SEMINARIO ESPECIALIZADO EQUIPOS ESTRATEGICOS EN SEGURIDAD: RED TEAM &BLUE TEAM

CAPACIDADES TECNICAS Y LEGALES DE GESTION PARA EQUIPOS BLUE TEAM & RED TEAM

JOAN MANUEL BUSTAMANTE CHAVERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICA, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN
2021

TABLA DE CONTENIDO

RESUMEN

Por medio de este documento se presenta un resumen de las etapas anteriores en el curso seminario especializado red team & blue team, en los cuales se plantearon diferentes situaciones en las cuales un especialista en seguridad de la información debe valerse de sus conocimientos, experiencia y manejo de herramientas para validar, identificar, comprender, y buscar soluciones que conduzcan a la corrección y mitigación de vulnerabilidades tanto a nivel de sistemas operativos como a nivel de aplicaciones, teniendo en cuenta la multiplicidad de amenazas que pueden presentarse en una organización buscando los puntos débiles para ser aprovechados como puede ser una fuga de información, accesos no autorizados, privilegios de administrador y creación de usuarios, lo que impacta directamente en los pilares de la seguridad de la información.

PALABRAS CLAVE: red team & blue team, fuga de información, Mitigación, Vulnerabilidad, Sistemas operativos, aplicaciones, amenazas, seguridad de la información.

ABSTRACT

Through this document, a summary of the previous stages in the specialized seminar course red team and blue team is presented, in which different situations were raised in which an information security specialist must use their knowledge, experience and management of tools to validate, identify, understand, and seek solutions that lead to the correction and mitigation of vulnerabilities both at the operating system level and at the application level, taking into account the multiplicity of threats that can arise in an organization by looking for weak points to be taken advantage of, such as information leakage, unauthorized access, administrator privileges and user creation, which directly impacts the pillars of information security.

KEY WORDS: red team & blue team, leak, mitigation, vulnerability, operating systems, applications, threats, information security.

GLOSARIO

VULNERABILIDAD: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

AMENAZA: toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

INFORMACION: Activo intangible en el cual se manejan identificaciones, datos personales, cuentas, datos empresariales y corporativos, propiedad intelectual, conocimiento comercial, formulación de productos o servicios.

DELITO INFORMATICO: Accionar que va en contras de las leyes establecidas y que mediante el manejo y conocimiento informático se aprovecha de las deficiencias en la seguridad de la información, para hacer uso abusivo a la información o bienes de terceros

ENTORNO DE PRUEBA: Laboratorio controlado en el cual se recrean las condiciones de una posible, falla de sistema, vulnerabilidad del sistema, o un ataque, con el fin de entenderlo, detallarlo, definirlo y proporcionar las herramientas para su mitigación

MAQUINA VIRTUAL: Entorno de virtualización mediante el uso de diferentes herramientas las cuales permiten a partir de un solo dispositivo físico contar con particiones virtuales en las cuales pueden convivir diferentes sistemas operativos, de este modo se pueden realizar pruebas de vulnerabilidad a aplicaciones y archivos.

EXPLOIT: Uso de la vulnerabilidad en una aplicación, sistema informático, archivo, la cual se aprovecha de manera no autorizada.

METASPLOIT: Metasploit Framework es una plataforma modular de pruebas de penetración basada en Ruby que le permite escribir, probar y ejecutar código de explotación. Metasploit Framework contiene un conjunto de herramientas que puede utilizar para probar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques y evadir la detección

METERPRETER: Meterpreter es un payload de Metasploit que proporciona un shell interactivo desde el cual un atacante puede explorar la máquina objetivo y ejecutar código.

REVERSE SHELL: Se conoce a la conexión que se inicia en un server y que termina en un usuario, en un caso normal es el usuario el que intenta conectarse al server, este tipo de ataque se utiliza para tomar control de un equipo cliente hasta obtener credenciales de administrador.

GPL: Licenciamiento de autor usado a nivel mundial para el software libre y código abierto.

INTRODUCCION

Para un especialista en seguridad informática es importante la identificación de los efectos y en especial de las causas frente a incidentes de seguridad empleando el análisis de las situaciones, la investigación y la creación de pruebas a partir de creación y montaje de laboratorios, además del empleo de las diferentes herramientas, entornos y posibilidades que puedan ser útiles para encontrar la solución o soluciones para corregir y mitigar las causas y efectos tanto de las vulnerabilidades como de las amenazas que buscan la pérdida de los pilares de la información y en muchos casos evitar un delito informático.

Actualmente se presentan múltiples fuentes de información confiable las cuales deben ser consultadas frecuentemente para estar actualizado frente a las nuevas vulnerabilidades y amenazas a las cuales se ven expuestos los diferentes sistemas informáticos, este tipo de fuentes por lo general brinda la manera de mitigar o corregir la vulnerabilidad eliminando una posible amenaza y permitiendo proteger y mantener los pilares de la información en una organización.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Desarrollar las actividades propuestas, alcanzando las competencias y destrezas requeridas identificando posibles vulnerabilidades y como se pueden fortalecer y corregir posibles fallos de seguridad identificados al interior de una organización.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar los aspectos legales de la seguridad de la información en Colombia
- Reconocer posibles actuaciones que incurran en delitos informáticos
- Hacer uso de entorno de prueba virtual y realizar uso de herramientas
- Identificar fallo de seguridad especifico que se presenta en entorno de prueba
- Documentar los pasos específicos para encontrar el fallo de seguridad en el entorno de prueba
- Investigar tipo vulnerabilidad y replicar ataque mediante uso de herramientas especializadas.
- Corregir posibles vulnerabilidades mediante hardening del sistema propuesto.
- Proponer herramientas de tipo GLP que permitan mejorar la seguridad de la información sin acarrear costos asociados a licenciamiento.

2. DESARROLLO DEL INFORME

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

- Clausula primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, **se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.**
  R/ Al ser la empresa Whitehouse Security una empresa multinacional con reconocimiento en el ámbito de la seguridad informática a grandes gobiernos es posible que maneje información clasificada, información sobre procesos ilegales que se puedan presentar en muchos ámbitos a nivel social, económico, jurídico, empresarial, político, clausula indica que la parte receptora, en este caso el prospecto al cargo se obliga a no divulgar la información no solo confidencial de Whitehouse Security, sino también cualquier tipo de procesos ilegales que se pueda presentar al interior de la información manejada o que se lleven a cabo por parte de Whitehouse Security, de forma física o remota a compañeros de trabajo, autoridades, o algún tipo de asesor.
  - Si es la empresa Whitehouse Security quien realiza procedimientos que van en contra de las leyes colombianas estipuladas al momento de los actos, esto incurre en un delito y falta de ética profesional, pues al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.
  - Si por el contrario la empresa Whitehouse Security dentro de sus hallazgos realizados mediante procedimientos legalmente establecidos, se informa sobre procesos ilegales, se debe revisar con el superior quien tendrá la facultad de velar por el resguardo de la información clasificándola según los parámetros de la empresa Whitehouse Security.

- Clausula segunda, Definición de información confidencial parágrafo 2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.
R/ En este parágrafo de la cláusula segunda se define la información considerada confidencial por parte de Whitehouse Security, la cual debe ser entendida y acatada por la parte receptora en caso de aceptar, y en la cual se realiza descripción de datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos.

- Es posible que dada la condición de la empresa Whitehouse Security al manejar grandes volúmenes de información de todo tipo, capte no solo la información legal, sino también la ilegal pero que es producto de la actividad misma de ciberseguridad y ciberdefensa.
- Por otro lado, si es desde la empresa Whitehouse Security que se realizan actividades de rastreo, interceptación de datos, y chuzadas que no sean consentidas por las leyes ni las autoridades colombianas.

Este tipo de actividades son reglamentadas y penalizadas por la ley de Colombia, además de ir en contravía de la ética profesional pues se debe buscar que la actividad profesional propende por el bien para todos y no es perjuicio para otros.

- Clausula cuarta, parágrafo 3. **No denunciar ante las autoridades actividades sospechosas de espionaje** o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
  R/ Esta cláusula indica que la parte receptora, se obliga a no divulgar la información de actividades sospechosas al interior de Whitehouse Security, sino también cualquier tipo de procesos ilegales que se pueda presentar al interior y que se lleven a cabo por parte de Whitehouse Security.
  Esto incurre en un delito ante la ley colombiana, además falta de ética profesional, pues al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.

- Clausula cuarta, parágrafo 4. **Abstenerse de denunciar y publicar la información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
  R/ Esta cláusula indica que la parte receptora, en este caso el prospecto al cargo se obliga a no divulgar la información no solo confidencial de Whitehouse Security, sino también cualquier tipo de procesos ilegales que se pueda presentar al interior y que se lleven

a cabo por parte de Whitehouse Security.
Esto incurre en un delito y falta de ética profesional, pues al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.

- Clausula cuarta, parágrafo 8. **Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento**.
  R/ En caso de aceptar la oferta, la parte receptora se obliga a responder por la información que tenga de Whitehouse Security y que se encuentre en su poder, en caso de que se realice una operación de allanamiento en contra de la parte receptora.

- Clausula cuarta, parágrafo 9. La parte receptora **se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal** sin el previo consentimiento por escrito por parte de Whitehouse Security.
  R/ Esta cláusula indica que la parte receptora, en este caso el prospecto al cargo se obliga a no divulgar la información no solo confidencial de Whitehouse Security, sino también cualquier tipo de procesos ilegales que se pueda presentar al interior y que se lleven a cabo por parte de Whitehouse Security, de forma física o remota a compañeros de trabajo, autoridades, o algún tipo de asesor.
  Esto incurre en un delito y falta de ética profesional, pues al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.

- Clausula quinta, parágrafo 8. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora: Octava. Solución de controversias: Las partes (nombre estudiante– nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo**. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.**
- R/ En caso de aceptar la oferta, la parte receptora se obliga a responder por la información que tenga de Whitehouse Security y que se encuentre en su poder, en caso de que se realice una operación de allanamiento en contra de la parte receptora.

- Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.
  R/Este punto es ambiguo porque en las cláusulas anteriormente mencionadas se habla de ilegalidad, procedimientos ilegales y ocultamiento de información a las autoridades, pero acá se indica que todo el acuerdo se regirá por las leyes de Colombia, esto puede ser con el fin de encubrir y aparentar falsamente la legalidad del documento, o por el contrario esto puede indicar que efectivamente el documento debe ser regido por la ley, con lo cual la parte receptora puede estar en libertad de denunciar en caso de evidenciar delitos informáticos.

2.2 Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.
R/ Si, se evidencia de que dentro del acuerdo y clausulas presentados por Whitehouse Security presentan evidencias de posibles delitos informáticos.

Ley 1273 de 2009
Por medio de la cual se realizan modificaciones en el Código Penal, creando un nuevo bien jurídico denominado como “de la protección de la información y de los datos” En el cual se deben preservan los sistemas que utilicen las tecnologías de la información y las comunicaciones de una manera integral.

Dentro de la ley N.º 1273 se tienen contemplados algunos de los delitos informáticos que se cometen y tipifica algunos de ellos.

1. Clausula primera y segunda, clausula cuarta, parágrafo 3. En el artículo 269A se enuncia el acceso abusivo a un sistema informático, se tiene en cuenta para todo lo que tiene que ver con accesos no autorizados, incluyendo lo que se denomina como “chuzada”, procedimiento en el cual se utilizan diferentes herramientas

2. En el artículo 269B indica que no se debe generar indisponibilidad o perdida de acceso sistemas informáticos, a información o bases de datos y a redes de telecomunicaciones.

3. En la Clausula segunda se viola el Artículo 269C el cual Habla de la no legalidad de interceptación de datos informáticos, en ningún punto ya sea origen o destino, además que contempla la no interceptación de ondas electromagnéticas.

4. El Articulo 269D indica que es ilegal cualquier tipo de daño a nivel de software y hardware, sea memoria o funcionamiento, para tener en cuenta ante ataques.

5. En el artículo 269E se indica el no uso de software malicioso o malware, pero no indica claramente cuáles son los tipos de Malware.

6. El Articulo 269F contempla la protección de datos personales contenidos en bases de datos, ficheros, los cuales no pueden ser sustraídos, vendidos, interceptados.

7. La suplantación de sitios Web con el fin de obtener datos personales este enunciado en el artículo 269G, atiende a personas que clonen paginas legales o realicen desvió de información para beneficio propio.

8. En los artículos 269 I y J se contempla el hurto por medios informáticos y la transferencia no consentida de activos.

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

R/ Como la empresa Whitehouse Security está buscando un especialista en seguridad informática, lo primero que solicita es la revisión del acuerdo entre las partes, por lo cual se logran evidenciar inicialmente unas posibles faltas a las leyes colombianas y ética profesional, como es un ejercicio de identificación, se le argumenta a la empresa Whitehouse Security los términos y cláusulas que pueden estar en contra de la legalidad, con base en esta información ellos pueden verificar y analizar teniendo en consideración la argumentación de un experto en seguridad informática, en caso de que el contrato sea revisado y ajustado aceptaría.

En caso de que el acuerdo revisado como prueba sea el acuerdo definitivo y no tenga ningún tipo de modificación, no aceptaría la posibilidad de un trabajo en el cual se puedan llevar a cabo actividades delictivas, criminales o que vayan en contra de la ley, no solo eso, también me considero un profesional integro que valora y respeta su conocimiento, como lo indica el código de ética el cual se apoya en la ley 842 de 2003:

“busca que los ingenieros, profesionales afines y auxiliares, actúen con compromiso y honestidad en aras de brindar a la ciudadanía un ejercicio ético de su profesión.

Además, desisto de un empleo en el cual pueda verme implicado en acciones ilícitas cometidas sin conocimiento, ya sea de mi parte o de compañeros de trabajo, ya que realizar actividades ilegales con el fin de cumplir las razones laborales no me exonera de la culpa.

En el Código emitido por el COPNIA el cual se indica como el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 31. Esta el parágrafo que indica “Son deberes generales de los profesionales los siguientes”:

> 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;

Si en caso de que estas acciones sean llevadas a cabo con pleno conocimiento, estaré incurriendo en un delito implicando no solo mi persona, sino la profesión y mi círculo familiar, social, académico, laboral.

De nuevo en el Código emitido por el COPNIA, Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 34. Esta el parágrafo indica, “Son 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 propia preparación.

En el caso de que un profesional incurra en participar de cualquier clase de delito en el desarrollo de sus funciones va en contra del código de ética, y en detrimento de su profesión, además en caso de un delito está obligado legalmente a revelar información.

En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, en su Capitulo II, DE LOS DEBERES Y OBLIGACIONES DE LOS PROFESIONALES. ARTÍCULO 39. Esta el parágrafo indica, “Son deberes de los profesionales para con sus clientes y el público en general:”:

a) Mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo;

Por último, se dejan en claro las faltas graves que un profesional de la ingeniería en este caso un especialista en seguridad informática debe evitar.

En el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares, se contemplan las faltas gravísimas contempladas en el artículo 53 de la ley 842 de 2003.

e) Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares;

f) Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que establecen el Código Ética y la presente ley.

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

R/ La operación militar que se mediatizo bajo el nombre de “Andromeda” y que dio cuenta de todo un escándalo por sus implicaciones sociales y políticas, fue un entramado creado por la inteligencia militar como una operación legitima, y que tenía como finalidad utilizar las habilidades informáticas de civiles en la búsqueda de información por medios abusivos.

Entendiendo como hackers personas civiles con conocimientos extensos en el uso de herramientas informáticas para la explotación de vulnerabilidades.

De esta manera se crea un lugar de acogida al parecer informal en el barrio Galerías en Bogotá y que tenía como nombre Buggly, donde confluían elementos atrayentes para los jóvenes como tatuajes, comida, paintball y claro salas con computadores y una mezcla de civiles y personal militar.

Entonces Andromeda Buggly fue una operación legitima y encubierta en la cual el ejercito mediante mentiras atraía a personal civil para que realizara actos ilegales, el tema se desbordo porque no se contaba con una ética clara para el actuar tanto de civiles como de militares.

El caso tuvo aún más revuelo por estar involucrado el llamado hacker Carlos Andrés Sepúlveda, quien al parecer compraba y obtenía información valiosa de Buggly, y que además servía a la campaña del entonces candidato presidencial por el centro democrático Oscar Iván Zuluaga, quien había contratado sus servicios, de una manera indirecta.

En toda la historia de la humanidad se ha dado gran relevancia a la información y al uso que de esta se puede hacer, ya sea para beneficio o en detrimento de personas, entidades, pueblos, pero hoy en día que la información es almacenada en medios electrónicos y viaja a través de redes de computadores es de suma importancia no solo conocer su acertado manejo sino también su resguardo, porque habrá personas inescrupulosas que harán lo que sea para obtenerla.

En el caso del ejercito es un actuar fuera de la ética, el usar a civiles mientras bien pudieran emplear los mismos fondos de operaciones de engaño a capacitar a funcionarios militares, es aún más falto de ética atraer y engañar con el fin de obtener datos e información de manera claramente abusiva, poniendo en evidencia a civiles que estaban cometiendo delitos informáticos como son la interceptación y robo de datos, crímenes que ya estaban legislados en su momento bajo la ley 1273 de 2009.

A nivel legal “Andromeda” al no tener control dejo que conocedores de la información se hiciesen con ella al mejor precio, personas que obviamente sabían qué hacer con la información que se obtenía en la operación y que pudiese ser destinada a cualquier clase de ilícito, incluso a ganar unas elecciones o sabotear al candidato opositor.

Al manejar la seguridad nacional y la seguridad de la información pública se debe contar con altos estándares en la ética profesional ya que pueden presentarse oportunidades de usufructuar la información que se maneja, así mismo se debe de tener conocimiento del marco legal en Colombia que define, reglamenta y penaliza los delitos informáticos para no pecar por omisión, y cometer un crimen por ignorancia o falta de conocimiento.

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

- **Fase de recolección de información**

Se recibe el requerimiento en el cual se indica lo sucedido, se procede al análisis de la información suministrada:

se tiene la evidencia sobre una de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia.

La información inicial con la que se cuenta es que el equipo donde se está generando la fuga de información tiene instalada una aplicación llamada Rejetto v. 2.3 bajo un windows 7 con arquitectura X64.

Se debe tener en cuenta que el sistema operativo Windows 7, ya no cuenta con actualizaciones de seguridad las cuales dejaron de ser emitidas por Microsoft desde enero de 2020, al considerar que este sistema operativo había cumplido con su vida útil, y para de alguna manera forzar y dar paso a Windows 10.

El empleo de este sistema operativo es cada vez mas riesgoso, pues aumentan los casos de nuevas vulnerabilidades encontradas, las cuales son aprovechadas para minar los pilares de la información, teniendo en cuenta que aun muchos usuarios y empresas no han realizado la actualización de sus sistemas operativos.

- **Fase de Búsqueda de vulnerabilidades.**

Dentro de la información entregada se tiene una aplicación, Se investiga sobre aplicación Rejetto v. 2.3 la cual es una HTTP file server, un servidor web para compartir archivos, es decir es una aplicación libre de malware y pensada para ser útil, pero tiene una vulnerabilidad.

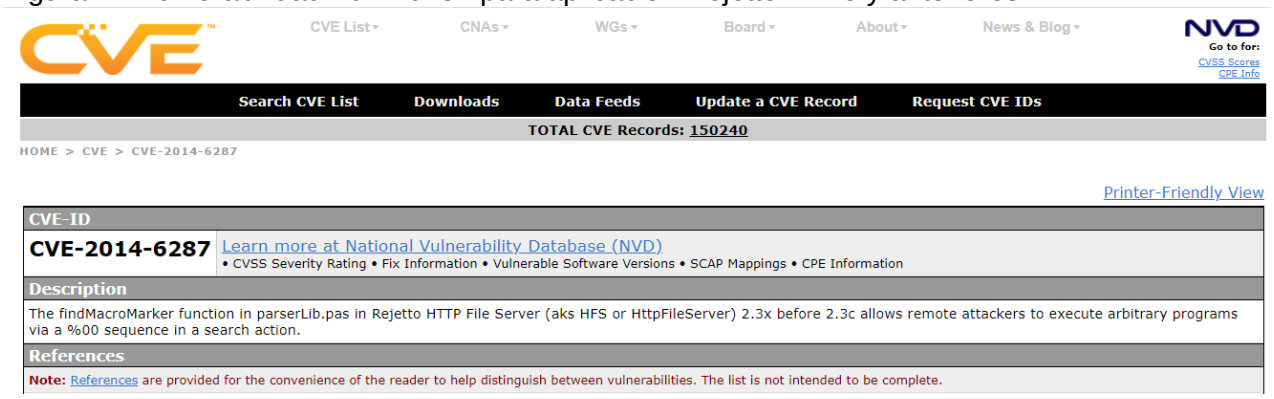
Se realiza revisión de casos similares e investigación en bases de datos de vulnerabilidades donde se encuentran dos vulnerabilidades para esta aplicación

Dentro de las paginas encontradas de fuente confiable se evidencian alertas sobre la vulnerabilidad presente en la aplicación Rejetto v. 2.3 y anteriores:

Figura 1 - Vulnerabilidad 2014-6287 para aplicación Rejetto v. 2.3 y anteriores

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

Figura 2 - Vulnerabilidad 2014-6287 para aplicación Rejetto v. 2.3 y anteriores

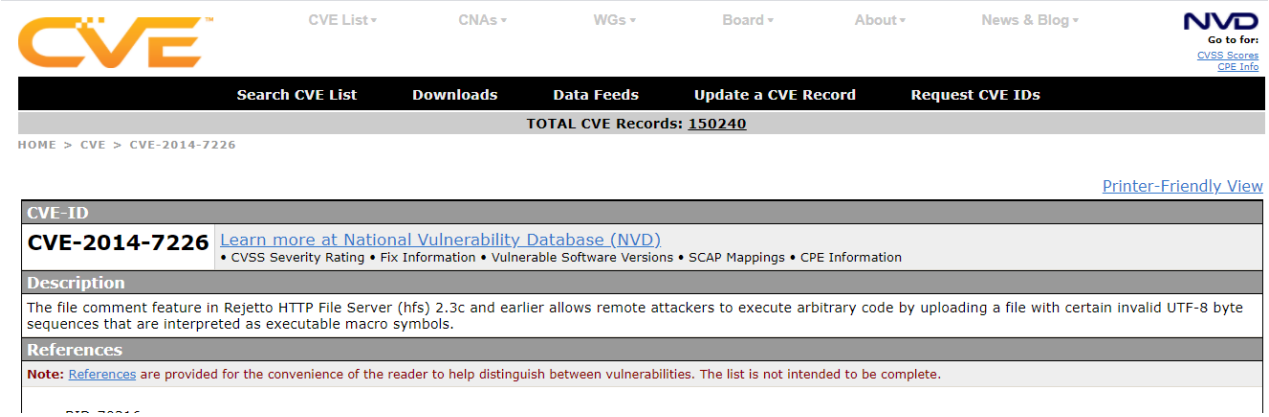


Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

La función findMacroMarker en parserLib.pas en Rejetto 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.
esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de Meterpreter.

Además, la aplicación Rejetto v. 2.3 y anteriores presenta dos vulnerabilidades más documentadas:

Figura 3 - Vulnerabilidad 2014-7226 para aplicación Rejetto v. 2.3 y anteriores



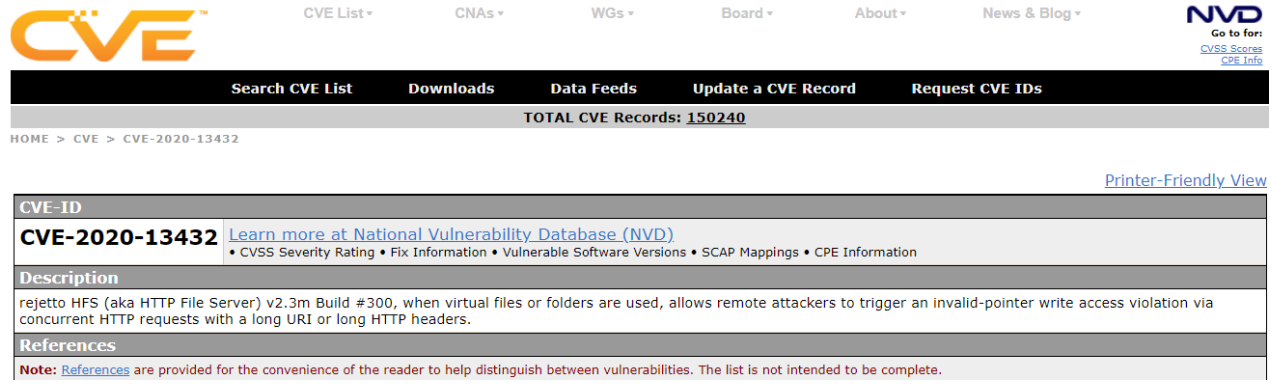
Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7226

La función de comentario de archivo en Rejetto HTTP File Server (hfs) 2.3cy versiones anteriores permite a los atacantes remotos ejecutar código arbitrario cargando un archivo con ciertas secuencias de bytes UTF-8 no válidas que se interpretan como macro símbolos ejecutables.

Por último, aparece una vulnerabilidad documentada para aplicación Rejetto v. 2.3 y anteriores:

Figura 4 - Vulnerabilidad 2020-13432 para aplicación Rejetto v. 2.3 y anteriores

CVE-2020-13432



Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13432

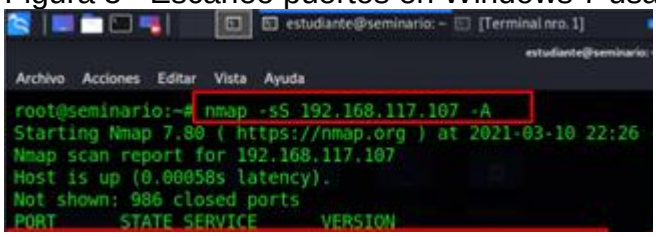
Rejetto v. 2.3 y anteriores, cuando se utilizan archivos o carpetas virtuales, permite a los atacantes remotos desencadenar una infracción de acceso de escritura de puntero no válido a través de solicitudes HTTP simultáneas con un URI largo o encabezados HTTP largos

- **Fase de Explotación de vulnerabilidades**

Se implementa un laboratorio de pruebas en el cual se recrea el escenario mediante una máquina virtual en la cual convive un sistema operativo un Windows 7 con arquitectura X64 (victima) que cuenta con la aplicación Rejetto v. 2.3 y un Kali Linux (atacante), ambos sistemas operativos se implementan en un mismo segmento de red, de esta manera se busca no solo identificar la vulnerabilidad sino también el entender como opera este fallo de seguridad, simulando el ataque.

Al analizar el sistema operativo Windows 7, usando la herramienta Nmap se encuentran puertos abiertos que generan una vulnerabilidad y pueden ser aprovechados para intentar el acceso no autorizado usando la IP de Windows 192.168.117.107:

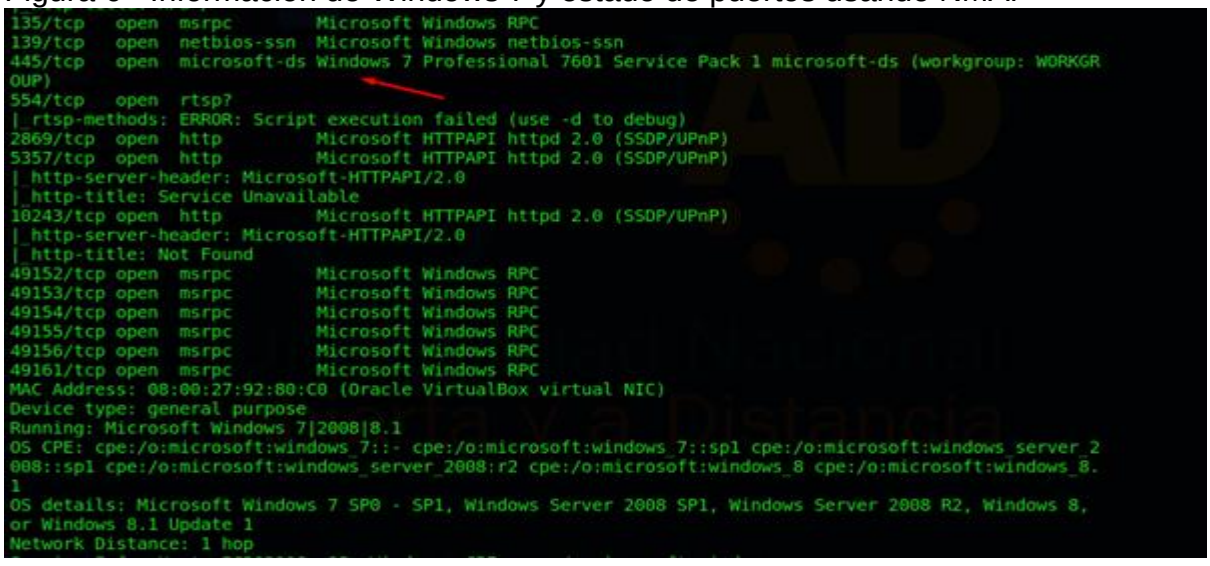
Figura 5 - Escaneo puertos en Windows 7 usando Nmap



Fuente propia

Este comando entrega la información del sistema operativo y sus puertos abiertos

Figura 6 - Información de Windows 7 y estado de puertos usando NMAP



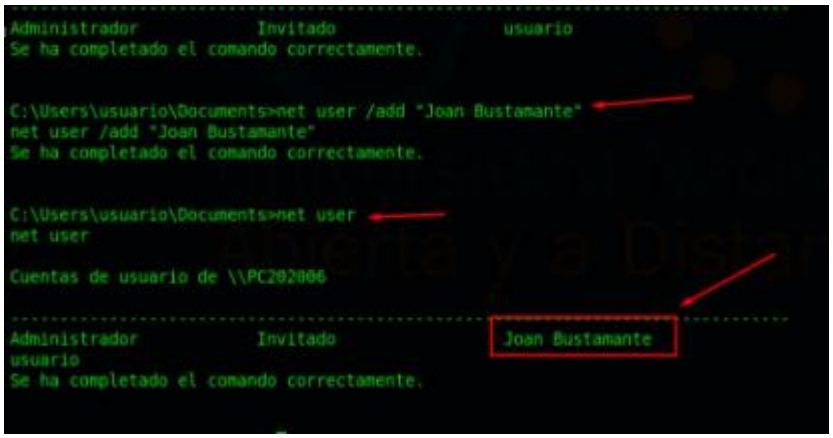
Fuente propia

- **Fase Post-explotación**

En esta fase luego de dejar en evidencia la posible forma y manera de que se realiza el ataque y se valida la fuga de información, se procede a realizar pruebas de que tanto alcance puede tener este tipo de ingreso abusivo, se intenta el acceso a archivos de información privilegiada, alcanzar usuarios y contraseñas auténticos, obtener privilegios como administrador, creación de usuario legítimo, copiado, alteración, borrado de información.

Se logra tener acceso al sistema atacado como administrador, esto permite obtener toda la información que está en el dispositivo.

Figura 7 - Acceso como administrador Windows 7



Fuente propia

- **Fase de Informe.**

Después del análisis de la información inicial, de la investigación requerida de las posibles vulnerabilidades y de la prueba de laboratorio en un entorno en el cual se replicó el escenario real, el hallazgo es claro en asegurar que no se estaban cumpliendo las políticas y controles que definen la seguridad de la información en que se tenía instalada una aplicación con múltiples vulnerabilidades y fallos de seguridad la cual al parecer no había sido revisada y testeada por el personal encargado de la seguridad de la información, en un sistema operativo no actualizado con vulnerabilidades y múltiples fallos de seguridad el cual no contaba con ningún otro tipo de seguridad sino la que brinda el mismo sistema operativo, el cual no cuenta ya con la actualización entregada por el proveedor, en este caso Microsoft.

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

Primero ya se tiene una evidencia y es sobre una de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia.

La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada Rejetto v. 2.3 bajo un Windows 7 con arquitectura X64.

Se investiga sobre aplicación Rejetto v. 2.3 la cual es una HTTP file server, un servidor web para compartir archivos, es decir es una aplicación libre de malware y pensada para ser útil, pero tiene una vulnerabilidad.

esta aplicación presenta múltiples vulnerabilidades, las cuales se pueden asociar a diferentes exploits los cuales pueden terminar entre otros en una Shell reversa y una sesión abierta de Meterpreter.

En un escenario típico de acceso al sistema remoto, el usuario es el cliente y la máquina de destino es el servidor. El usuario inicia una conexión de Shell remota y el sistema de destino escucha dichas conexiones.
Existe la posibilidad de invertir este proceso donde es la máquina de destino la que inicia la conexión con el usuario, y la computadora del usuario escucha las conexiones entrantes en un puerto específico.

La razón principal por la que los atacantes suelen utilizar Shells inversos es la forma en que se configuran la mayoría de los firewalls. Los servidores atacados generalmente permiten conexiones solo en puertos específicos. Por ejemplo, un servidor web dedicado solo aceptará conexiones en los puertos 80 y 443. Esto significa que no hay posibilidad de establecer un escucha de Shell en el servidor atacado.
Tener los puertos abiertos o en modo escucha es una mala práctica ya que los sistemas operativos y aplicaciones como correo, almacenamiento de información, navegadores, bases de datos, almacenamiento de contraseñas y usuarios quedan completamente expuestos a rastreo o escaneo de puertos por medio de herramientas como Metasploit, Nessus, Nmap.

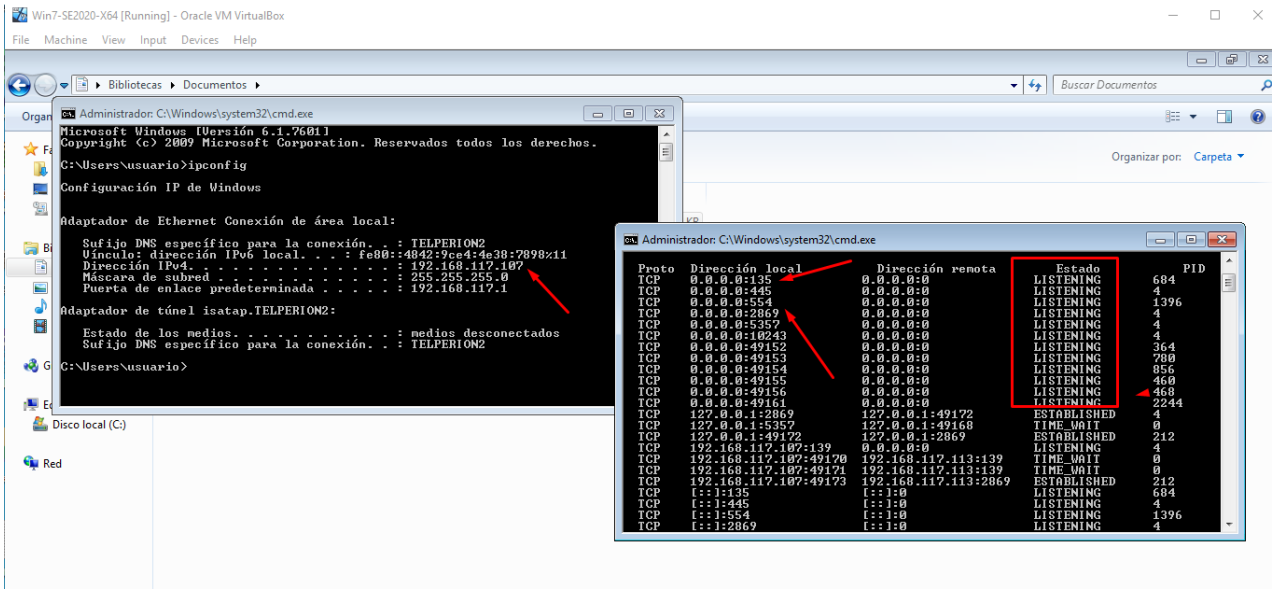
La mala gestión en las políticas y controles de los puertos genera una gran cantidad de vulnerabilidades y posibles amenazas a la seguridad de la información.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

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

La máquina con sistema operativo Windows 7, tiene servicios ejecutándose como servicio y el cual acepta conexiones entrantes, dado que se detecta que su firewall no las bloquea.

Figura 8 - Resultado comando ipconfig - Windows 7

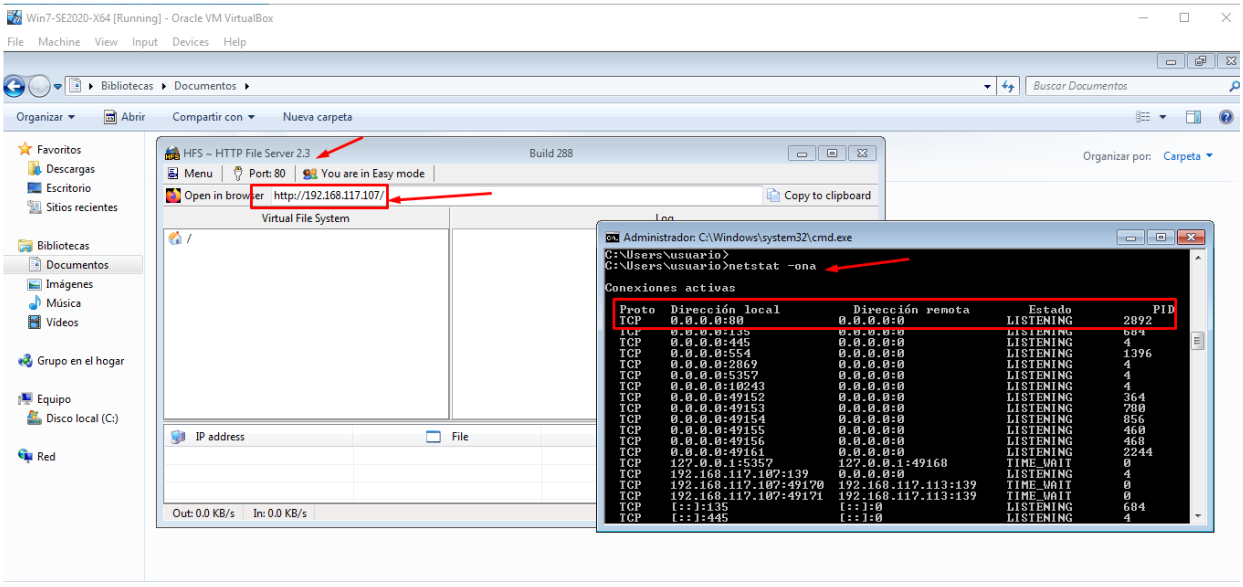


Fuente propia

Con la herramienta **ipconfig**, se observa que tiene configurada la ip: 192.168.117.107, con la herramienta de comandos **netstat** se observa los puertos que tiene abiertos y que están en estado LISTENING como se observa en la imagen de la derecha (**cmd**)

El aplicativo que se ejecuta en el host (servidor expuesto), corre una aplicación que tiene una vulnerabilidad conocida, al activarla se abre un nuevo puerto en el equipo, el cual es detectado con la herramienta **netstat** (en este caso la aplicación abre el puerto 80, como se observa en la siguiente imagen:

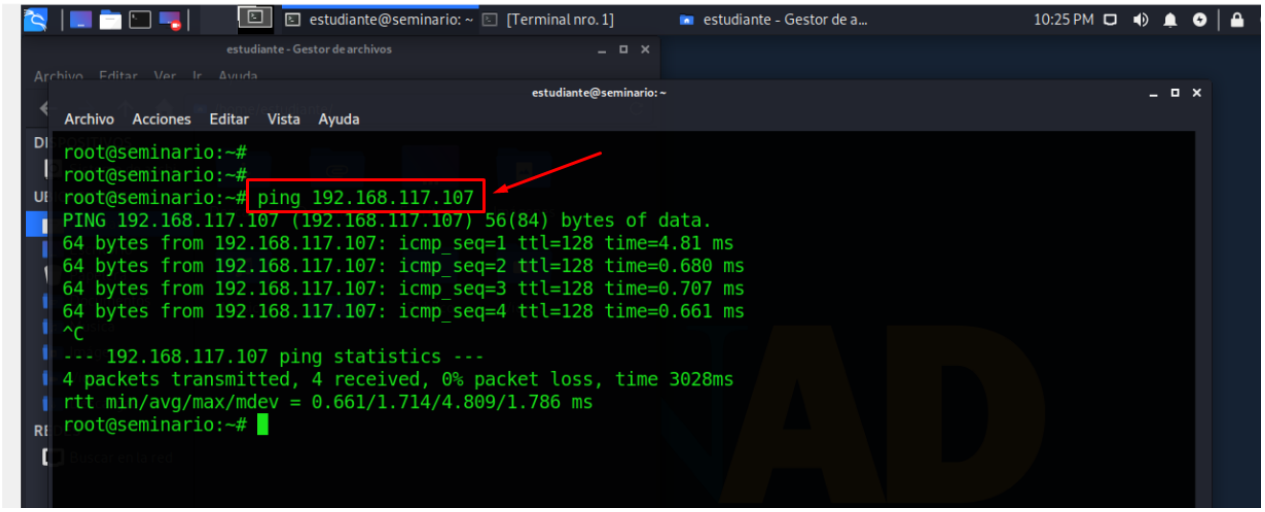
Figura 9 - Puerto 80 en modo listening - Rejetto v. 2.3



Fuente propia

En este caso un atacante usando un sistema operativo de pentesting (Kali) que puede alcanzar dicha maquina dado que están en red, como lo muestra la siguiente imagen:

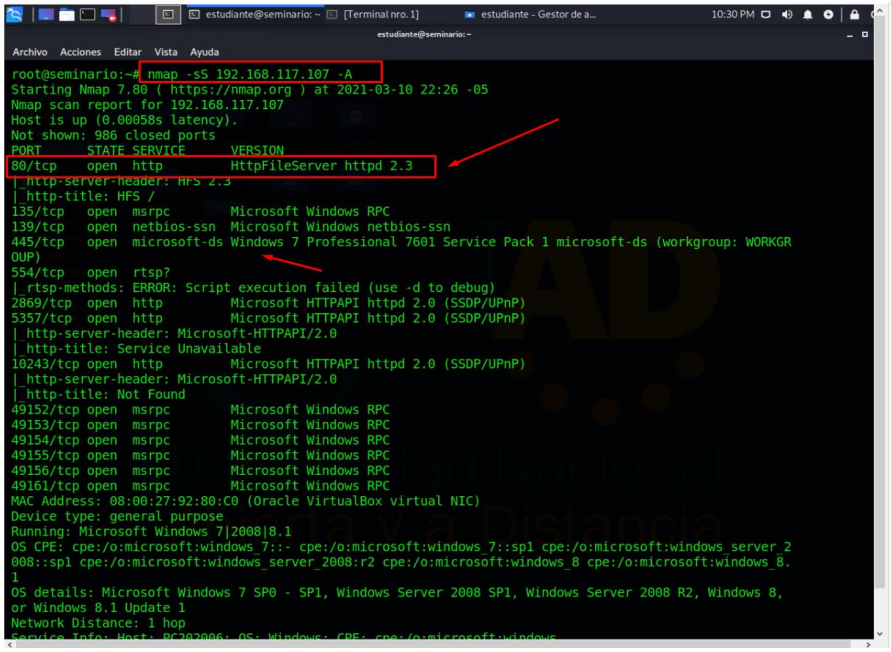
Figura 10 - Comando ping a IP servidor



Fuente propia

Con la herramienta Nmap, un atacante puede detectar los puertos abiertos que tiene el equipo y el servicio que los tiene corriendo (ejecutando en background)

Figura 11 - Uso de Nmap - Puerto 80 open - Rejetto v. 2.3



Fuente propia

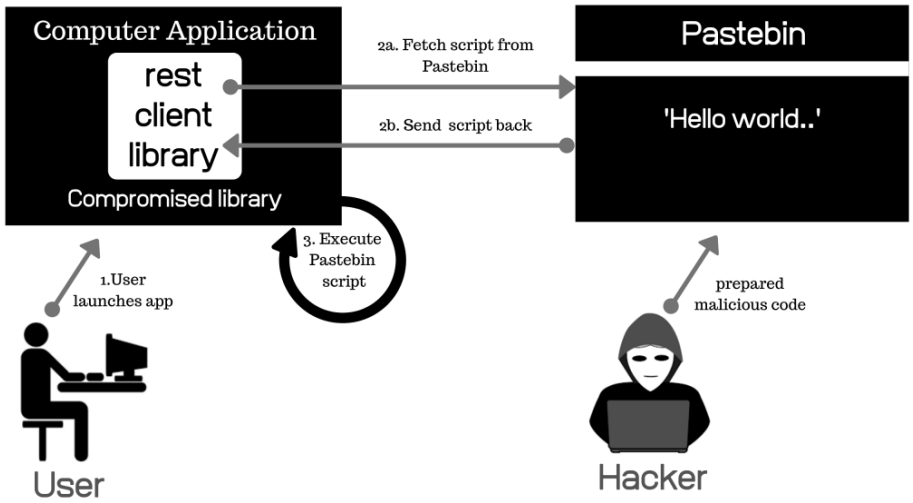
Se observa como un atacante detecta los servicios ejecutándose en el host remoto y la versión del software que se ejecuta.

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

Un atacante puede entonces saber de acuerdo con la versión de software que se corre en el host remoto, saber que vulnerabilidades conocidas tiene la aplicación, y si no se han parchado se corre el riesgo de que sean explotadas. Como se hará en este PoC, se aprovecha el bug conocido que permite a un atacante remoto ejecutar código arbitrario en el servidor (host) que hospeda la aplicación. En este caso el equipo con dirección IP: 192.168.117.107

La función de comentario de archivo en Rejetto HTTP File Server (hfs) 2.3cy versiones anteriores permite a los atacantes remotos ejecutar código arbitrario cargando un archivo con ciertas secuencias de bytes UTF-8 no válidas que se interpretan como macro símbolos ejecutables, como se explica gráficamente en la siguiente Imagen:

Figura 12 – Explicación de ataque



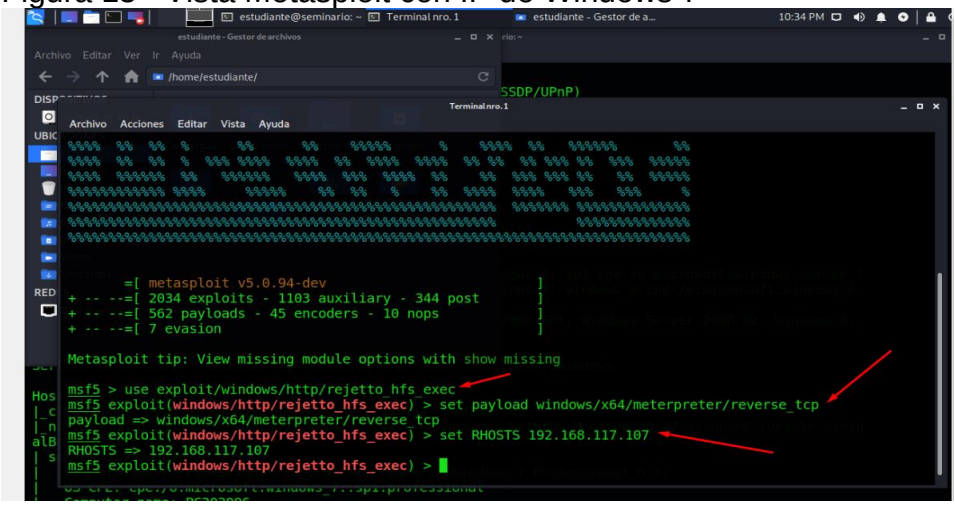
Fuente: https://blog.meterian.com/2019/08/27/vulnerability-focus-remote-code-execution-rce-attacks/

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

Dado que ya se conoce entonces que el servidor tiene una aplicación vulnerable y escuchando en el puerto 80, se pretende entonces demostrar cómo se puede ganar acceso a una Shell (cmd), de forma remota para poder controlar el servidor.

- La siguiente imagen muestra el inicio de Metasploit (el framework para realizar en este caso el ataque)

Figura 13 - Vista Metasploit con IP de Windows 7

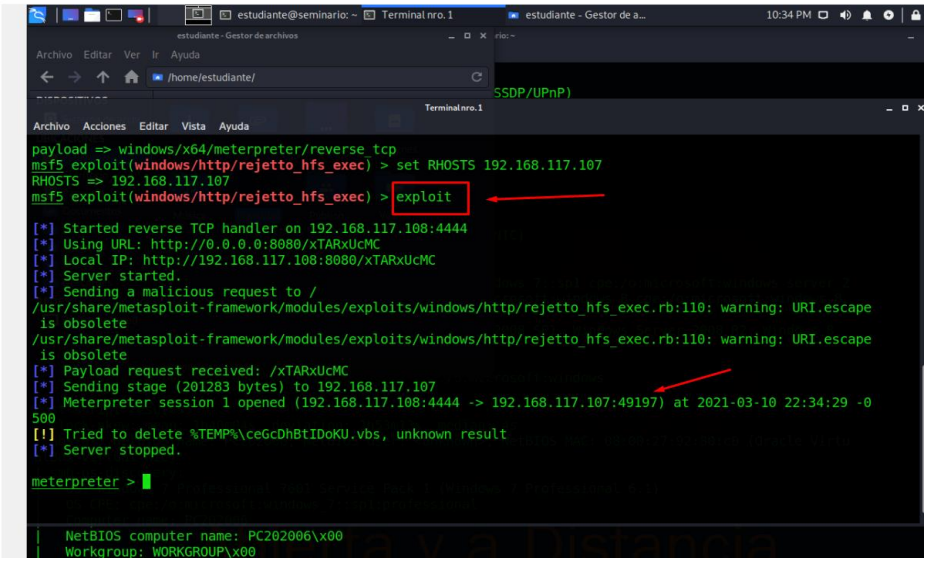


Fuente propia

1. Luego se ingresa a la base de datos que contiene los exploits de las vulnerabilidades ya conocidas
2. Se carga un payload para que una vez explotada la vulnerabilidad el equipo servidor haga una conexión reversa al equipo del atacante, en este caso el SO Kali Linux
3. Se especifica el target (RHOST), que será el host remoto, en este caso el servidor que se ataca.

Una vez se definen los parámetros, se explota la vulnerabilidad:

Figura 14 - Vista Metasploit con sesión Meterpreter

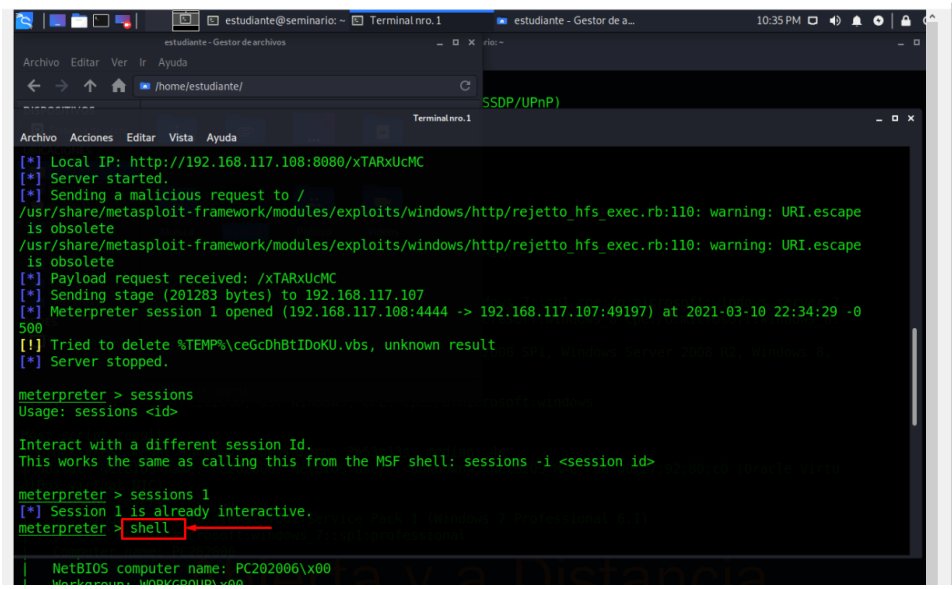


Fuente propia

Como se observa en la imagen anterior, el equipo Kali Linux establece una sesión con la víctima en este caso el servidor 192.168.117.107

En la siguiente imagen se muestra como la vulnerabilidad permite ejecutar código en el servidor, dado esto, se puede obtener acceso a la Shell de Windows, en este caso el programa (cmd.exe) que permite ejecutar código como si se estuviera localmente en el servidor:

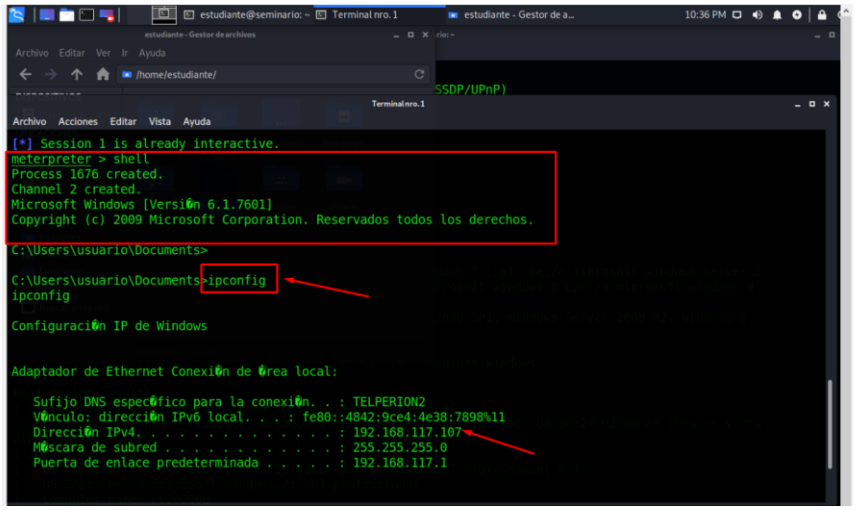
Figura 15 - Shell abierto en Windows 7



Fuente propia

Ya con acceso al equipo atacado, se recolecta información que permita verificar que efectivamente estamos al interior del equipo deseado, se utiliza comando ipconfig:

Figura 16 - Sesión en Windows 7 – ataque exitoso – revisión IP

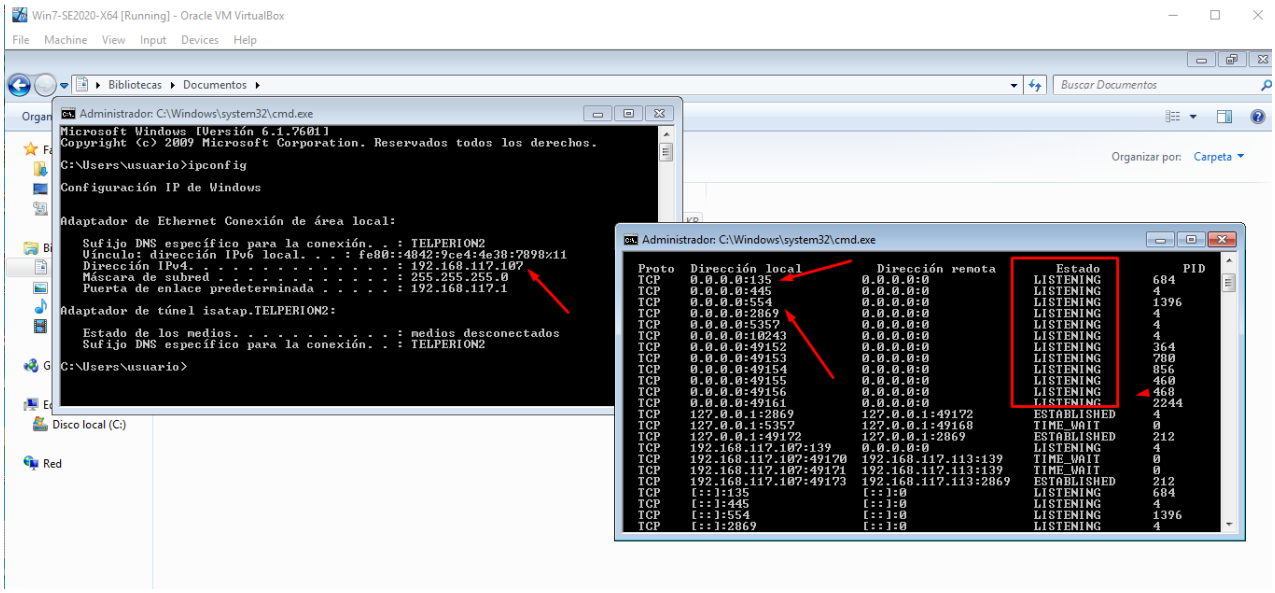


Fuente propia

Como se evidencio en la imagen anterior, el atacante obtiene acceso a la Shell de Windows y en este caso se ejecuta el comando **ipconfig** que muestra la dirección ip del servidor (host remoto), lo que indica que el equipo ahora está bajo control del atacante.

Para confirmar la IP del equipo atacado, se ingresa y se recolecta la información de direccionamiento, con el comando **ipconfig** pero esta vez desde Windows 7

Figura 17 - Resultado comando **ipconfig** desde Windows 7



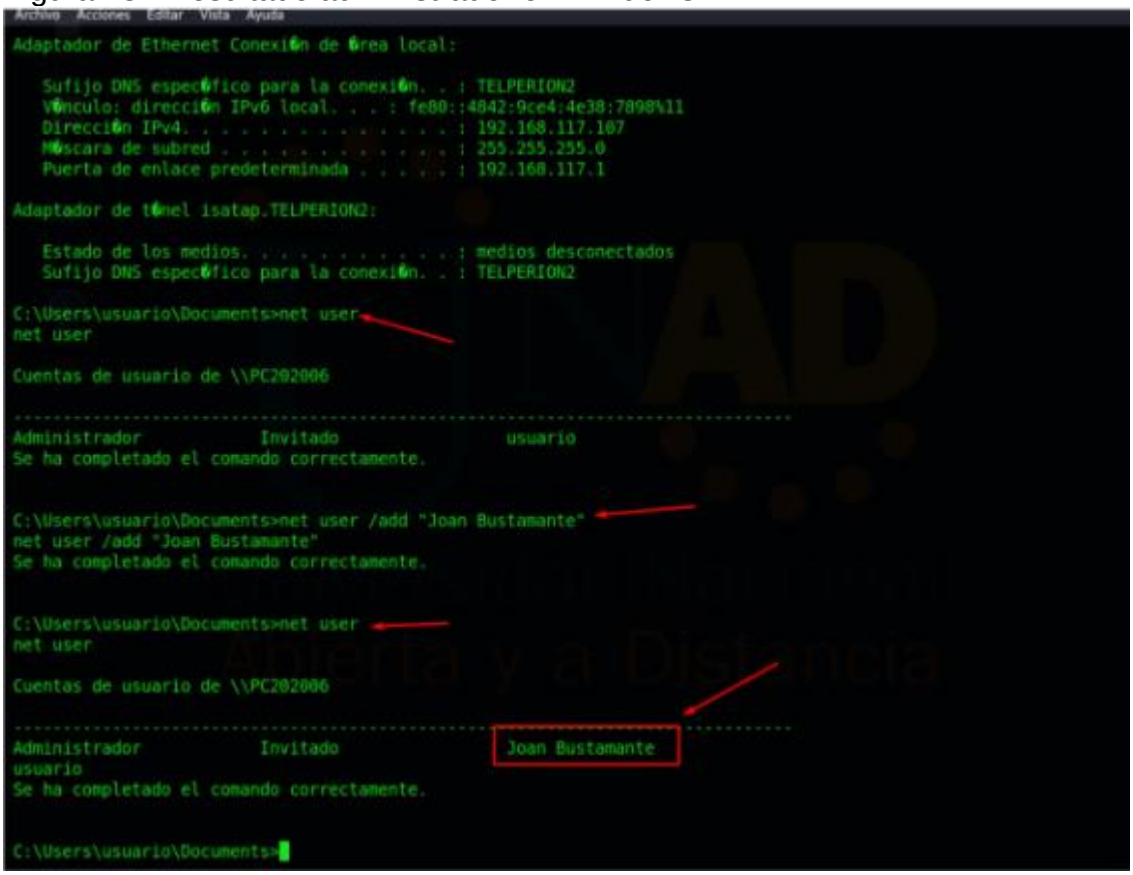
Fuente propia

Se evidencia entonces como por medio de la vulnerabilidad presente en una aplicación instalada en un sistema operativo se puede tener un fallo en la seguridad y una fuga en la información, en este caso se evidencia que gracias a Rejetto v. 2.3, se deja abierto el puerto 80 por el cual se puede realizar un ataque exitoso.

Se valida la falla de seguridad y se explota con el fin de crear un usuario con el primer nombre del estudiante: **Joan** y primer apellido: **Bustamante**, creando un usuario como administrador para demostrar una PoC ante los altos directivos.

Se demuestra a los altos directivos como por medio de una vulnerabilidad en una aplicación, además instalada en un sistema operativo que ya no recibe parches de seguridad pone en peligro los pilares de la seguridad de la información mediante un ataque en el cual un tercero logra un acceso como administrador en el sistema.

Figura 18 - Resultado administrador en Windows 7



Fuente propia

2.10 Situación problema: Análisis Blue team

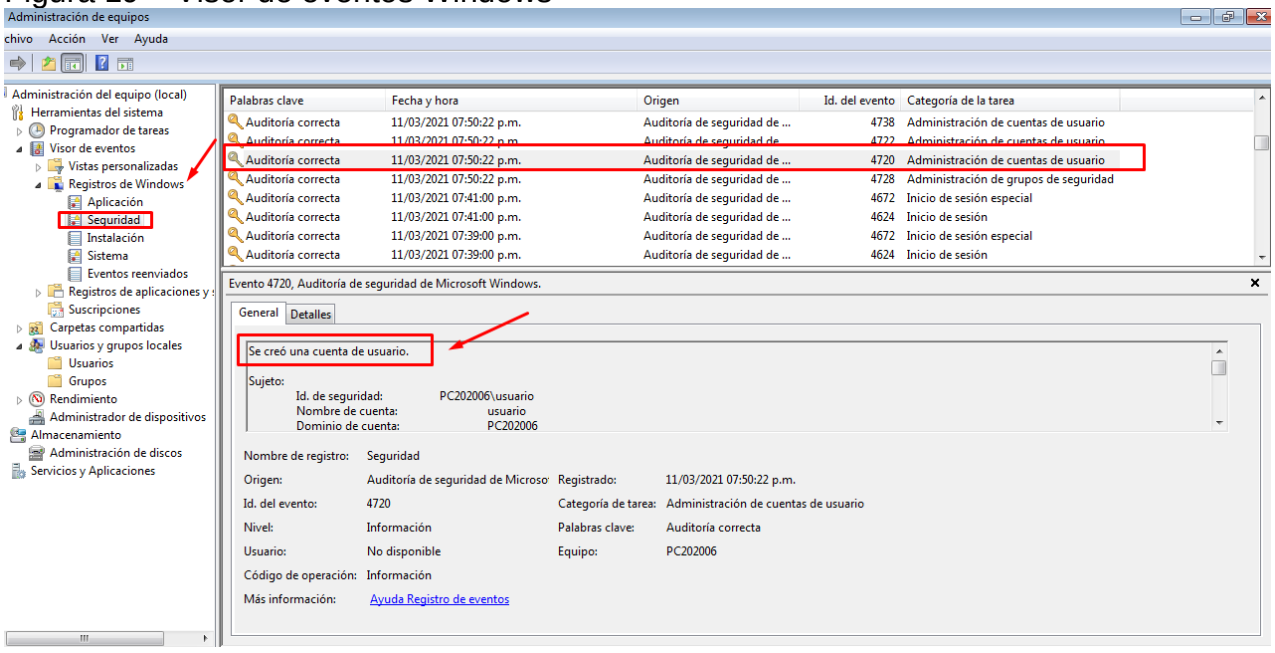
WhiteHouse Security solicita a sus integrantes de Blue team contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

El equipo de Blue Team debe analizar entonces varios aspectos antes de aislar el equipo blanco de ataques, en este caso Windows 7x64, dado que está corriendo un servicio que probablemente es un recurso importante dentro de la organización y que se debe mantener estable, con disponibilidad para los usuarios.

- **Detección del ataque:**

El sistema operativo afectado, en este caso cuenta con herramientas nativas y que dan información sobre acciones realizadas:

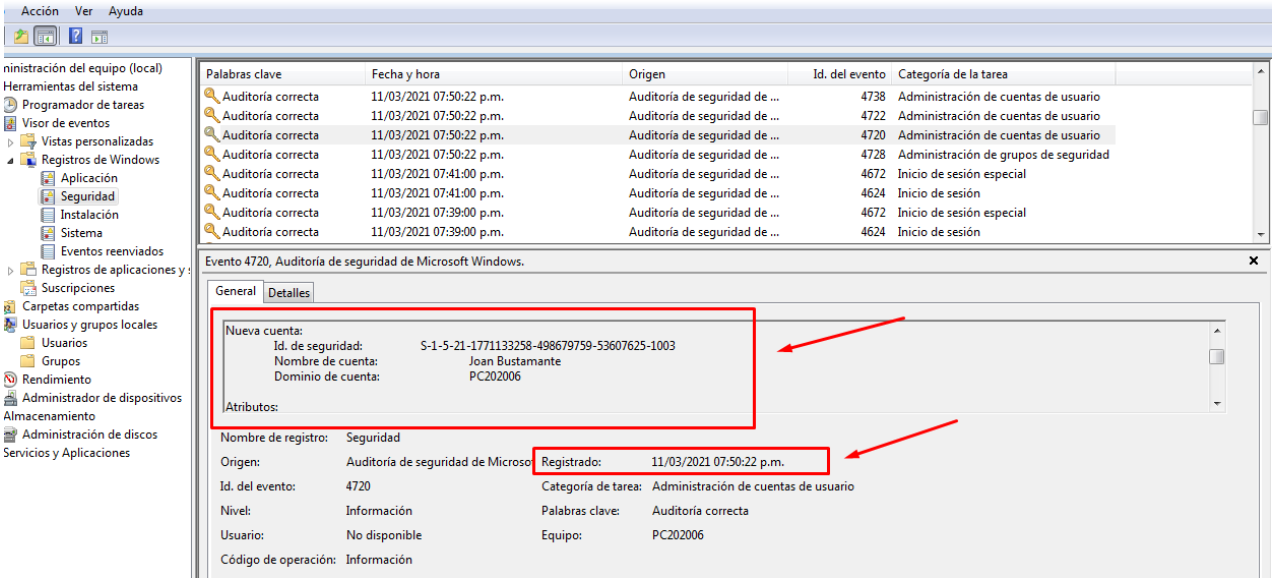
Figura 19 – Visor de eventos Windows



Fuente: Propia

Como se observa en la imagen anterior, se puede ver en el visor de eventos (herramienta nativa del sistema afectado) que ha sido creada una cuenta. La sección de seguridad indica la creación de cuenta de usuario, en los detalles, efectivamente se puede observar los valores:

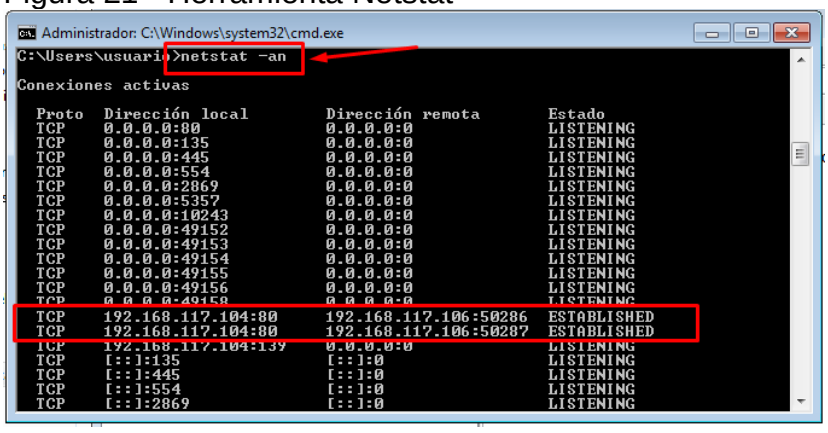
Figura 20 – Información creación cuenta - Visor de eventos Windows



Fuente: Propia

La fecha de realización de la actividad. (Si este evento esta correlacionado con un sistema que alerta cuando se ejecuta este tipo de acciones, entonces la detección se hace en tiempo real, de lo contrario este sujeto a la revisión manual que se haga de los eventos de la seguridad.)
Siguiendo con la detección de una intrusión, sabemos que una cuenta local con privilegios fue creada y que posiblemente y dado que no fue realizado por alguien del equipo de seguridad o de sistemas TI, se sabe entonces que el sistema ha sido comprometido, podemos usar la herramienta ***(netstat)*** para ver que conexiones establecidas están en el equipo:

Figura 21 - Herramienta Netstat



Fuente: propia

Como se observa en la imagen anterior, el puerto por el que hay una sesión establecida es el 80, sabríamos entonces la dirección IP remota que tiene establecida la sesión, esta IP puede ser reconocida o finalmente ser una dirección que aumente el nivel de sospecha que se tiene sobre la relación con el ataque.

Factores que ayudan a identificar porque fue atacado el sistema

- El uso de un sistema operativo que no está parchado, es decir no cuenta con las debidas actualizaciones y que adicional no es la última versión desarrollada, da indicaciones de que inevitablemente se pueden recibir ataques y que el nivel de riesgo de la exposición es alto.

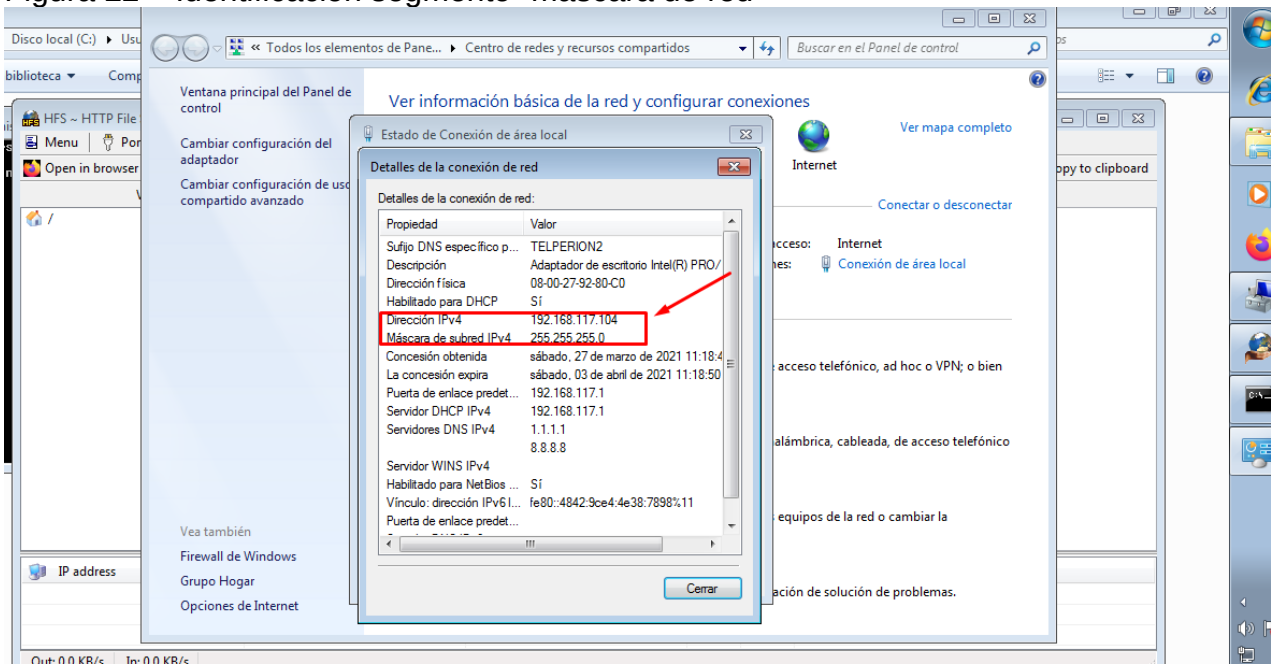
- Ejecutar software que abre puertos en el sistema y que presenta vulnerabilidades se suma al indicador de nivel de riesgo al que ya está expuesto el sistema. En este caso la versión del aplicativo tiene CVN conocidos y con exploits desarrollados.

- Servicios como Firewall de Windows deshabilitado, Windows Defender, entre otros.

Contención

Debido a que el atacante ya hizo una intrusión en el sistema, posiblemente ya ha hecho un levantamiento de información y sabe que otros blancos existen dentro de la red, por lo que es imperante aislar el equipo afectado.

Figura 22 – Identificación segmento -mascara de red



Fuente: Propia

Como se observa la dirección IP del servidor tiene una máscara /24, lo que indica que posiblemente un escaneo de red realizado por el atacante detecte otro host dentro de la red y que también estos presenten vulnerabilidades (si tienen la aplicación Rejetto Instalada en sistemas operativos no actualizados), por lo que es importante aislar el sistema afectado para que no sirva como punto de ataque para otros equipos dentro de la red.

Las acciones de contención que se pueden realizar una vez identificado el ataque y el blanco afectado son:

- Bloqueo de la dirección IP del atacante, detectada con el comando Netstat
- Habilitar firewall de Windows y permitir solo equipos de la red interna (Si el atacante está en la red LAN, esta acción puede no ser efectiva)
- Cerrar puertos TCP no necesarios
- Actualización del software que ejecuta el servicio (parcheo)
- Ejecutar el servicio con privilegios de usuario no de administrador
- Instalación de parche de sistema operativo Windows

Si no es posible realizar alguna de las acciones anteriores, se debe entonces recurrir al método físico de aislar el sistema, es decir desconexión física de cableado de red, para ejecutar herramientas como antivirus, desinstalación de rootkits, backdoors etc.

2.11 Análisis con acciones necesarias para contener un ataque en tiempo real.

Se deben tener en cuenta**:**

Monitoreo: Se deben tener elementos ya sea hardware o software que generen el monitoreo de la red y que permitan la detección del incidente, es decir que exista una continua revisión de diferentes parámetros que indiquen si la red opera con normalidad, o si por el contrario está en una situación fuera de lo común.

Alerta: Además del monitoreo, se debe contar con alarmas o alertas en las que se le informe al personal encargado de la seguridad informática sobre posibles anormalidades en la red o ataques que se estén llevando a cabo sobre la infraestructura.

Identificación: Esta se debe definir ya sea por medio de filtros y políticas en equipos de seguridad o y sea por el personal encargado de la seguridad informática, se debe contar con procedimientos claros para identificar y definir un ataque según los hallazgos entregados por el monitoreo y alerta, además de análisis de los logs de los diferentes equipos y según la afectación que se presente.

Contención: luego de las etapas anteriores de monitoreo, alerta e identificación, la etapa de contención contempla las acciones que permitirán mitigar o controlar el ataque**,** esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la seguridad de la información.
El NIST (National Institute of Standards and Technology) cuenta con el marco de seguridad Cybersecurity Framework CSF (V1.1, 2018)

Dentro del CFS se tiene un enfoque conocido como Framework Core el cual consta de cinco funciones simultaneas y continuas:

- Identificar (Identify): Determina los sistemas, activos, datos y competencias de la organización en su contexto, negocio, recursos y demás elementos que soportan las funciones críticas, así como los riesgos de ciberseguridad que pueden llegar a generar una afectación.
- Proteger (Protect): Permite el desarrollo e implementaciones como contramedidas y salvaguardas, las cuales son necesarias con el fin de mitigar o contener la afectación de un posible evento de ciberseguridad.
- Detectar (Detect): Busca desarrollar e implementar los métodos y estrategias adecuadas mediante monitoreo continuo para realizar detecciones de ocurrencia de un evento de ciberseguridad.
- Responder (Respond): Al contar con un correcto diagnóstico de un evento de ciberseguridad se debe contar con acciones y actividades de contención y reacción para mitigar su posible impacto o afectación.
- Recuperar (Recover): Vuelta a la normalidad luego de presentarse un evento o incidente de ciberseguridad, incluyendo las acciones que den lugar a restablecimiento de los servicios.

2.12 Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.

- Actualización de sistemas operativos
- Parcheo de vulnerabilidades
- Desactivar la opción de acceso remoto
- Ejecución de servicios con privilegios de usuario no-administrador
- Software antivirus
- Software antiransomware
- Manejo de herramientas de seguridad perimetral como Firewall activado con solo puertos de servicio OPEN y en CLOSE puertos que no están dando servicio a la red.
- Manejar uso de información encriptada, seguridad usuarios, datos, carpetas
- Cliente EDR (para la automatización de acciones o respuesta a incidentes)
- Manejo de herramienta que alerten sobre actividades sospechas IDS-IPS
- Sistemas integrados de IoC (Indicator of Compromise) para monitoreo de eventos.

El hardening se puede hacer en varias capas, empezando desde el perímetro hasta llegar al equipo servidor:

Perímetro
Integración de soluciones que aseguran la protección de servicios en este caso de aplicaciones web (como es el caso de WAF – *Web Application Firewall*) esta herramienta permite protección de ataques XSS, SQL-Injection, Exploit DB, entre otros.
Políticas de firewall *(next generation firewall)* de borde en el que se controla el acceso por direcciones IP fuente, acceso por país, reputación de IP, entre otros.
Puertos abiertos por aplicaciones que solo se usan en el servidor.

Zona DMZ
Integrar el servidor o equipos con nivel de riesgo expuesto a una zona DMZ, en el cual, si alguno de ellos se ve comprometido, por políticas de control de acceso o firewall, no pueden ser punto de ataque a otros servicios de red o host.

Endpoint
Es el punto final o destino de las conexiones, en este caso si es el servidor que ejecuta el aplicativo de servicios debe contar con las siguientes medidas de protección (Adicional a las mencionadas en el punto anterior: relacionadas a la contención)

Firewall
Son elementos de protección perimetral de red que mediante políticas establecidas proceden al control de tráfico en la red, su función es identificar un tipo de tráfico y permitirlo o denegarlo en un puerto determinado.
Los puertos pueden permitir una posible vulnerabilidad del sistema y un acceso a la información de manera no autorizada, por lo cual deben ser monitoreados.
En muchos casos puertos inutilizados pueden ser blanco de ataques que sin la debida protección se hacen aún más vulnerables.

Dentro de los Firewall también se cuenta con DMZ o también llamada zona desmilitarizada, la cual permite crear dentro de una red interna una red alterna solo para uso de dispositivos que necesiten estar en contacto con redes externas, es decir que necesiten ser visibles públicamente, de esta manera se realiza un control sobre la seguridad de los equipos netamente internos, lo que mejora la seguridad de la información más sensible.

UTM
Un UTM o Firewall UTM es un dispositivo de redes que permite la gestión unificada de amenazas, por ese motivo se maneja un solo proveedor para todos los servicios de seguridad lo que permite una simplificación al momento de implantar controles y políticas y al realizar la gestión y el manejo de cada servicio de seguridad.

Muy utilizado para la gestión de la seguridad de la información en pequeñas y medianas empresas, este tipo de dispositivos cuenta con una centralización de varias funcionalidades en una sola consola lo que permite una visión unificada de elementos que comúnmente se tendría que operar aisladamente y con diferentes proveedores y configuración.

Un UTM tiene operación como un Firewall perimetral que permite el control de políticas de puertos, pero ofrece otras funcionalidades como IDS/IPS y antivirus. En versiones más avanzadas este tipo de soluciones también entregan: NAT – VPN - Filtros de contenido
Presenta ventajas de flexibilidad, tener una integración completa lo que significa un menor costo que implementar soluciones individuales, menor dificultad del manejo y complejidad

Por el hecho de manejar toda la seguridad en una sola consola pueden presentarse desventajas al ser un único punto de seguridad o presentar inconvenientes en cuanto al rendimiento pues por el UTM pasaría todo el tráfico a proteger.

NGFW
Firewalls de última generación brindan una revisión profunda de paquetes, gracias a los avances tecnológicos que lo permiten, de esta manera se tiene una verificación sobre las aplicaciones y no sobre los puertos como lo hacía un Firewall convencional, está destinado a empresas que cuenten con gran tráfico de datos, esto hace que en conjunto se creen políticas de control de acceso más eficientes que estén alineadas con las actuales amenazas de la seguridad de la información.

Estos dispositivos se presentan en consola física o en máquina virtual, con múltiples puertos 10GE en formato SFP+ o QSFP en formato CFP2, dependiendo de la capacidad de procesar el tráfico y con un conjunto de servicios como:
Control de aplicaciones - Filtrado Web – IPS – Antivirus - VPN

IDS
Los IDS son los sistemas de detección de intrusiones que permiten hacer un seguimiento tanto a host como a redes a nivel de tráfico, permite la prevención de posibles amenazas o intrusiones que pongan en peligro la disponibilidad, integridad y confidencialidad de la información.

IPS
Los IPS son los sistemas de prevención de intrusiones que permiten hacer un seguimiento tanto a host como a redes a nivel de tráfico, permite no solo la detección sino también prevención de posibles amenazas o intrusiones que pongan en peligro la disponibilidad, integridad y confidencialidad de la información.

EDR
Las soluciones EDR son de tipo software instalado en los equipos finales, sean host o servidores, estas aplicaciones permiten combatir las amenazas avanzadas y responder a incidentes en los puntos finales de la red, combinan características que incluyen I.A, realimentación de ataques a nivel mundial, alarma de vulnerabilidades, análisis de comportamiento, control de aplicaciones, listas blancas de aplicaciones, monitorización de la red y respuesta a incidentes.

De esta manera se puede hacer gestión de la seguridad de la información de una manera proactiva en conjunto con otros dispositivos, de esta manera se puede mejorar la visibilidad de los comportamientos y procesos en el punto final, administrar los activos físicos y de información, apoyo en la recopilación de datos para proporcionar a TI análisis

de dispositivos.
Las Plataformas para este tipo de solución es entregada por el mismo proveedor, es decir, no se compran o instalan equipos, se realiza la instalación de software en cada máquina cliente según licencia y proveedor, con lo cual se vincula este a un sistema especifico que el cliente puede visualizar en línea.

XDR
XDR presenta un enfoque EDR que incluyen más posibilidades de verificación como servidores, e-mail, red, y aplicaciones Cloud mediante una plataforma virtual, que maneja IA y aprendizaje automático, análisis de amenazas y verificación de eventos de una manera más rápida y eficiente, esto permite al menos en teoría una proactividad ante amenazas y una reacción inmediata frente a ataques.

Este tipo de tecnología lo que busca es condensar toda la información en una sola plataforma, evitando grandes grupos especializados de personal de seguridad, utilización de diferentes plataformas, equipos y software que en muchos casos dificulta la identificación apropiada de vulnerabilidades y ataques, por lo que de esta manera se logra una eficiencia de personal, al contar con la información optima e incluso procedimientos para corregir los eventos de seguridad.
Las soluciones XDR están disponibles como paquetes de servicio gestionado los cuales apoyaran los equipos internos de seguridad informática, además de obtener análisis. Completos, búsqueda de amenazas, planes de respuesta y recomendaciones de reparación 24×7.

Antivirus
Los antivirus quizás son la más conocida y utilizada herramienta para la seguridad de la información, se basan en software que identifica el Malware mediante la comparación de bases de datos de virus ya identificados, algo conocido como firmas, por lo tanto, es primordial mantenerlo actualizado, así como contar con uno que sea adecuado a las necesidades y que preferiblemente cubra una buena cantidad de malware como:
Actualmente este tipo de soluciones viene evolucionando a presentación de paquetes de seguridad tipo EDR, en la cual se instalan en las máquinas de usuarios el cual opera no solo como un antivirus convencional, sino que también permite funcionalidades más avanzadas para la protección de los datos.

WAF
Firewall de aplicaciones web, sirve para la protección de páginas y aplicaciones tipo web en el cual se realiza un análisis de tráfico basados en protocolos HTTP desde y hacia la página, de esta manera se busca minimizar las posibles vulnerabilidades, así como sus amenazas asociadas, entre ellas inyección de código SQL, XSS, CSRF o falsificación de petición en sitios cruzados.
Los WAF pueden presentarse tanto a nivel de hardware como de software

Firewall de Base de Datos
Orientados para la protección específica de bases de datos, un Firewall de base de datos es un software que busca restringir el tráfico al emplear políticas más estrictas al ingresar

a las bases de datos, por tal motivo mitigan las posibilidades de una amenaza o un ataque exitoso.
Puede ser útil para evitar inyecciones de código, ataques DoS, perdida de información o autenticación, auditoria de ingreso de usuarios, control de usuarios, análisis forense en caso de intentos de intrusión.

2.13 Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

El equipo de Blue Team hace un deep-inspection sobre las medidas de seguridad implementadas en la infraestructura de red normalmente de una organización, es decir que realiza una defensa de la seguridad de la información según hallazgos del Red Team, de una manera proactiva.

- Seguridad perimetral
  Políticas de seguridad
  Políticas de Prevención de intrusos (IPS)
  Políticas de WAF para protección de servicios web

- Seguridad DMZ
  Aislamiento automático de servidores comprometidos
  Contención del atacante

- Seguridad de Endpoint
  Integración a herramientas de seguridad para la correlación de eventos

De esta manera el Blue Team mantiene vigilancia permanente sobre sistemas, aplicaciones y posibles vulnerabilidades, actuando de manera que estas puedan ser mitigadas antes de que se pueda presentar una amenaza.

Por su parte un equipo de respuesta a incidentes informáticos (CSIRT- CERT) puede hacer parte de una organización, pero normalmente se implementa para sectores públicos, militares o gubernamentales, que busca ser una fuente de información y mitigación ante posibles amenazas a la seguridad informática.
Por eso dentro de sus funciones se encuentran:

- Brindar información sobre hallazgos
- Alertar sobre vulnerabilidades
- Entregar pautas para la configuración de herramientas de seguridad
- Gestionar los incidentes de seguridad
- Gestionar las vulnerabilidades cuando estas se presenten.

2.14 Análisis sobre la pertinencia de trabajar con CIS "Center For Internet Security" como propuesta de aseguramiento por parte de un equipo de Blue Team.

El Center for Internet Security es el principal estándar reconocido de la industria para la guía de configuración segura, que desarrolla listas de verificación con el fin de ayudar a identificar y mitigar las vulnerabilidades de seguridad conocidas en una amplia gama de plataformas.
Este sería un gran banco de información útil y actualizada para Blue Team al aplicar las buenas prácticas de configuración o implementación de la seguridad de la información, El CIS provee de documentación para el manejo y correcta operación de herramientas de ciberseguridad para la prevención y detección de amenazas, así como para múltiples sistemas operativos, server software, dispositivos de red, software de escritorio, cloud providers.

Empresas de ciberseguridad forman lo que hoy en día se conoce como CiberThreat Alliance para compartir internamente datos sobre amenazas de cero día (0-day) lo que garantiza colaborar con estas organizaciones es que ayuda a tener un panorama de visibilidad frente a los riesgos que abundan en la red y que son explotados a cada momento.

Como propuesta de aseguramiento, Blue Team garantiza que estas integraciones ayudan a la organización a ser parte de esta alianza que busca proteger el más valioso activo: la información.

2.15 Análisis sobre las funciones y características principales de un SIEM.

SIEM (Security Information and Event Management) o Gestión de Eventos e Información de Seguridad, es un software que hace recopilación y monitoreo de los logs de diferentes dispositivos y elementos de seguridad el cual se encarga de analizar los diferentes datos entregados por dispositivos de seguridad como son Firewalls, IDS (Sistema de detección de intrusiones) , IPS (Sistema de prevención de intrusiones), Antimalware, WAF (Firewall de aplicaciones web), Firewall de base de datos, proxys, EDR (Endpoint Detection and Response).

Gartner definió el termino SIEM en un reporte del año 2005 en el cual se reúnen los conceptos de Gestión de Eventos de Seguridad (SEM) y el de Gestión de Información de Seguridad (SIM), donde el SEM es el encargado de cubrir el monitoreo y relación de los eventos en tiempo real, mientras el SIM se encarga de las etapas de almacenamiento, así como del análisis y generación de reportes.

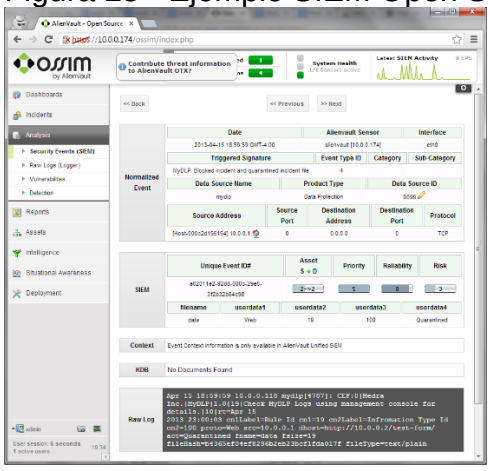
Por lo tanto, SIEM debe estar en la capacidad de:

- Centralizar la información sobre potenciales amenazas
- Determinar qué amenazas requieren resolución y cuáles son solamente ruido (falsos positivos)

- Escalar temas a los analistas de Seguridad apropiados, mediante las debidas alertas, para que estos puedan tomar una acción acertada y rápida.
- Documentar el contexto de los eventos de Seguridad para permitir resoluciones bien informadas – generación de base de datos.
- Documentar, en un registro de auditoría, los eventos detectados y cómo fueron resueltos.
- Cumplir con las regulaciones de la industria en un formato de reporte sencillo PCI DSS – ley de protección de datos.

Por lo tanto, el SIEM proporciona los medios para integrar aquellas fuentes de información que en principio están separadas para ver y analizar todos los datos en tiempo real, con el fin de poder actuar rápida y acertadamente ante algún evento anormal que se registre en los equipos.
Una solución basada en SIEM se convierte en un elemento fundamental para obtener, gestionar y presentar la información necesaria para monitorizar datos y consecuentemente actuar rápidamente sobre la explotación de vulnerabilidades amenazas, cuando toda esta actividad está capturada en un registro de auditoría detallado, el personal de seguridad de la información tomara las decisiones más acertadas para proteger datos y mitigar la amenaza.
Dentro de estos elementos que centralizan la información de diferentes fuentes y puntos geográficos se tienen:

SIEM open source
SIEM basado en open source, el cual puede ser tenido en cuenta para Pymes ya que es intuitivo, relativa fácil instalación, tiene como ventajas que presenta una comunidad que está retroalimentando y mejorando la aplicación, otra ventaja es que es gratuito y puede contar con buenas funcionalidades, como contra este tipo de proyectos no cuentan con asesores, sino que se apoyan en la investigación directa para identificar casos de éxito o error.
Figura 23 - Ejemplo SIEM Open Source con OSSIM de AlienVault



Fuente: https://mydlp.com/mydlp-ossim/

SIEM comercial
SIEM de carácter privado, el cual es desarrollado por una empresa para su comercialización, por esta razón es más extenso que un SIEM open source en cuanto a recursos, como ventajas cuenta con soporte de fabricante, y acompañamiento para implementaciones enfocadas a las necesidades puntuales, por otro lado, también presenta limitaciones financieras pues son aplicaciones costosas, por otro su complejidad puede evitar que se alcance todo su potencial.

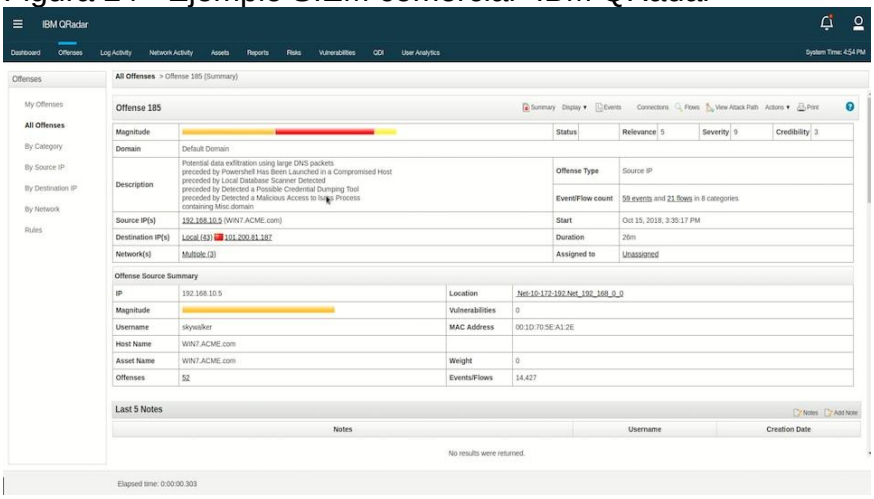
Dentro de esta solución se presentan SIEM físicos, en software, híbridos y en nube, los físicos plantean el despliegue de dispositivos físicos que permiten recolectar la información de los diferentes elementos de red y host en un entorno especifico, los sensores o sondas de adquisición de datos deben estar comunicados con un sensor principal, y de esta manera el sensor principal debe estar conectado con todos los sensores remotos ubicados en los sitios, debido a esto su implementación y costo puede incrementarse, además está implícito que los equipos físicos pueden no ser escalables a futuro con nuevos tipos de amenazas o ataques que se desarrollen a partir de tecnología más avanzada.
La implementación física de un SIEM como anteriormente se utilizaba está dejando de ser una práctica acertada teniendo en cuenta el rápido desarrollo de amenazas, así como el descubrimiento de nuevas vulnerabilidades que antes eran desconocidas, lo cual puede hacer que un SIEM físico se haga obsoleto en un tiempo relativamente corto.

Por su parte también se pueden encontrar soluciones SIEM a partir de software, que puede hacerlo menos costoso y más escalable gracias a las actualizaciones que se realicen adecuadamente, la idea de este tipo de SIEM es que la implementación final utilice menos dispositivos físicos, también es importante aclarar que este tipo de soluciones tiende a que el proveedor realice un acompañamiento antes, durante y después de la puesta en marcha.
Las soluciones empresariales de SIEM en la nube buscan reducir completamente el uso de hardware y software dejando todo en manos de la implementación y nube del proveedor, con lo cual se facilita la puesta a punto y se recibe para administrar.
SIEM en la nube, este tipo de soluciones se da completamente en la nube, los equipos de monitoreo se direccionan a elementos específicos en la red, en este sitio particular se almacena la información recolectada, donde además también se clasifica y se presenta al usuario, por esto normalmente este tipo de soluciones están apoyadas en el uso de aplicaciones con IA, las cuales pueden generar las alertas más eficientemente luego de pasar por un filtro de falsos positivos o simplemente de eventos en la red que no necesariamente son una amenaza.

Un monitoreo de SIEM basado en soluciones de cloud se presenta como una buena opción sin tener la necesidad de invertir en equipo, al operar como un SIEM convencional entrega la información necesaria para la toma de decisiones, este tipo de soluciones también presenta la posibilidad de contar con apoyo de expertos para la identificación de eventos de seguridad, lo que sin duda lo hace aún más funcional, pues ya no se hace necesario todo un grupo de expertos en seguridad.

Como ejemplo de SIEM de este tipo se tiene IBM QRadar on Cloud el cual es una solución que puede ayudar a detectar ataques de ciberseguridad y brechas en la red, para que pueda adoptar medidas antes de sufrir daños considerables o para que pueda responder inmediatamente ante cualquier pérdida de datos críticos. El equipo encargado de la seguridad informática solo se debe enfocar en revisar condiciones anómalas y en aplicar parches a las vulnerabilidades más importantes de los activos, ya que no se hace necesario la instalación, revisión, gestión de elementos anexos a la red.

Figura 24 - Ejemplo SIEM comercial -IBM QRadar



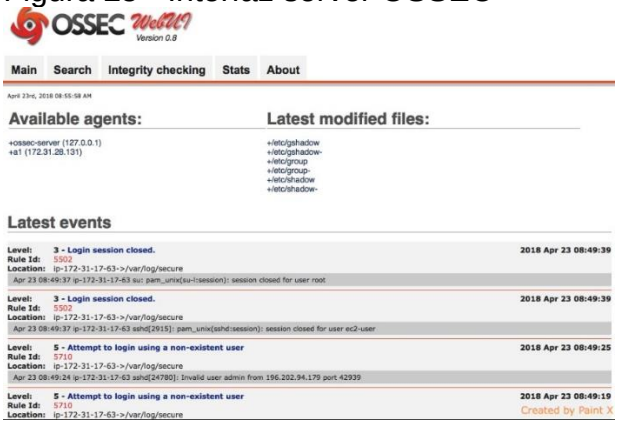
Fuente: https://itbutler.com.au/qradar/

2.16 Informe de elección de 3 herramientas que permitan contener ataques informáticos.

OSSEC (IDS)

Es uno de los más populares open-source IDS que incluye herramientas para correlación de eventos, capacidades de monitoreo, análisis de vulnerabilidades, respuesta automática de amenazas.

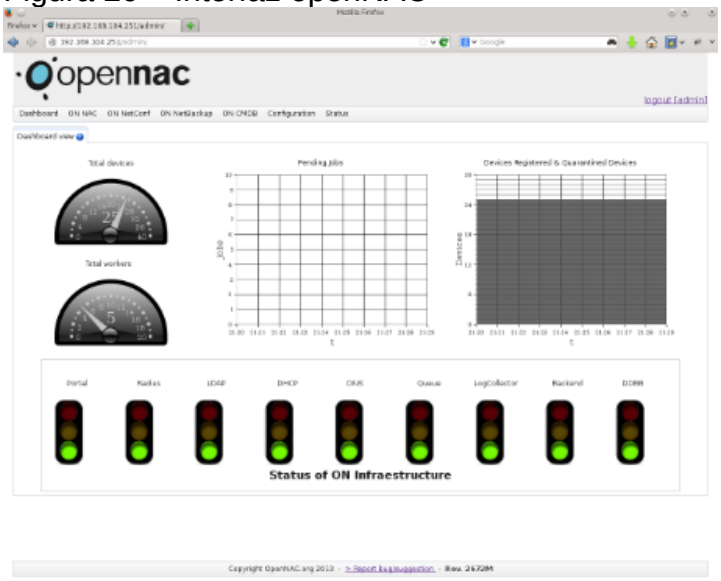
Figura 25 - Interfaz server OSSEC



Fuente: http://grepthelinuxblog.blogspot.com/2012/03/installing-ossec-hids-web-user.html

Open NAC (NAC – Network Access Control)
Esta herramienta también se integra con herramientas de análisis, el cual detectan equipos con un comportamiento anómalo y mediante un IoC, aíslan el equipo si este se encuentra comprometido.

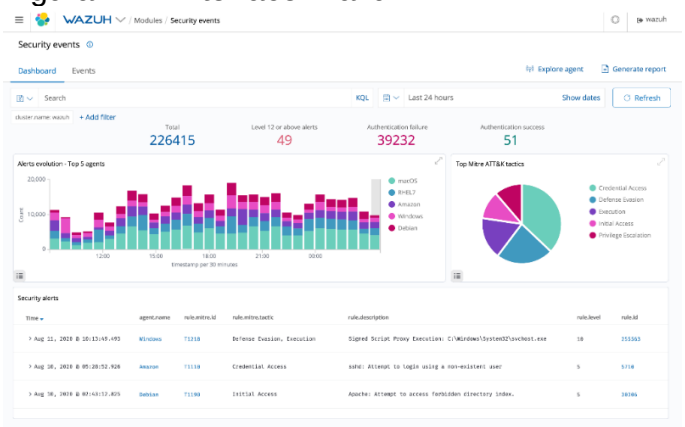
Figura 26 – Interfaz openNAC



Fuente: http://www.opennac.org/opennac/en/solution/screenshots-opennac.htmlOpen

WAZUH EDR (Endpoint Detection and Response)
El perímetro o borde de red, no es el único punto donde se establecen las políticas de seguridad a pesar de ser importante, las redes modernas tienden a ser cada vez más abiertas y sin fronteras, hay escenarios externos como vpn, proveedores, proveedores cloud, los cuales crean retos para los administradores de la ciberseguridad de la información. Las herramientas EDR están enfocadas en la respuesta automática desde el punto de vista de los endpoints, servidores o equipos finales de usuarios.

Figura 27 – Interface Wazuh



Fuente: https://wazuh.com/

Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam.

Es importante tener en cuenta que este tipo de implementaciones lo que busca es aprovechar los conocimientos del personal a cargo y herramientas disponibles para identificar, analizar, corregir y mitigar las diferentes posibles vulnerabilidades que se encuentren en un sistema informático, de esta esta manera se reducen los riesgos a la información y la posibilidad de que sea explotada una posible amenaza, el Red Team & Blue Team deben trabajar por un objetivo común a ambos a pesar de que aparentemente sus estrategias, metodologías y fines sean diferentes, lo que se pretende es alcanzar estado solido y permanente de los pilares de la seguridad de la información

Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

A nivel corporativo se pueden tener dificultades de presupuesto que pueden retrasar el correcto uso de herramientas que permitan una extensa protección de la seguridad informática, en cualquier caso, el especialista en seguridad de la información debe contar con elementos adecuados ya sean pagos o de software libre.

- Actualización de sistemas operativos: debe de ser global en empresas, entidades, corporaciones que se cuente con la última actualización de los sistemas operativos en producción, evitar trabajar con sistemas operativos en desuso y migrar lo que sea necesario a nuevas plataformas.

- Parcheo de vulnerabilidades: Identificar y analizar las diferentes vulnerabilidades que pueda presentarse a nivel lógico del software y aplicaciones, buscando fortalecer en conjunto el aspecto de la seguridad de la información.

- Software antivirus: Manejar un antivirus que cumpla con necesidades básicas, preferiblemente que tenga funciones avanzadas para simplificar su manejo.

- Manejo de herramientas de seguridad perimetral como Firewall, UTM, que permitan generar DMZ, esto impactara positivamente la seguridad de la información al segmentar equipos que tengan acceso publico y unos equipos con acceso limitado.

- Manejar uso de información encriptada: Hacer uso de encriptación para el almacenamiento de la información sensible, genera una mayor preservación de esta a ser victima de una fuga de información.

- Manejo de herramienta que alerten sobre actividades sospechas IDS-IPS: Estos permiten identificar un evento en tiempo real, haciendo mas rápida su contención y mitigación, también permite mantener un monitoreo permanente en la red y hacer uso de logs para auditoria.

3. CONCLUSIONES

- Para el Especialista en Seguridad Informática es de vital importancia conocer los diferentes delitos informáticos contemplados en las leyes colombianas, no solo para intentar proteger la red que administra frente a ellos, sino también para concienciar a nivel laboral, social y personal a su entorno, de las diferentes amenazas informáticas que pueden presentarse a diario.

- Realizar actividades en las cuales se ponen a prueba los conocimientos informáticos para la búsqueda y hallazgo de posibles vulnerabilidades, así como su tratamiento para mitigar y evitar amenazas o ataques.

- Estar preparado no solo con el conocimiento de las herramientas informáticas, sino también poder identificar posibles delitos informáticos como en este caso mediante una propuesta o contrato de trabajo, en la cual se puede llegar a cometer un ilícito y acarrear con las consecuencias legales en caso de tener o manejar información obtenida por métodos abusivos y no autorizados.

- Entender cómo se presentan los riesgos a la seguridad de la información por medio de vulnerabilidades en un sistema, haciéndolas aptas para su explotación, la identificación y mitigación de amenazas debe ser una tarea en constante desarrollo que no se permite pausas, mantenerse al tanto de nuevas vulnerabilidades y formas de aprovecharla así como la manera de contrarrestarlas puede ayudar al especialista en seguridad de la información a estar un paso antes y brindar la seguridad que requiere su sistema.

- Se presentan diferentes tipos de tecnologías las cuales hacen parte del universo de la protección de la seguridad informática, dentro de estos se deben elegir aquellos que presenten funcionalidades acordes a los requerimientos puntuales.

- Tener sentido crítico para el análisis y la investigación de incidentes desarrollando la capacidad de identificar y entender la manera en la cual se ejecutan posibles delitos informáticos. como en este caso realizar un hardening a la información a través del uso de herramientas de tipo GPL.

4. REFERENCIAS BIBLIOGRÁFICAS

MINTIC. (2009). Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/inicio/3705:Ley-1273- de-2009

COPNIA. (2020). Código de ética | Copnia. https://www.copnia.gov.co/tribunal-deetica/codigo-de-etica

COPNIA (2003). Ley 842 de 2003. | Copnia. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

EL TIEMPO (2015). Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea]. https://www.eltiempo.com/archivo/documento/CMS-15141236

EL ESPECTADOR (2018). Caso Andrómeda y sus interrogantes [En línea]. https://www.elespectador.com/noticias/judicial/casoandromeda-y-sus-interrogantes/

EL ESPECTADOR (2018). Los detalles de Andrómeda, según la Procuraduría. [En línea] https://www.elespectador.com/noticias/judicial/losdetalles-de-andromeda-segun-la-procuraduria/

Villanueva, Lina María Patricia Manrique. (2019) "en Colombia: agencias y complicidades mediáticas. https://www.researchgate.net/profile/Lina-Manrique-Villanueva/publication/336273968_Complicidades_y_agencias_mediaticas/links/5d97e75b458515c1d395778f/Complicidades-y-agencias-mediaticas.pdf

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28).

Salazar, J. F. (2011). Situación normativa de la Sociedad de la Información en Colombia. Criterio Jurídico, 9(1).

TINOCO LINARES, Ana, et al. Análisis y clasificación de los ataques y sus exploits: Framework Metasploit como caso de estudio. 2020.

PASTOR RICÓS, Fernando. Pentesting y generación de exploits con Metasploit.2020

NIÑO ORDOÑEZ, José Rafael, et al. Capacidades Tecnicas, Legales y de Gestión para Equipos BlueTeam y RedTeam. 2020.

AVILA GUALDRÓN, Miguel Andrés, et al. Estudio de las mejores prácticas de Ethical Hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración.2018.

DENIS, Matthew; ZENA, Carlos; HAYAJNEH, Thaier. Penetration testing: Concepts, attack methods, and defense strategies. En 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016. p. 1-6.

JASWAL, Nipun. Mastering Metasploit. Packt Publishing Ltd, 2016.

Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287). 2014.
https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-6287

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). CVE-2014-6287CVE-111386. 2016.
https://www.exploit-db.com/exploits/39161
https://www.exploit-db.com/exploits/34852

Rejetto HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution.2014.
https://www.kb.cert.org/vuls/id/251276

Security vulnerabilities of Rejetto Http File Server : List of all related CVE security vulnerabilities.
https://www.cvedetails.com/vulnerability-list/vendor_id-14180/product_id-29196/Rejetto-Http-File-Server.html

FUENTES FORERO, Álvaro Augusto, et al. Estudio de la eficiencia y eficacia de las metodologías hardening en la reducción de vulnerabilidades en las empresas colombianas.

CRUZ MORENO, Oscar Alonso. Diseño e implementación de un proceso de hardening. 2017.

IBÁÑEZ NARANJO, Camilo Alejandro, et al. Construcción de guías de hardening que eleven los niveles de seguridad para los funcionarios de entidades financieras que laboran desde la modalidad del teletrabajo. 2021.

GARCIA, Jairo. Ventajas e implementación de un sistema SIEM. Máster universitario en seguridad de las tecnologías de la información y las comunicaciones. España Universidad Abierta de Cataluña. 2018. 84 p.

GARCIA, Javier Antonio. Propuesta de diseño e implementación de un Centro de Operaciones de Seguridad (SOC) y un Centro de Repuesta a Incidencias (CSIRT) para la Universidad de Ingeniería. Informe final para optar al título de Máster en gestión de la seguridad de la información. Managua. Universidad Nacional de ingeniería. Facultad de ciencias y sistemas. 2016. 115 p.

LINK VIDEO PRESENTACION

https://www.youtube.com/watch?v=c5j4xtX-EHk

REVISION DE PLAGIO

	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud	Calificación	Nota general	
Ver recibo digital	etapa5	1549302775	2/04/2021 18:47	16%	N/A	--	Entregar Trabajo