuta HTML arbitrario, generando que el servidor pueda ser vulnerable ante inyecciones de “IFRAME”.

Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

Fuente: Elaboración Propia

Cuadro 10 Vulnerabilidad N° 3 - Nessus

Vulnerabilidad - CGI Generic XSS (quick test).

Severidad: Media (4.3)

Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: El servidor Web remoto contiene un script CGI que no desinfecta adecuadamente las cadenas de solicitud con JavaScript malicioso.

Impacto: Un atacante ejecuta codigo script y HTML arbitrario, generando que el servidor pueda ser vulnerable en secuencias de comandos entre sitios.

Remediación – No Contiene Fix: No se contiene una solución o Fix ante esta vulnerabilidad, lo recomendable es actualizar la versión rejetto v. 2.3 o ser reemplazado por otro producto (Uso de almacenamiento en la Nube Google Drive o OneDrive).

Fuente: Elaboración Propia

Cuadro 11 Vulnerabilidad N° 4 - Nessus

Vulnerabilidad - Web Application Potentially Vulnerable to Clickjacking.

Severidad: Media (4.3)

Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: Un encabezado de respuesta X-Frame-Options o un encabezado de respuesta Content-Security-Policy 'frame-ancestors' en todas las respuestas de contenido.

Impacto: Exposición a ataques de secuestro de “clics”, generando que la víctima realice transacciones fráudenlas o acciones maliciosas sin su consentimiento.

Remediación – Mitigación: Devuelve el encabezado HTTP X-Frame-Options o Content-Security-Policy (con la directiva 'frame-ancestors') con la respuesta de la página. Esto evita que otro sitio represente el contenido de la página cuando se usan las etiquetas HTML de marco o IFRAME.

Fuente: Elaboración Propia

Cuadro 12 Vulnerabilidad N° 5 - Nessus

Vulnerabilidad - Web Server Uses Basic Authentication Without HTTPS.

Severidad: Media (4.3)

Puerto Afectado: 8080/TCP (Http – HttpFileServer httpd 2.3 (Aplicación rejetto v. 2.3).

Descripción: El servidor Web remoto contiene varias páginas Web con protocolo Http, texto no cifrado.

Impacto: Un ataque puede acceder al tráfico entre el servidor y el usuario, obteniendo usuarios y Password en texto claro.

Remediación – Solución Alterna: Detener el uso del protocolo Http y usar el protocolo seguro Https (SSL/TLS).

Fuente: Elaboración Propia

Resultados de Hardening – Blue Team.

Luego de la implementación de las acciones de Hardening en la maquina objetivo, se realiza de nuevo un analisis de vulnerabilidades por medio de las herramientas OpenVas y Nessus, y así conocer el nivel de seguridad actual luego de la ejecución de Hardening.

Resultados de Hardening – OpenVas.

Luego implementación de Hardening, se ejecuta la Tarea 1 “Analisis de Vulnerabilidades - Windows 7 64 Bits” hacia el Objetivo, desde la herramienta OpenVas se observa que el rango de Severidad General Alta (9.8) pasa a Media (5.0) luego de la ejecución de Hardening. Aumentando el nivel de seguridad de la maquina objetivo.

Ilustración 34 OpenVas Resultados.

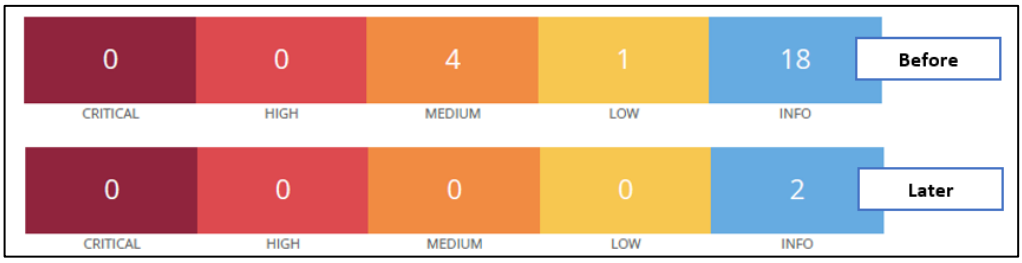
Status	Task	Severity	High	Medium	Low	Log	False Pos.
Done	Analisis de Vulnerabilidades - Windows 7 64 Bits	5.0 (Medium)	0	1	1	22	0
Done	Analisis de Vulnerabilidades - Windows 7 64 Bits	9.8 (High)	3	3	1	30	0

Fuente: Elaboración Propia.

Resultados de Hardening – Nessus.

Después implementación de Hardening, se ejecuta la Tarea 1 “Web Application Tests Windows 7 64 Bits” hacia el Objetivo”, la herramienta Nessus pasa de identificar 5 Vulnerabilidades a “0” Vulnerabilidades.

Ilustración 35 Nessus Resultados



Fuente: Elaboración Propia.

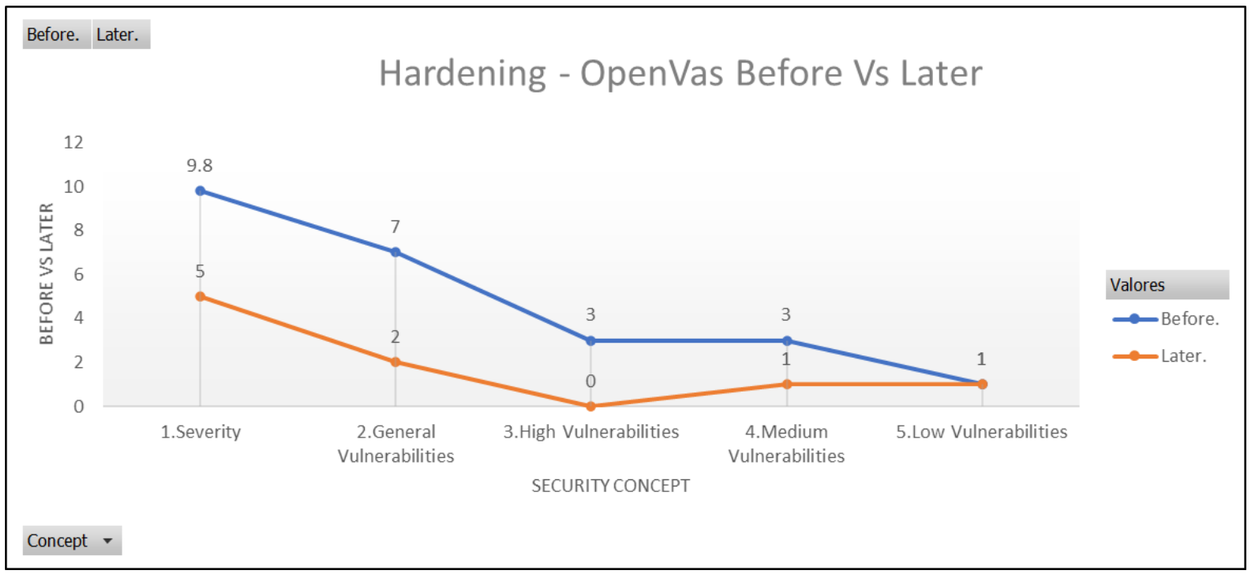
Resultados de Hardening – Blue Team.

Cuadro 13 Hardening OpenVas

Hardening OpenVas				
Concept	**Before**	**Later**	**Decrease Percentage**	**Increase Percentage**
1.Severity	9.8	5	48.97%	0%
2.General Vulnerabilities	7	2	71.42%	0%
3.High Vulnerabilities	3	0	100%	0%
4.Medium Vulnerabilities	3	1	66.66%	0%
5.Low Vulnerabilities	1	1	0%	0%

Fuente: Elaboración Propia.

Ilustración 36 Hardening - OpenVas Before Vs Later



Fuente: Elaboración Propia.

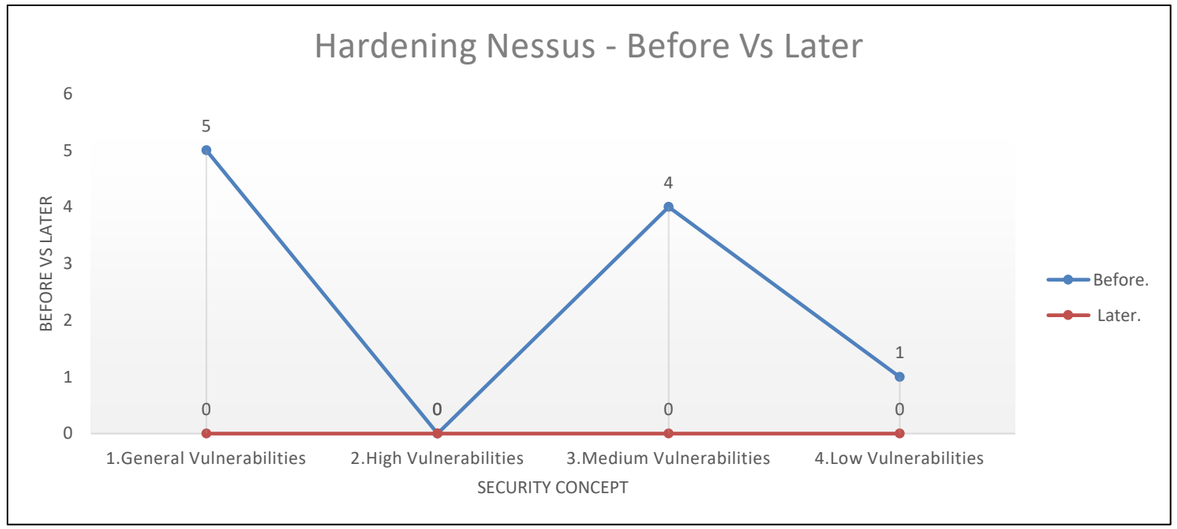
-

Cuadro 14 Hardening Nessus

Hardening Nessus				
Concept	**Before**	**Later**	**Decrease Percentage**	**Increase Percentage**
1.General Vulnerabilities	5	0	100%	0%
2.High Vulnerabilities	0	0	0%	0%
3.Medium Vulnerabilities	4	0	100%	0%
4.Low Vulnerabilities	1	0	100%	0%

Fuente: Elaboración Propia.

Ilustración 37 Hardening - Nessus Before Vs Later



Fuente: Elaboración Propia.

En conclusión, se evidencia una disminución considerable en las vulnerabilidades identificadas por Red Team, luego del analisis e implementación de Hardening en la maquina objetivo.

Como se observa en la **Ilustración 36 Hardening - OpenVas Before Vs Later** el Rango de Severidad General pasa de Alta (9.8) a Media (5.0) y la cantidad de Vulnerabilidades identificas por OpenVas pasa de 7 a 2. En base al **Cuadro 13 Hardening OpenVas** se evidencia una reducción porcentual de 100% (High Vulnerabilities), 71.42% (General Vulnerabilities), 66.66% (Medium Vulnerabilities) y 48.97% (Severity), con un aumento porcentual General de 0%.

Junto a la **Ilustración 37 Hardening - Nessus Before Vs Later** se evidencia la cantidad de vulnerabilidades identificas por Nessus pasa de 5 a 0. Respecto al **Cuadro 14 Hardening Nessus** se observa una reducción porcentual de 100% (General Vulnerabilities, Medium Vulnerabilities y Low Vulnerabilities), con un aumento porcentual General de 0%.

Con la reducción de vulnerabilidades y brechas de seguridad presentes en la Maquina Objetivo Windows 7 64 Bits, aumenta el nivel de seguridad y esto conlleva a la disminución de incidentes de seguridad.

Reporte OpenVas – Antes de la Implementación de Hardening:

Link:https://drive.google.com/file/d/1CKsqNdb7evZf-claZR018-XFz7rMO2jc/view?usp=sharing

Reporte Nessus – Antes de la Implementación de Hardening:

Link:https://drive.google.com/file/d/1BojD27_JrYXQvSi5eQx0uyYhwCpaa9It/view?usp=sharing

Reporte OpenVas – Después de la Implementación de Hardening:

Link:https://drive.google.com/file/d/1CKJeB_j34vJXAxMtz3nMeJBu-bZ_nmnF/view?usp=sharing

Reporte Nessus – Después de la Implementación de Hardening:

Link:https://drive.google.com/file/d/1C0sApzeK20BILS8b5u6P4rPNy5M2XjJi/view?usp=sharing

3 CONCLUSIONES

A partir del planteamiento del problema ¿Cómo la implementación de estrategias como Red y Blue team, contribuyen en mejorar la ciberseguridad de la infraestructura TI de una organización?, se desarrolla cada uno de los objetivos propuestos, bajo pruebas de intrusión e implementación de estrategias de Hardening en un ambiente controlado.

Red Team es un conjunto de Profesionales enfocados a identificar cada una de las vulnerabilidades y brechas de seguridad presentes en un sistema o infraestructura determinada, a la vez de valorar el nivel de seguridad de cada uno de las salvaguardas presentes en dicha Infraestructura. Red Team es considerado un Equipo Ofensivo, dado en la forma de ejecución de sus funciones y procesos, pensando y actuando de la misma manera que lo haría un ciberdelincuente, con su cualidad de “proactividad”, estando un paso más adelante sobre las acciones del ciberdelincuente.

Red Team se apoya de varias herramientas enfocadas al hallazgo y explotación de vulnerabilidades presentes en diferentes entornos que componen una Infraestructura, como lo son la Red, Bases de Datos y Sitios Web; comprometiendo los activos importantes para dicha Infraestructura, por medio de la ejecución de amenazas diseñadas a explotar cada tipo de vulnerabilidad presente, afectando la Integridad, Confidencialidad y Disponibilidad de la información sensible que procesa, transmite o almacena dicho activo. Los resultados obtenidos, luego de la ejecución de las pruebas de Intrusión, depende del alcance de Red Team pactado en el inicio del proyecto bajo contrato, donde se da a conocer el tipo de Pentesting (Black Box, White Box and Gray Box) y periodicidad a implementar.

Se dan a conocer los resultados de las pruebas implementadas, los cuales son dados a conocer a Blue Team (Defensivo), donde en conjunto con Red Team, logran obtener un sistema de seguridad alto y compacto, por medio de las cualidades y herramientas que definen cada uno de estos dos Equipos, cuyo objetivo final es la identificación de vulnerabilidades y brechas de seguridad, diseño e implementación de salvaguardas y evaluar el nivel de seguridad de estos controles, teniendo en cuenta las vulnerabilidades antes halladas. La implementación Red Team en una Infraestructura Tecnológica es prácticamente estar bajo ataque en todo momento, pero de manera controlada; pero lo importante aquí, es que este ataque no genera daño o impacto negativo, si no un impacto positivo a la mejora del Nivel de Seguridad.

En base a la pregunta planteada, las estrategias basadas en metodologías de ciberseguridad Red Team y Blue Team, permiten evaluar un sistema informático y aumentar el nivel de seguridad de dicho sistema por medio de la identificación y gestión de vulnerabilidades.

4 RECOMENDACIONES

La Era Digital, con el pasar del tiempo, ha venido incrementado su uso en la vida cotidiana de los seres humanos, dado a las cualidades que da a sus usuarios, al ofrecer una vida mucho más fácil y sencilla; estas características van ligadas a pequeñas y grandes Infraestructuras Tecnológicas que otorgan muchas más funciones, pero de manera masiva a diferentes entornos y áreas.

En la gran parte de estos servicios que ofrece la Era Digital, se encuentra información sensible de personas tanto compañías, como lo son datos personales, bancarios y credenciales de acceso a diferentes sitios Web; donde los ciberdelincuentes utilizan diferentes metodos de identificación y explotación de vulnerabilidades en dichas Infraestructuras, para lograr obtener su cometido.

Teniendo en cuenta lo mencionado, se sugiere la implementación de las estrategias basadas en metodologías de ciberseguridad Red Team y Blue Team de manera periódica sobre estas Infraestructuras, cuyo objetivo es estar a la Defensiva ante nuevas técnicas de ataque, por medio de la identificación proactiva de vulnerabilidades y brechas de seguridad presentes en dicho sistema, por medio de herramientas diseñadas para tal fin. Dado que, junto a la evolución de la Era Digital, surgen nuevas vulnerabilidades y amenazas que son usadas por los Ciberdelincuentes, por ende, Red Team permite identificar o incursionar estas brechas de seguridad antes que los Ciberdelincuentes; y así Blue Team diseñar e implementar los Salvaguardas correspondientes para cerrar dicha vulnerabilidad identificada desde Red Team.

BIBLIOGRAFÍA

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. [en línea]. [Consulta: 20 de marzo 2022]. Recuperado de http://ticbogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

ALCALDIA MAYOR DE BOGOTA DC. Ley 1273 del 2009. [en línea]. [Consulta: 20 de marzo 2022]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

ALTUVE VERA, Rafael. Qué es OpenVas. [en línea]. [Consulta: 2 de marzo 2022]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

ALVAREZ, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

AMBIT TEAM. ¿Qué significa SIEM y cómo funciona? [en línea]. [Consulta: 11 de marzo 2022]. Recuperado de: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

AVAST**.** Malware y Tipos. [en línea]. [Consulta: 20 marzo del 2022]. Disponible en: https://www.avast.com/es-es/c-malware

BRUNO, Diego. (2020). Introducción al Red Team – Parte 1. [en línea]. [Consulta: 20 marzo del 2022] Recuperado de: https://www.blackmantisecurity.com/introduccion-al-red-team-parte-1/

CCNA. Segmentación de VLAN: Introducción. [en línea]. [Consulta: 14 de marzo 2022]. Disponible en: https://ccnadesdecero.es/segmentacion-de-vlan-definicion-y-tipos/

CIBERSEGURIDAD. (2019). ¿Qué es el Pentesting? [en línea]. [Consulta: 8 de febrero 2022]. Recuperado de: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

CIS. Sobre nosotros. [en línea]. [Consulta: 11 de marzo 2022]. Recuperado de: https://www.cisecurity.org/about-us

CODE SPACE. CSIRT y el trabajo de un BlueTeam. [en línea]. [Consulta: 11 de marzo 2022]. Recuperado de: https://codespaceacademy.com/blog/csirt-trabajo-blueteam/

COPNIA. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

COPNIA. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [en línea]. [Consulta: 20 marzo del 2022]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE. CVE-2020-0796. [en línea]. [Consulta: 2 de marzo 2022]. Disponible en: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=2020-0796

CVE. Sobre el Programa CVE. [en línea]. [Consulta: 2 de marzo 2022]. Disponible en: https://www.cve.org/About/Overview

DELOITTE. Pasos a seguir ante un ataque informático. [en línea]. [Consulta: 11 de marzo 2022]. Recuperado de: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

DIGICERT. ¿Qué son SSL, TLS y HTTPS? [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https

DOMINGUEZ AGUILAR, Angie. Firewall de bases de datos. [en línea]. [Consulta: 14 de marzo 2022]. Disponible en: https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

EL TIEMPO. Intermediario de pagos en internet, negocio que crece con poco control [en línea]. [Consulta: 20 de marzo del 2022]. Recuperado de: https://www.eltiempo.com/economia/sector-financiero/intermediarios-de-pagos-por-internet-en-colombia-no-estan-muy-controlados-175320

ESET. Cómo utilizar OpenVas para la evaluación de vulnerabilidades [en línea] (2 de marzo 2022). Recuperado de: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

ESIC. (2018). Red Team: qué es, estrategias y ejemplo de un caso real. [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

ETHICAL HACKING. Red Team vs Blue Team vs Purple Team. [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://blog.ehcgroup.io/2021/09/06/16/56/17/11717/red-team-vs-blue-team-vs-purple-team/hacking/ehacking/

EXEVI. Servicio Pentesting de Webs, Apps y Sistemas [en línea]. [Consultado: 2 de marzo 2022]. Disponible en: https://www.exevi.com/soluciones/servicio-pentesting-de-webs-apps-y-sistemas/

EXPLOIT DATABASE. [en línea] (2 de marzo 2022). Recuperado de: https://www.exploit-db.com/

EXPLOIT DATABASE. Microsoft Windows - 'SMBGhost' Remote Code Execution. [en línea] (2 de marzo 2022). Recuperado de: https://www.exploit-db.com/exploits/48537

F5 GLOSSARY. ¿Qué es un WAF (Web Application Firewall)? [en línea]. [Consulta: 14 de marzo 2022]. Disponible en: https://www.f5.com/es_es/services/resources/glossary/web-application-firewall

HELP SYSTEMS. ¿Qué es un SIEM? [en línea]. [Consulta: 11 de marzo 2022]. Recuperado de: https://www.helpsystems.com/es/blog/que-es-un-siem

INCIBE. (2019). Qué es una DMZ y cómo te puede ayudar a proteger tu empresa. [en línea]. (Consulta: 14 de marzo 2022). Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

INFOSECMATTER. Rejetto HttpFileServer Ejecución remota de comandos - Metasploit**.** [en línea]. [Consulta: 02 de marzo 2022]. Disponible en: https://www.infosecmatter.com/metasploit-module library/?mm=exploit/windows/http/rejetto_hfs_exe

INTERNETPASOAPASO. Exploit: ¿Qué son, para qué sirven y cómo se clasifican este tipo de software informático? [en línea] (2 de marzo 2022). Recuperado de: https://internetpasoapaso.com/exploits

IT DIGITAL SECURITY. (2018) ¿Qué es un Red Team y cuál es su propuesta de valor? Bankia lo tiene claro. [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://www.itdigitalsecurity.es/actualidad/2018/11/que-es-un-red-team-y-cual-es-su-propuesta-de-valor-bankia-lo-tiene-claro

KALITOOLS (2020). Listado de herramientas de Kali Linux. [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://tools.kali.org/tools-listing

MANAGE ENGINE. ¿Qué son los controles de CIS? [en línea]. [Consulta: 11 de marzo 2022]. Recuperado de: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

MINTIC. (2018). Guía de Auditoria. Mintic. (pp. 12-19). [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

MINTIC. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://www.mintic.gov.co/gestionti/615/articles5482_G20_Transicion_IPv4_IPv6.pdf

NEURAL CODERS. ¿Has escuchado del Blue Team y Red Team? [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://www.facebook.com/neuralcoders/posts/800267244120740/

OFFENSIVE SECURITY. Penetration Test Report. [en línea]. [Consulta: 20 de noviembre 2022]. Recuperado de https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

OPTIMITI NETWORK. Equipos de respuesta a incidentes. [en línea]. [Consulta: 11 de marzo 2022]. Recuperado de: https://optimiti.com.mx/equipos-de-respuesta-a-incidentes/

PEÑARREDONDA, José Luis. Detrás de Buggly: la historia de la fachada Andrómeda. [en línea]. [Consulta: 22 de febrero 2022]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

QUINTERO, J. F. (2020). Red Team y Blue Team al interior de una organización. [en línea]. [Consulta: 20 marzo del 2022]. Recuperado de: https://repository.unad.edu.co/handle/10596/35497

REDESBASICO150. Que es el Modelo OSI [en línea]. [Consultado: 14 de marzo 2022]. Disponible en: https://sites.google.com/site/redesbasico150/protocolos-de-red/-que-es-el-modelo-osi

REVISTA SEGURIDAD. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con MetasploitFramework | Revista. Seguridad. [en línea]. [Consulta: 13 de noviembre 2021]. Recuperado de: https://revista.seguridad.unam.mx/numero-19/pruebas-depenetraci%

TXETXU (2015). Pentesting de caja negra, caja blanca y caja gris, diferencias. [en línea]. [Consulta: 2 de marzo 2022]. Recuperado de: http://www.lostinth3net.com/seguridad-hacking/pentesting-caja-negra-caja-blanca-caja-gris-diferencias/

UNAD. Anexo 2 – Escenario 2**.** [en línea]. [Consulta: 16 de febrero 2022]. Disponible en: https://campus107.unad.edu.co/ecbti99/mod/folder/view.php?id=2937

UNAD. Anexo 3 – Acuerdo**.** [en línea]. [Consulta: 16 de febrero 2022]. Disponible en: https://campus107.unad.edu.co/ecbti99/mod/folder/view.php?id=2937

UNAD. Anexo 4 – Escenario 3 [en línea]. [Consulta: 2 de marzo 2022]. Disponible en: https://campus107.unad.edu.co/ecbti99/mod/folder/view.php?id=2939

UNIR. (2020) Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? [en línea]. [Consulta: 01 de octubre 2020]. Recuperado de: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

ANEXO

Link Video Sustentación Seminario Especializado - Equipos Estratégicos en Ciberseguridad - Red Team & Blue Team:

https://youtu.be/BBt9o3yjHDc