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

JEAN POLO CEQUEDA OLAGO

Monografía

M.Sc. JOHN F. QUINTERO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2022

CONTENIDO

LISTADO DE FIGURAS

RESUMEN

En este documento se recopila un breve recuento de la legislación Colombiana frente a la seguridad informática, se documenta uno de los procesos más valiosos para determinar el grado de riesgo de la informática empresarial, como lo son las pruebas de intrusión, se documentan herramientas para estas pruebas y se estable un banco de trabajo para desarrollar practicas sobre el tema. Se realiza un breve análisis de una situación que no está lejos de la realidad, que basándose en la legislación existente y el código de ética para las ingenierías, se intentan identificar posibles actuaciones ilegales y que quebrante la ética profesional. Por último de determina el proceder ante situaciones que puede degradar el normal funcionamiento de un sistema informático, se contextualiza con la simulación de un ataque informático controlado en el banco de trabajo. Se reconocen roles importantes en los equipos de respuesta a incidentes, donde cada equipo aporta desde su perspectiva los conocimientos adquiridos, pero de forma sinérgica benefician la seguridad informática de la organización.

GLOSARIO

VULNERABILIDAD, es la incapacidad de resistencia cuando se presenta un fenómeno amenazante.

EXPLOTACIÓN, es el proceso mediante el cual se puede sacar provecho de un sistema informático.

EXPLOIT, herramienta utilizada para explotar una vulnerabilidad.

VIRTUALBOX, software hypervisor sobre un sistema anfitrión.

NMAP, software utilizado para el reconocimiento de sistemas informáticos.

INCIDENTE, materialización de un evento que provoca un impacto en un activo informatico

HARDENING, proceso mediante el cual se aplicar uno o varios controles sobre un sistema informatico en pro de reducir la probabilidad de ocurrencia de incidentes.

SIEM, Información sobre seguridad y gestión de eventos

AMENAZA, circunstancia desfavorable que puede ocurrir de forma natural, accidental o intencionada y que deriva en un incidente de seguridad.

PENTESTING, es un conjunto de pruebas de penetración con ataques hacia los sistemas informáticos con la intención de encontrar sus debilidades o vulnerabilidades

INTRODUCCIÓN

Las empresa u organizaciones comprenden que uno de los activos más importantes que tienen son la información; el estado Colombia, por convicción o requerimientos de otros países para establecer Tratados de Libre Comercio, han ido agregando a su gran compendio de leyes y normatividad existente, intentando blindar ese activo que tanto valoran los empresarios.

La seguridad informática toma cada día un papel más importante en la humanidad, la pandemia dejo al descubierto muchas cosas y entre esas, lo vulnerable que somos. Hoy en día la información se puede considerar uno de los activos más valiosos de una organización, la dinámica de muchos negocios genera cada días más datos, los cuales deben ser organizados, almacenados, procesados, transmitidos, pero sobre todo protegidos.

La legislación Colombiana en cuando a delitos informáticos o vulneraciones sobre la información es relativamente nueva, la primera ley tiene vigencia desde el 2009, casi a punto de cumplir 13 años y la ley 1581 de 2012, menos de 10 años, son una primera aproximación a salvaguardad el valioso activo, la información. La reglamentación, la interpretación, las sentencias de la corte constitucional son muy pocas, pero van clarificando las diferentes situaciones que se presentan.

Los ataque informáticos son inminentes, los incidentes se pueden presentar en el momentos menos esperado, constantemente se debe revisar, analizar, identificar posibles escenarios por los cuales los sistemas informáticos pueden pasar. Tener claro que posibles acciones se pueden realizar antes para evitar que existan incidentes, pero que si se presentan se le pueda dar manejo y darle continuidad al negocio.

OBJETIVOS

GENERAL

Reconocer el rol, características y funcionalidades de los Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

ESPECÍFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.
- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión
- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

1. ASPECTOS LEGALES Y CONCEPTUALES

1.1. LEGISLACIÓN COLOMBIANA PARA LA SEGURIDAD DE LA INFORMACIÓN

1.1.1. LEY 1273 DE 2009

La ley 1273 de 2009 fue la primera ley donde se podían tipificar situaciones, que involucraban acciones con o contra equipos informáticos, como delitos, lo cual permitía a las autoridades Colombianas sancionar o privar de la libertad a ciudadanos Colombianos que estuviesen atentando contra sistemas informáticos. Se conoce como la ley de "Delitos Informáticos" en el momento de aprobación, en el año 2009, nuestro país estaba en pleno crecimiento del uso de las TIC y se empezaba a reconocer lo valioso que puede ser la información.

Las tipificaciones son:

- ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO
- OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN
- INTERCEPTACIÓN DE DATOS INFORMÁTICOS
- DAÑO INFORMÁTICO
- USO DE SOFTWARE MALICIOSO
- VIOLACIÓN DE DATOS PERSONALES
- SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES
- HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES
- TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

La ley estable penas de prisión hasta de 120 meses y multas hasta 1500 salarios mínimos legales mensuales vigentes en Colombia según el delito, además puede agregar más tiempo y dinero si existen gravámenes, como por ejemplo, que las actuaciones sean contra el estado o el sector financiero, o que sean realizadas por un servidor público, entre otras situaciones.

1.1.2. LEY 1581 DE 2012

La ley estatutaria 1581 de 2012 está orientada a reglamentar los artículos 15 y 20 de la constitución nacional, derechos al buen nombre, intimidad personal y a la información.

La ley es bastante amplia y precisa, define principios para evitar interpretaciones ambiguas, categoriza los datos que una persona puede proporcionar, aclara el manejo de datos personales de niños, niñas y adolescentes, define los derechos que tienen los titulares de la información, establece los procedimientos que se

pueden realizar sobre los datos personales recolectados, define los deberes de los responsables o encargados del tratamiento de los datos personales, establece que la superintendencia de industria y comercio, velará por la garantía que se haga un buen tratamiento de los datos suministrados, establece sanciones, entre otras disposiciones.

Su carácter de ley estatutaria indica que en prevalencia de leyes, lo único que está por encima de ella es la constitución nacional, lo cual brinda muy buenas garantías a los titulares de la información y grandes responsabilidades a los responsables o encargados del tratamiento de la información.

1.1.3. Decreto 886 de 13 de mayo de 2014

El cual reglamenta la información que debe contener el registro Nacional de Bases de Datos y las condiciones que inscripción de los responsables del tratamiento de los datos. Adicionalmente estable características de los canales para ejercer los derechos que tienen los titulares a realizar acciones sobre su información.

1.1.4. Decreto 1377 de 27 de junio de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012

Este decreto reglamenta parcialmente la ley 1581 del 2012, amplia algunas definiciones, aclara el uso de datos sensibles, el proceso de autorización, requisitos especiales para el tratamiento de datos personales de niños, niñas y adolescentes.

1.1.5. Ley 1266 de 2008

La ley 1266 de 2008 es conocida como la ley de habeas data, está orientada al igual que la ley 1581 a reglamentar el artículo 15 de constitucional nacional, derecho al buen nombre, al manejo respetuosa de los datos personales, pero, principalmente en entidades bancarias, crediticias, financieras, etc. Al igual que todas las leyes mencionadas, existen excepciones a los procedimientos pero solo mediante órdenes judiciales o situaciones excepcionales para que el estado actúe.

1.1.6. Directiva presidencial 03 de 15 de marzo de 2021

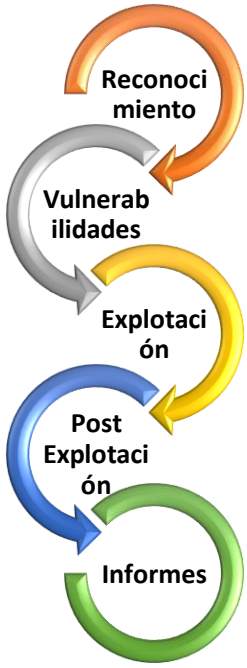
Esta directiva define unos lineamientos respecto a la seguridad digital, enmarcada en la ley 1955 de 2019, el cual contiene le Plan Nacional de Desarrollo y que buscaba disminuir costos de funcionamiento y mejorar los servicios mediante la innovación. La directiva invita a que se cumplan las directrices del MinTIC, se

definan políticas fuertes, se establezcan matrices de riesgo, implementación de modelos de seguridad y privacidad de la información, entre otras.

1.2. ETAPAS DE LAS PRUEBAS DE INTRUSIÓN

Para la realización de pruebas de intrusión, dependiendo de la metodología o de las diferentes formas de hacer las cosas, en la siguiente imagen se establecen cinco fases

Fig. 1. Fases de una prueba de intrusión



Fuente: Jean Polo Cequeda Olago

1.2.1. Reconocimiento

En la fase de reconocimiento se identifica todos los posibles datos del sistema probado, dependiendo de la modalidad de la prueba, blanca, negra o gris, la cantidad de información suministrada al tester varia, lo cual implica que el profesional que realiza la prueba, debe dedicar más tiempo, utilizar más herramientas y valerse de su experiencia para intentar conocer más al sistema probado. En esta fase se puede utilizar herramientas tan sencillas como el comando ping o telnet para determinar que dispositivos hay en la red o si algún puerto está abierto, herramientas un poco más especializadas como nmap que nos escanea sistemas informáticos e intentar brindar tanta información como sea posible, por ejemplo la versión del paquete informático que tiene un socket accesible y que fue

identificado por nmap. Dependiendo del sistema informático probado, se puede utilizar herramientas para identificar metadatos en los sitios web, incluso el metabuscador más famoso o popular puede proporcionar información importante para esta fase.

1.2.2. Análisis de vulnerabilidades

La segunda fase que se puede dar en una prueba de intrusión es el establecimiento de las posibles vulnerabilidades existentes, con toda la información recopilada se puede buscar que vulnerabilidades tienen los sistemas encontrados, existen herramientas tan completas como puede ser NESSUS o NEXPOSE, con sus versiones gratuitas pero con la gran potencia que puede dar una versión licenciada, pero también existen bases de datos con las posibles vulnerabilidades documentadas, con scripts, mejor llamados exploits desarrollados para explotar dichas vulnerabilidades.

1.2.3. Explotación

La fase explotación se utilizan herramientas desarrolladas, documentadas y de fácil utilización, disponibles para muchas personas de una manera muy fácil, pero también son herramientas desarrolladas prueba tras prueba, conformando un banco de pruebas personal. Una excelente herramienta utilizada en esta fase es Metasploit un framework con una gran cantidad de exploits muy bien documentados y con una gran cantidad de información que sirve para utilizar esta herramienta. Adicionalmente existen sitios web que proporcionan información de la vulnerabilidad lo cual permite comprender como se pudiese comprometer la seguridad, está en la habilidad de programación que el tester desarrolle nuevas herramientas.

1.2.4. Post Explotación

Una vez comprometido un sistema informático es importante determinar el alcance que puede tener un ciberdelincuente si explotase dicha vulnerabilidad, determinando el impacto y las acciones que desde ese sistema puede desencadenar en otros sistemas. Es importante intentar determinar qué relaciones de confianza existen desde este sistema comprometido para planear pruebas de intrusión a estos otros sistemas posiblemente comprometidos. Adicionalmente, se debe determinar si comprometido este sistema informático, se puede escalar privilegios, crear super usuarios, crear puertas traseras para garantizar el acceso no autorizado, entre otras acciones. Algunas herramientas que se pueden utilizar son proxys o keyloggers, incluso la misma CLI del sistema informático proporciona comandos que se puede utilizar después de comprometido el sistema.

1.2.5. Informes

Esta es una fase que algunas teorías no la contemplan como fase, pero requiere buen tiempo y es realmente muy importante, ya que, la generación de un buen informe de la prueba de intrusión permite no solo hablar bien del profesional o empresa que lo realiza, sino que desde el punto de vista del cliente, le permite tomar decisiones partiendo de una comprensión sencilla del informe y planteando soluciones o medidas para mitigar las situaciones encontradas. Es importante la evidencia, por lo tanto los pantallazos, videos o registros de acciones son relevantes, así como una descripción clara y sencilla de la situación, alcance, impacto y demás detalles que sean importantes; por último posible recomendaciones ante las situaciones encontradas. En esta fase es suficiente un procesador de texto, pero se pueden adicional otras herramientas ofimáticas para la creación del informe.

1.3. HERRAMIENTAS PARA PRUEBAS DE INTRUSIÓN

1.3.1. Herramientas

Existen muchas herramientas, algunas más sencillas, algunas más conocidas, algunas más eficientes que otras para utilizarlas en pruebas de intrusión, cada prueba es diferente; existen muchos factores que de un sistema a otro muy similar marcan diferentes caminos a tomar, aquí es donde la experticia del profesional encargado de la prueba de intrusión es pues a prueba.

Algunas herramientas relevantes, muy conocidas, bastante documentas y muy eficientes se listan a continuación.

1.3.1.1. Metasploit

Es un framework para intentar explotar vulnerabilidades según sus bases de exploits que tiene, la versión libre tiene unas funcionalidades y cantidad de exploits reducido comparado con la versión comercial; Su consola MFSCONSOLE, le permite ejecutar en una línea de comandos, dependiendo del exploit requiere la URL o dirección de la víctima, puede requerir parámetros como el payload u otros parámetros requeridos para lograr explotar la vulnerabilidad.

1.3.1.2. Nmap

Networt Mapper es una excelente herramienta para identificar rápidamente socket abiertos e identificar nombres y versiones que están corriendo por dichos sockets,

es muy liviana, su CLI es muy versátil y ajustable ante la presencia de herramientas de seguridad como firewall o IPS.

1.3.1.3. OpenVas

Es una herramienta para el escaneo de puertos e identificación de vulnerabilidades, una herramienta más avanzada que NMAP, donde no solo se reconoce que puertos y software existe en el sistema testeado, sino que cuenta con bases de datos de vulnerabilidades, las cuales le son asociadas, según la información recolectada, cuenta con versión gratis y versión licenciadas, al igual que otras herramientas como NESSUS o NEXPOSE u otras más especializadas como acunetix, deben estar en la biblioteca de todo Pentester.

1.3.2. Servicios en línea

A nivel mundial existen herramientas, sitios web o bases de datos de herramientas para la seguridad informática, estos son ejemplos de ella.

1.3.2.1. ExploitDB

Es una base de datos de herramientas que permiten explotar vulnerabilidades reconocidas, son script, aplicativos y documentación para comprobar si los paquetes reconocidos, realmente son vulnerables. Estos script están disponibles, solo es necesario descargar, compilar o ejecutar.

1.3.2.2. CVE

Es una base de datos de vulnerabilidades, descubiertas, informadas, organizadas, categorizadas y divulgadas, de muchos aplicativos, sistemas operativos y cualquier otro software que se quiera vincular al proyecto. Es mantenido por la misma comunidad con la publicaciones de nuevas vulnerabilidades o por aceptaciones de vulnerabilidades de los fabricantes. Puede ser utilizada por cualquier persona interesada en el tema.

1.4. BANCO DE TRABAJO

Para la desarrollo de la prueba de intrusión se requiere un banco de trabajo para simular o probar los diferentes sistemas informáticos a probar.

1.4.1. Paso A: VirtualBox

Descargar la herramienta virtualizadora “VirtualBox” en su última versión. En la siguiente figura se puede observar la página oficial de descarga de VirtualBox y la ventana de instalación.

Fig. 2. Descarga e instalación última versión VirtualBox

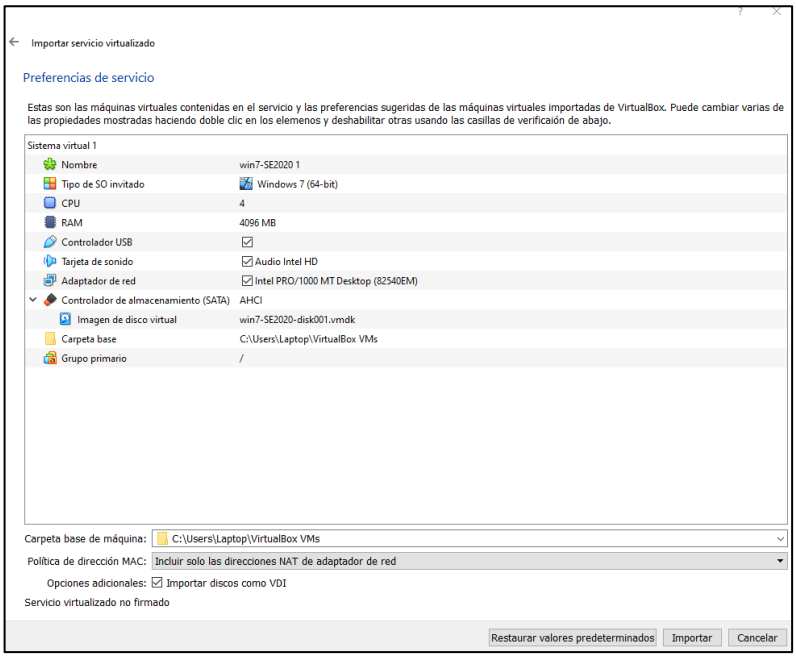
Fuente: Jean Polo Cequeda Olago

1.4.2. Paso B: Montaje del banco de trabajo

Importación de las imágenes en formato .OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico.

La siguiente imagen muestra los parámetros de la maquina Windows 7 que se importó a VirtualBox.

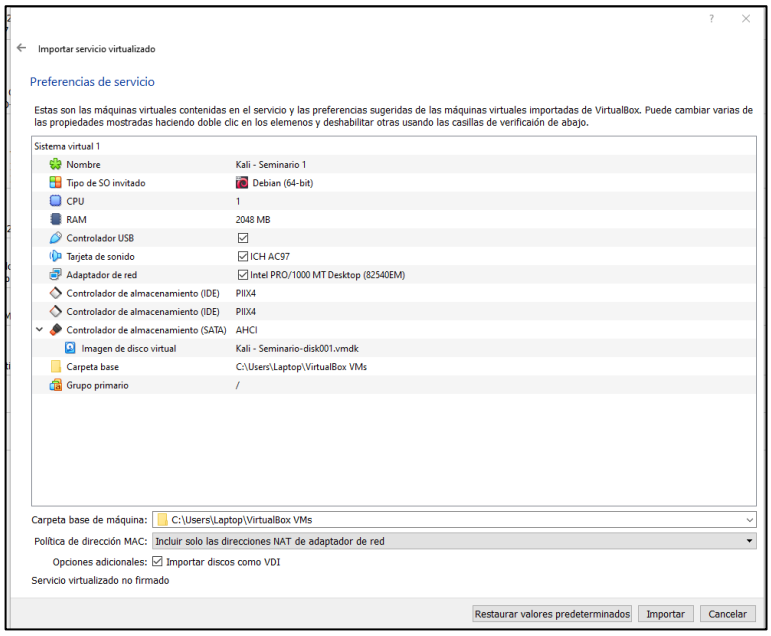
Fig. 3.Importación de máquina virtual Windows 7



Fuente: Jean Polo Cequeda Olago

La siguiente imagen muestra los parámetros de la maquina Kali Linux que se importó a VirtualBox.

Fig. 4. Importación de máquina virtual Kali Linux

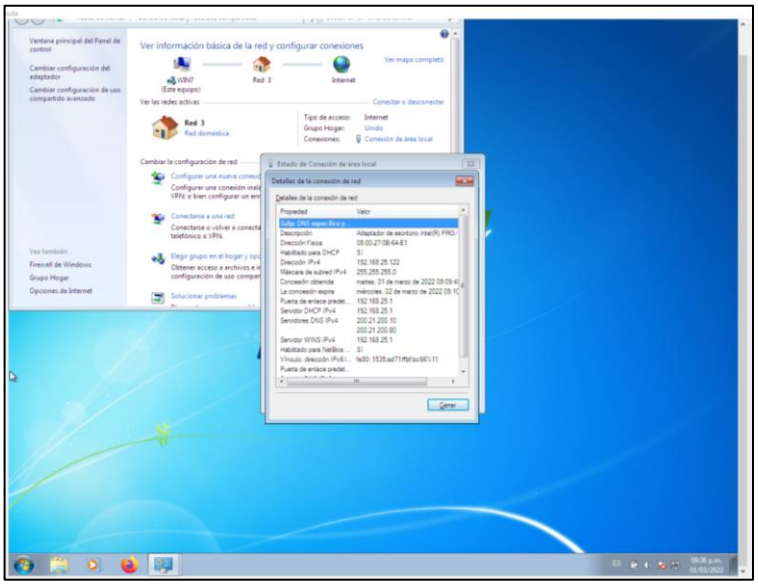


Fuente: Jean Polo Cequeda Olago

1.4.3. Paso C: Validación de la comunicación entre máquinas virtuales.

La siguiente imagen muestra los parámetros de red de la maquina Windows 7, recién importada a VirtualBox y que se tendrán en cuenta para realizar la prueba.

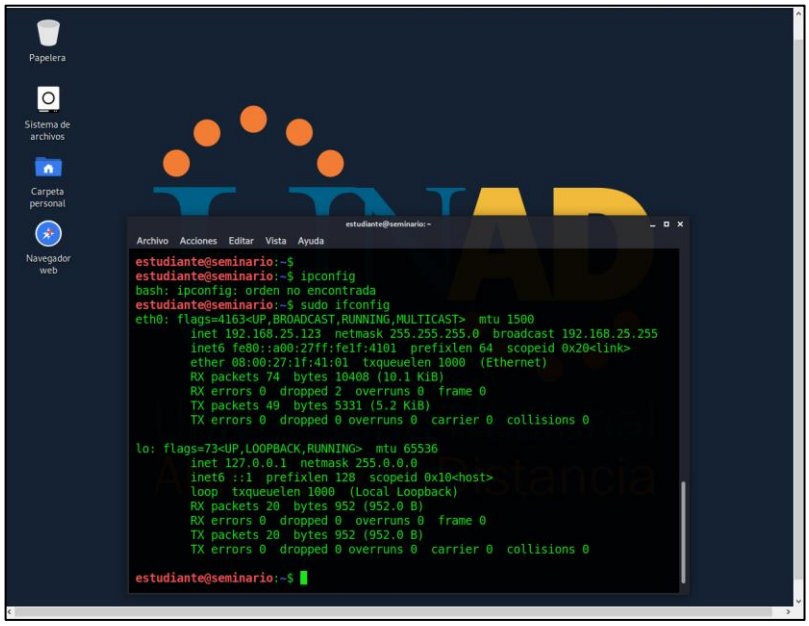
Fig. 5. Dirección IPv4 de máquina virtual Windows 7 - 192.168.25.122



Fuente: Jean Polo Cequeda Olago

La siguiente imagen muestra los parámetros de red de la maquina Windows 7, recién importada a VirtualBox y que se tendrán en cuenta para realizar la prueba.

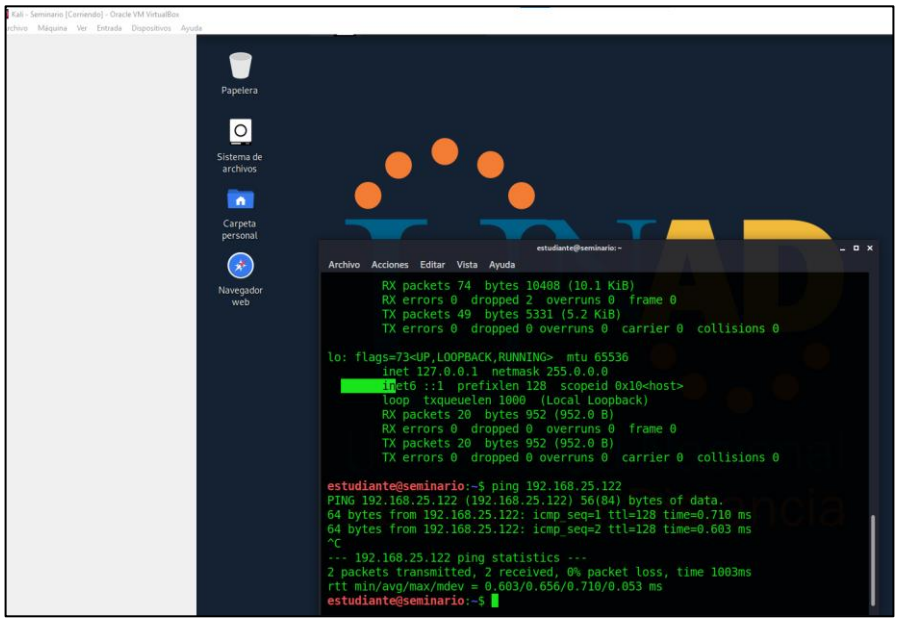
Fig. 6. Dirección IPv4 de máquina virtual Kali Linux – 192.168.25.123



Fuente: Jean Polo Cequeda Olago

En la siguiente imagen se puede evidencia la comunicación entre la maquina Windows 7 y la maquina Kali Linux, siendo este el primer requisito para realizar la prueba.

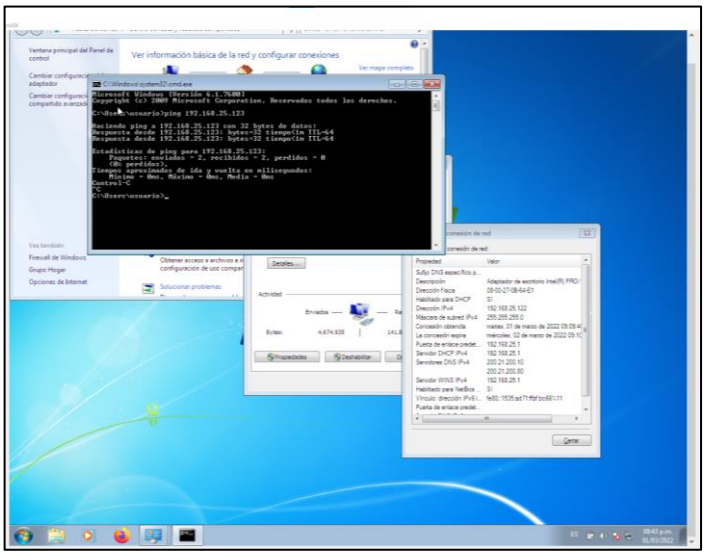
Fig. 7. Prueba de comunicación maquinas Kali Linux a Windows 7



Fuente: Jean Polo Cequeda Olago

En la siguiente imagen se puede evidencia la comunicación entre la maquina Kali Linux y la maquina Windows 7, siendo este el primer requisito para realizar la prueba.

Fig. 8. Prueba de comunicación maquinas Windows 7 a Kali Linux

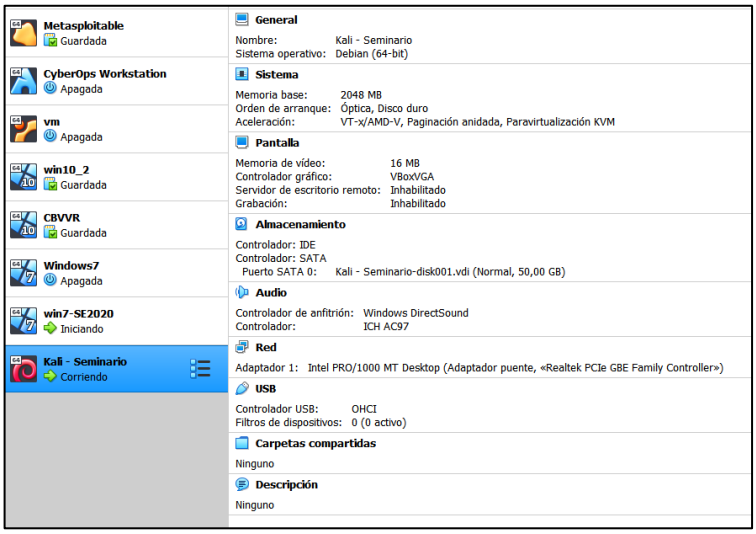


Fuente: Jean Polo Cequeda Olago

1.4.4. Paso D: Características técnicas de hardware

La siguiente imagen muestra las características técnicas del hardware virtualizado para las maquinas importadas, primero la maquina Kali Linux.

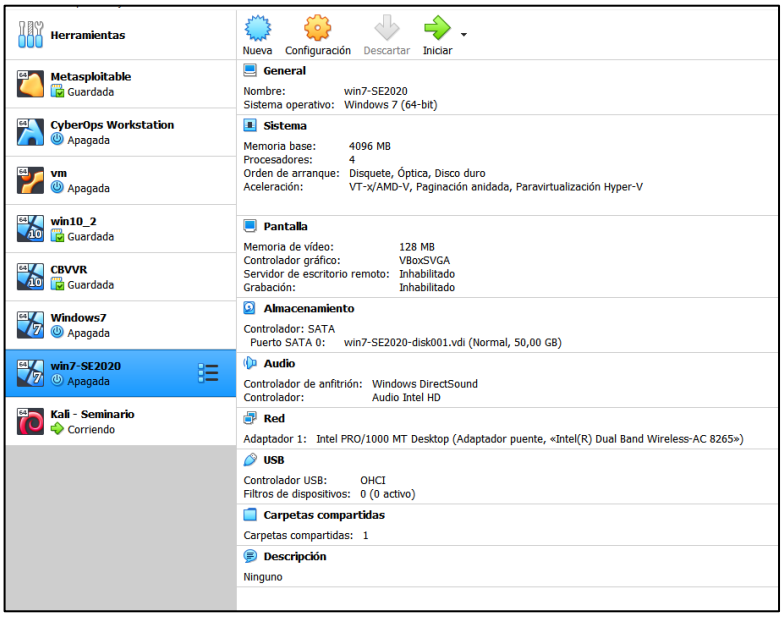
Fig. 9. Características de hardware máquina virtual Kali Linux



Fuente: Jean Polo Cequeda Olago

La siguiente imagen muestra las características técnicas del hardware virtualizado para las maquinas importadas, la maquina Windows 7.

Fig. 10. Características de hardware máquina virtual Windows 7



Fuente: Jean Polo Cequeda Olago

2. SITUACIÓN PROBLEMA

2.1. CONSIDERACIONES

2.1.1. Puntos relevantes a considerar.

- De la situación planteado se puede resaltar los siguientes puntos interesantes:
- El core del negocio de la organización WhiteHouse Security es la ciberseguridad y ciberdefensa
- El objetivo es conformar el Red team, encargado de la identificación de vulnerabilidades y el Blue team encargado de mitigar las vulnerabilidades identificadas.
- El proceso de contratación se apoya en un contrato elaborado por una abogado que le encontraron algunos procesos ilícitos.
- La gerencia entrega como contrato a utilizar un documento poco confiable
- La gerencia no se apoya en un asesor u oficina jurídica para establecer la viabilidad jurídica del documento.
- El proceso de admisión se basa en situaciones problemáticas u incidencias reales identificadas en la organización
- En el proceso de admisión también se requiere un ambiente controlado de pruebas, basado en máquinas virtuales en el hipervisor VirtualBox.

2.1.2 Puntos relevantes a considerar anexo 3

- Existe una clasificación de la información, privada, publica, sensible, etc.
- La información proporcionada es propiedad de la organización
- La utilización de dicha información en el proceso de admisión no elimina la clasificación dada a la información proporcionada
- Existe información confidencial recopilada en procesos ilegales
- Información confidencial: 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”.
- Origen de la información confidencial: Toda aquella suministrada física o digital en el proceso de admisión.
- Mantener confidencial la información proporcionada sea obtenida de manera legal o ilegal, aun cuando pueda constituir un delito.

2.2. Análisis legal

Evidentemente existen una ilegalidad, según las leyes Colombianas, una inducción al error, un acuerdo para delinquir, ya que se está aceptando unas cláusulas que así lo expresan.

2.2.1. Procesos ilegales

La siguiente ilustración es un fragmento del documento de acuerdo de confidencialidad entre el aspirante al cargo y la organización WHITEHOUSE SECURITY. En ella se puede observar el contenido de la primera cláusula que se pretende acepten los aspirantes al cargo durante el proceso de selección. En ella claramente se puede leer que se realizan procesos ilegales, de los cuales se obtiene información confidencial, pero no solo tiene la clasificación de confidencial sino que viene de un proceso viciado por los mecanismos, actividades o desarrollo de procesos ilegales.

Fig. 11. Fragmento documento acuerdo de confidencialidad – Clausula 1

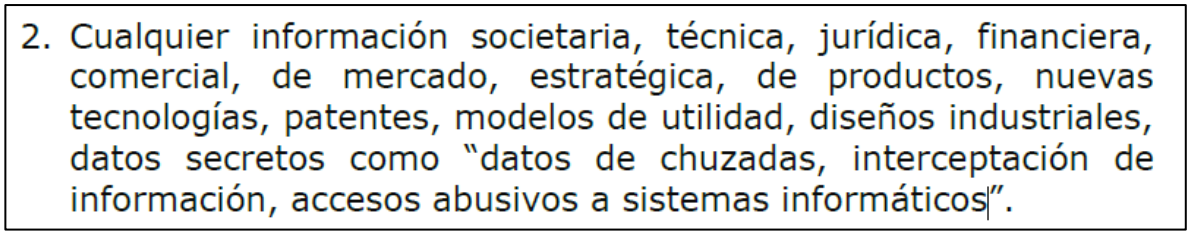
Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con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

Fuente: Anexo 2 – Seminario Seguridad - UNAD

2.2.2. Delitos informáticos

En la siguiente ilustración muestra otro fragmento del documento de acuerdo, en este numeral 2 de la cláusula 2, se puede leer claramente que la información confidencial de la organización y proporcionada por la organización al aspirante, considerados datos secretos, son datos de chuzadas, es decir interceptaciones ilegales y accesos abusivos a sistemas informáticos.

Fig. 12. Fragmento documento acuerdo de confidencialidad – Clausula 2, numeral 2

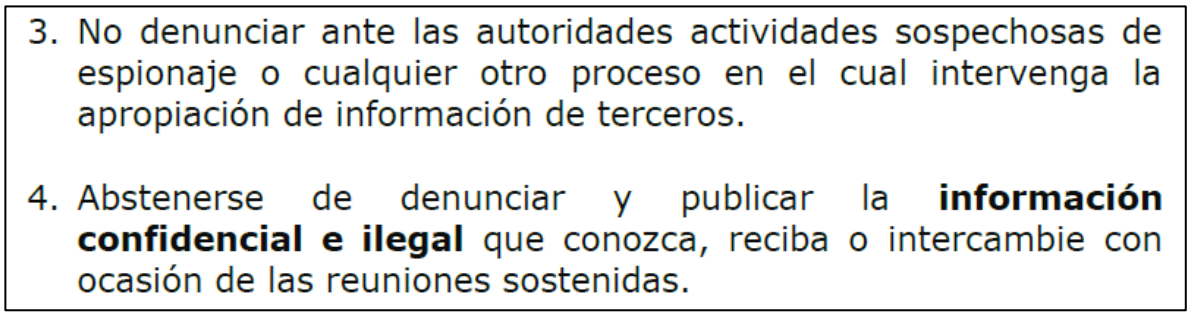


Fuente: Anexo 2 – Seminario Seguridad - UNAD

2.2.3. Deber denunciar

En el siguiente fragmento del acuerdo de confidencialidad proyectado por el ex asesor jurídico de la organización deja una clara falencia e induce a un delito al aspirante en su proceso de selección, ya que en los numerales 3 y 4 de la cláusula 5, requiere que el aspirante se abstenga de denunciar actividades posiblemente delictivas que se realizaron para obtener, posiblemente fuera de la ley, información confidencial o ilegal.

Fig. 13. Fragmento documento acuerdo de confidencialidad – Clausula 5, numeral 3 y 4



Fuente: Anexo 2 – Seminario Seguridad - UNAD

2.2.4. Ley 1273 de 2009 – De la protección de la información y de los datos

La primera ley Colombiana que intenta preservar los sistemas informáticos y la información en el país. En este caso es evidente que existen dos delitos explícitamente definidos. La interceptación de información y accesos abusivos a sistemas informáticos, pero se pueden imputar otros delitos como transferencia no consentida de activos, ya que la información recopilada puede estar siendo no solo

utilizada en las pruebas de admisión sino que la organización se lucra con dicha información.

Los artículos vulnerados de manera explícita son:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS

Estos dos artículos se vulneran cuando en el numeral 2 de la cláusula 2 se habla de datos secretos que provienen de datos de chuzadas, lo cual se reconoce como una interceptación ilegal a algún sistema tecnológico, no autorizada por un juez y no ejecutada por una autoridad competente; los mismo sucede con un acceso no autorizado por el dueño o custodio del activo informático o no ejecutado por una autoridad competente motivada por una orden judicial. Adicionalmente si se habla de espionaje, lo cual indica que no solo hay información comprometida sino que seguramente datos personales, lo cual nos lleva no solo a contemplar los delitos de la ley 1273, sino también de la ley estatutaria 1581.

2.3. Aplicación al cargo.

Los acuerdos de confidencialidad son muy explícitos y se nota que en el desarrollo de las actividades del cargo se tendrán que cometer muchos delitos para lograr el objetivo de la organización. Si fuese institución que sea una autoridad competente para realizar estas operaciones legales, fiscalía, policía, fuerza militares, etc, que motivadas por una orden judicial, dentro de un proceso jurídico, se puede contemplar en participar en el proceso de selección y optar por el cargo. Pero ninguna suma de dinero lo blindará para no ser objeto de una posible investigación.

Por otra parte el código de ética profesional para las ingenierías y profesiones afines, ley 842 de 2003, en el artículo 31. DEBERES GENERALES DE LOS PROFESIONALES, numeral f, define que se deben denunciar delitos, faltas, contravenciones en contra de la profesión de ingeniería, así como el numeral b del articulo 32 PROHIBICIONES GENERALES A LOS PROFESIONALES, tolerar o facilitar la ilegalidad de la profesión.

2.4. Operación ANDROMEDA

Estas operaciones son cada vez más importantes, no es secreto que el reclutamiento de unidades para una ciberdefensa es cada vez más popular, pero ya no es de forma descarada como se hizo en este caso en particular, quizás por la inmadurez de la ley 1273, quizás por el famoso dicho, siempre lo hemos hecho así y nunca paso nada, este es un claro ejemplo de que si algo puede salir mal, sale mal, famosa ley de Murphy.

La operación ANDROMEDA desde el punto de vista del estado, fue una necesidad, una forma más de demostrar que se pueden realizar muchas cosas fuera de la ley argumentando buscar la seguridad de la nación, pero estas instituciones llámese "Comunidad Buggly", Sala gris, Centro de control de operaciones o de contra inteligencia, fracturan gravemente varios derechos fundamentales, pero el problema sigue siendo que se argumentaran cosas, se buscaran otras cortinas de humo y se desmontara esa estructura que siembre ha estado acostumbrados a montar para buscar "proteger" la nación pero que en casos transcienden a objetivos personales o interés políticos.

La ley es muy clara, se debe siempre llevar el debido proceso, todo bajo la constitución y las diferentes leyes que el honorable congreso, el poder legislativo, le proporcionan, al poder judicial, pero todas estas estructuras son formadas por seres humanos con necesidades y problemas, con valores y sin ellos, finalmente termina en algunos casos en satisfacción los interés particulares y de algún sector de la clase política.

Esta operación, esta fachada operativa, de manera descarada demostró a la sociedad Colombiana que algunos individuos de las diferentes instituciones que deben velar por los derechos de los Colombianos, terminan vulnerando esos derechos, la Intimidad, libre desarrollo de personalidad, entre muchos otros, incluso derecho a la vida, empiezan o empezaros a quebrarse desde estas oficinas.

Los únicos facultados para autorizar acciones que se pueden tipificar como delitos o faltas a los códigos de ética son los jueces de la república, dentro de un proceso judicial, civil o penal, ejecutado por una autoridad competente; cualquier actuación fuera de este contexto es y deberá ser castigado

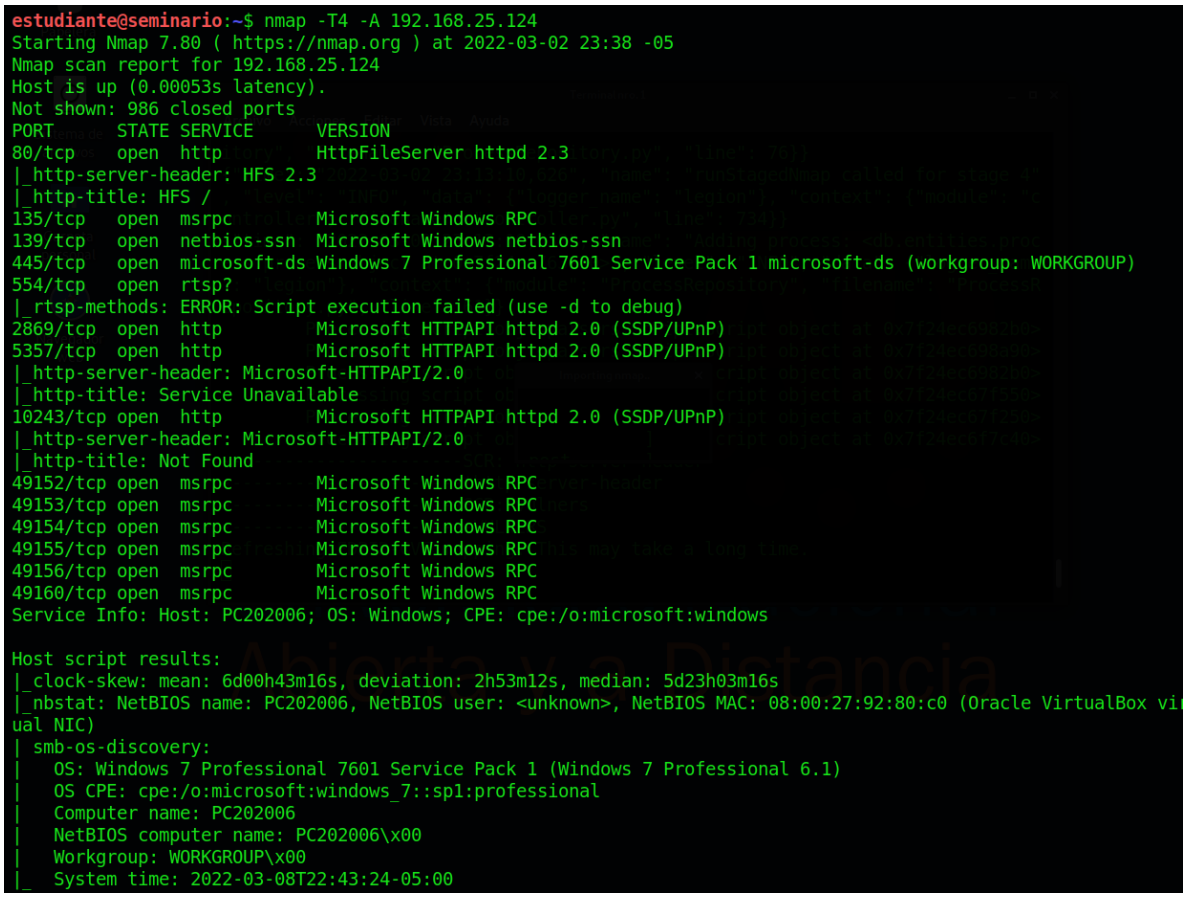
3. VULNERABILIDADES

3.1. Descripción de herramientas

La principal herramienta es la distribución Kali Linux, especializada en la realización de pruebas de intrusión, su compendio de herramientas, permite realizar más fácilmente la prueba de intrusión.

A continuación de muestra el escaneo con NMAP a la maquina víctima.

Fig. 14. Listado de puertos abierto en la maquina Windows 7 de 64bits reconocidos por NMAP

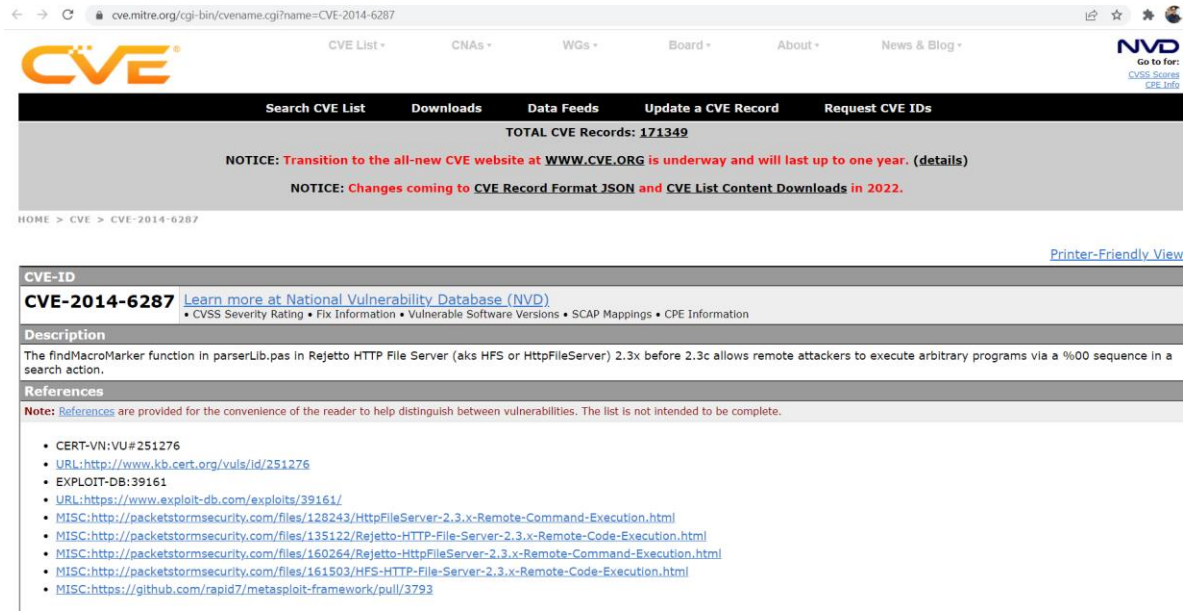


Fuente: Jean Polo Cequeda Olago

3.2. Fallo de seguridad

Esta versión de Rejjeto V.2.3 presenta la vulnerabilidad CVE-2014-6287 la cual permite ejecutar código remoto, abriendo una interface de línea de comandos en la victima.

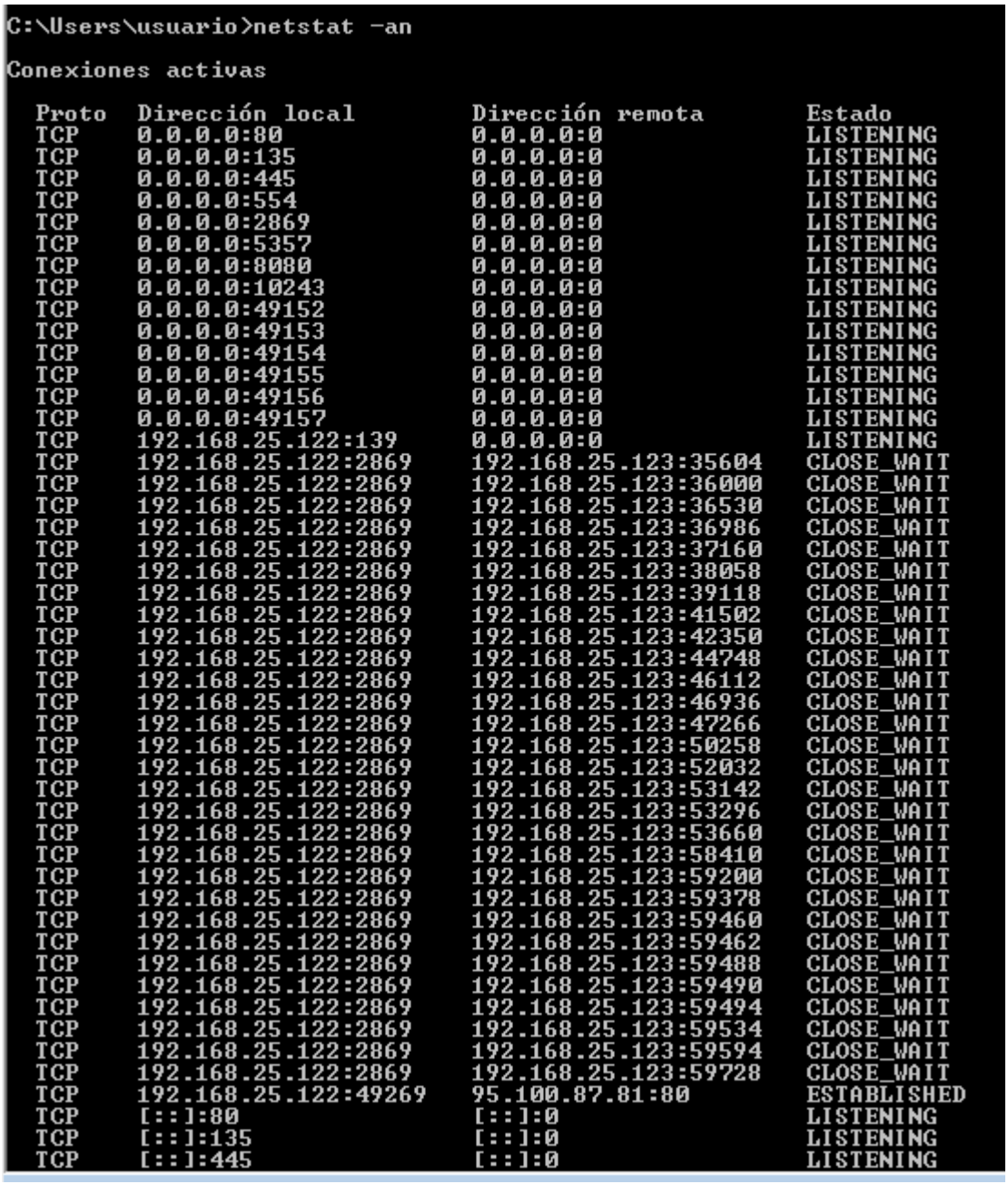
Fig. 15. Listado de vulnerabilidades Rejjeto v2.3



Fuente: Jean Polo Cequeda Olago

3.3. Herramientas

Para identificar el fallo se utiliza primero que todo NMAP para identificar los puertos y los paquetes informáticos que están corriendo en esa máquina. El puerto que abre en la maquina Windows 7 de 32 bits es el puerto 8080 ya que el puerto 80 está ocupado. En la maquina Windows 7 de 64 bits abre el puerto 80 ya que esta libre. Tal como se puede observar en la siguiente imagen.



```
C:\Users\usuario>netstat -an

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    192.168.25.122:139     0.0.0.0:0              LISTENING
  TCP    192.168.25.122:2869    192.168.25.123:35604   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:36000   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:36530   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:36986   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:37160   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:38058   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:39118   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:41502   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:42350   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:44748   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:46112   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:46936   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:47266   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:50258   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:52032   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:53142   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:53296   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:53660   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:58410   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59200   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59378   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59460   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59462   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59488   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59490   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59494   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59534   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59594   CLOSE_WAIT
  TCP    192.168.25.122:2869    192.168.25.123:59728   CLOSE_WAIT
  TCP    192.168.25.122:49269   95.100.87.81:80        ESTABLISHED
  TCP    [::]:80                [::]:0                 LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
```

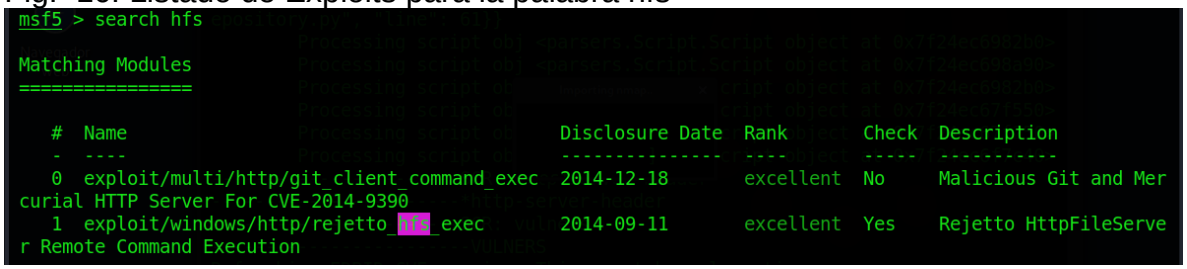
Fuente: Jean Polo Cequeda Olago

3.4. Explotación

La vulnerabilidad explotada debería darle acceso completo, decir poder ejecutar comandos en el servidor, en esta caso lograr administrar los usuarios de este sistema operativo.

La siguiente imagen muestra el exploit que MetaSploit tiene para el software Rejetto versión 2.3 desde el año 2014.

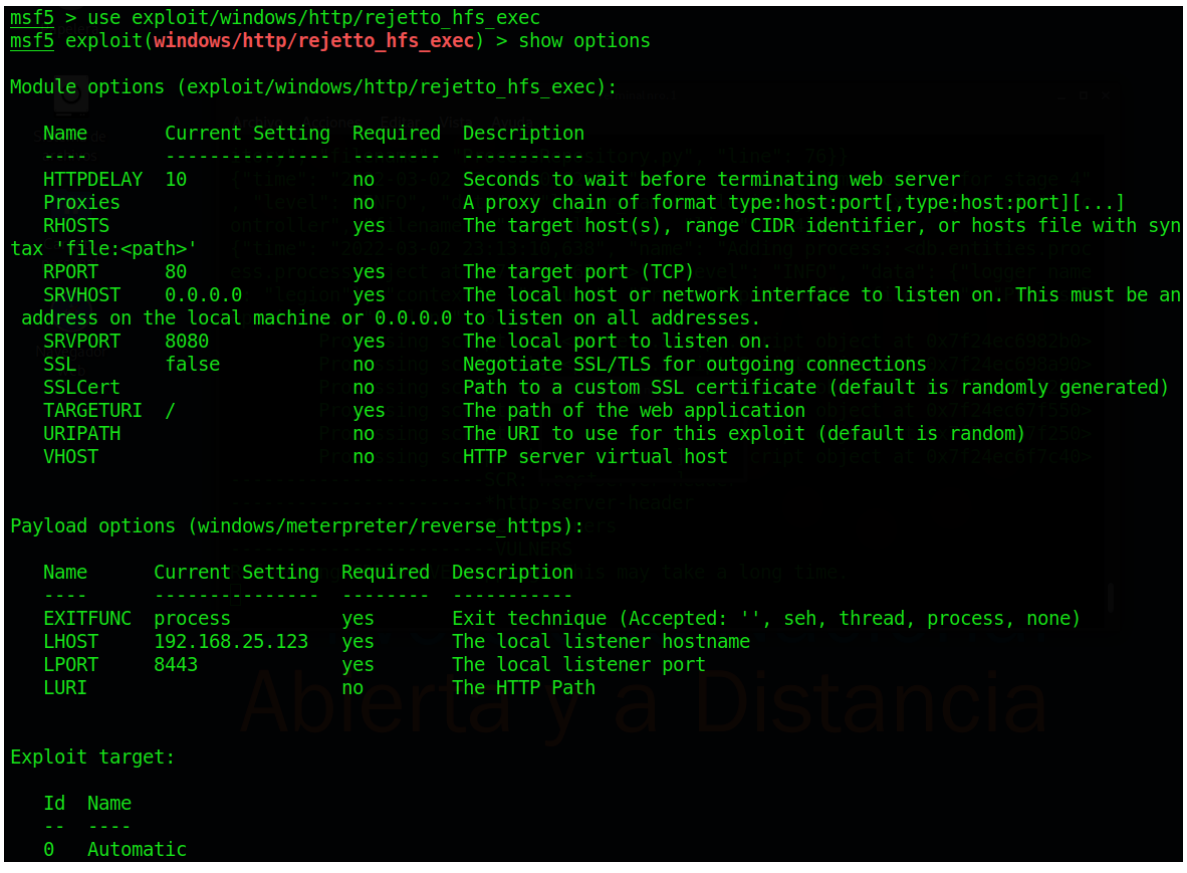
Fig. 16. Listado de Exploits para la palabra hfs



Fuente: Jean Polo Cequeda Olago

Para usar un exploit se requieren unos datos, como la dirección o URL de la víctima, el número de puerto utilizado y otras opciones que finiquitan el poder realizar la explotación; la siguiente imagen muestra dichas opciones, de las cuales se denota RHOSTS que es la variable donde se define la IP de la víctima.

Fig. 17. Listado de opciones del Exploit para Rejjeto

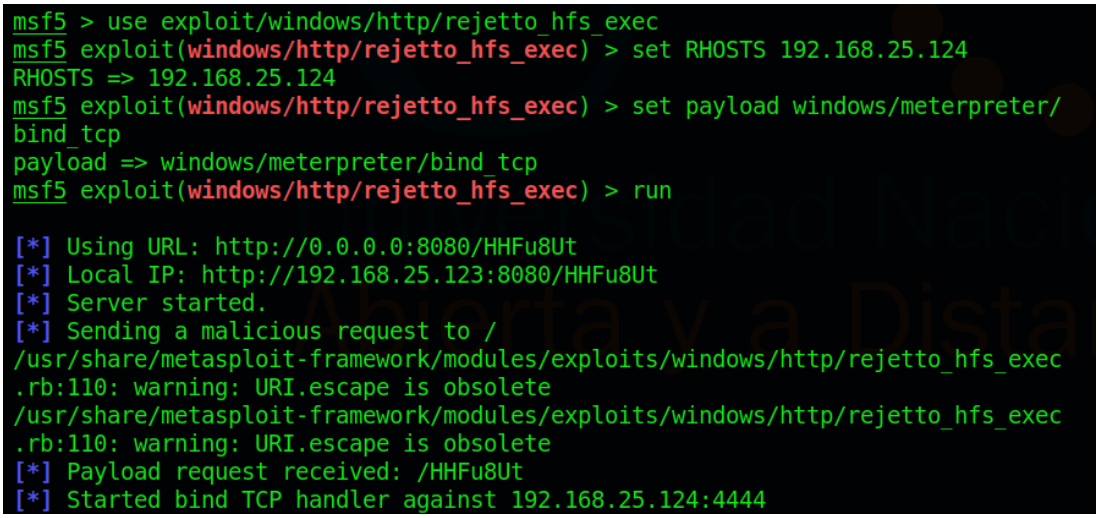


Fuente: Jean Polo Cequeda Olago

Para usar el exploit que consideramos se pueda aplicar a la vulnerabilidad encontrada, se utiliza el comando use, seguido de la ruta donde está el exploit, tal

como se observa en la siguiente figura. Luego de seleccionado el exploit se debe definir el RHOSTS y el payload que se intentará utilizar, en este caso una puerta trasera con meterprer, definidas estas dos opciones, el comando run inicia el exploit, como se observa en la figura.

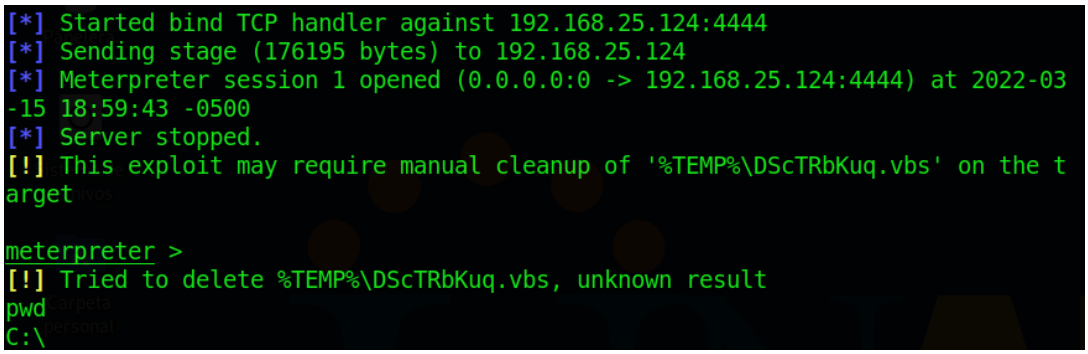
Fig. 18. Ejecución del exploit rejetto



Fuente: Jean Polo Cequeda Olago

El exitoso proceso de explotación permite abrir una puerta trasera para ejecutar comandos en el sistema víctima, en este caso se requiere verificar si se puede crear usuarios con los más altos privilegios posibles tal como se observa en la siguiente figura.

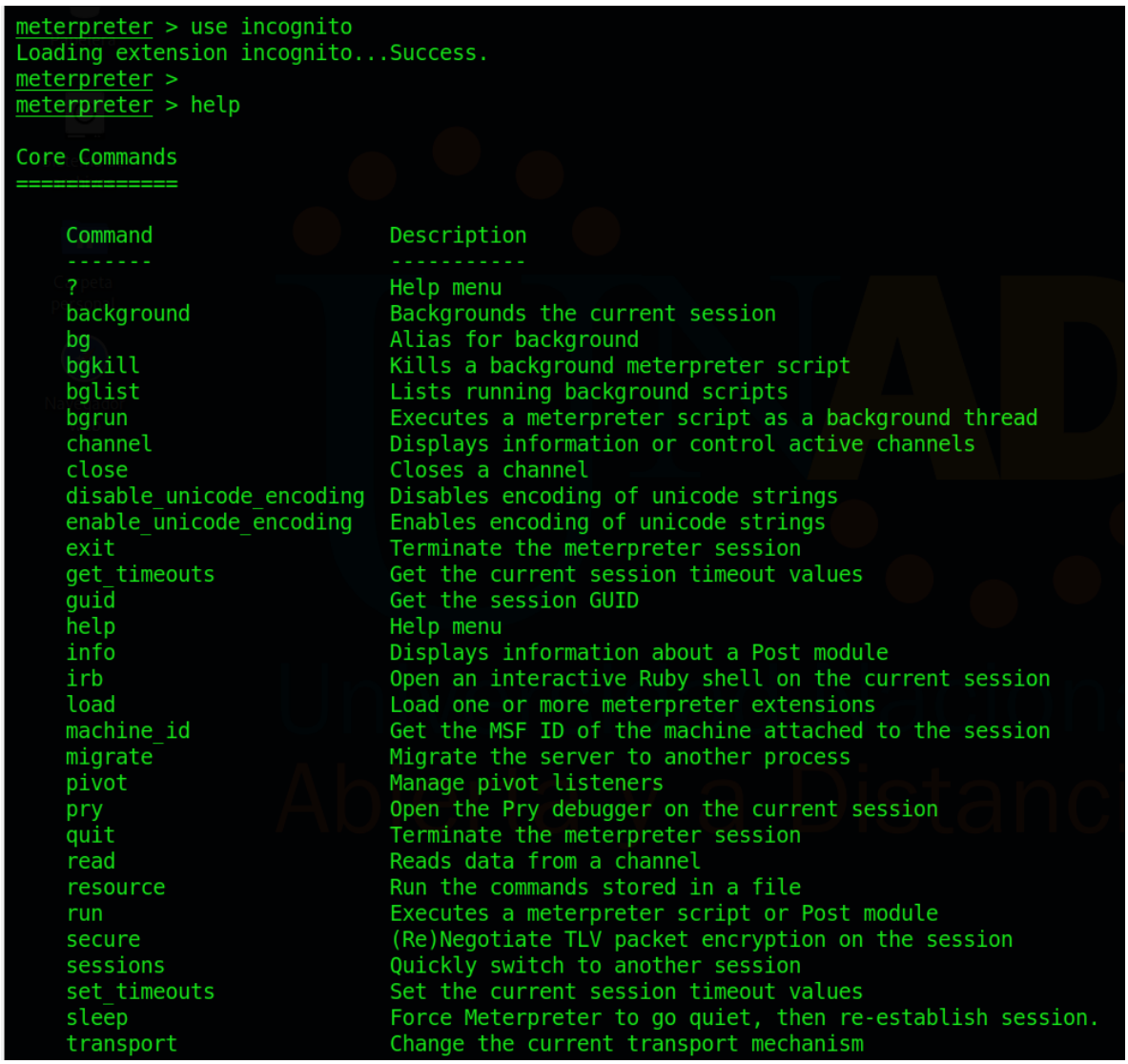
Fig. 19. Resultado exitoso de ejecución del exploit y cargue del payload



Fuente: Jean Polo Cequeda Olago

El payload meterpreter tiene una serie de opciones que se puede ejecutar en el sistema vulnerado, incluso puede ejecutar plugins para realizar instrucciones un poco más elaboradas y de forma sencilla, tal como se observa en la siguiente imagen.

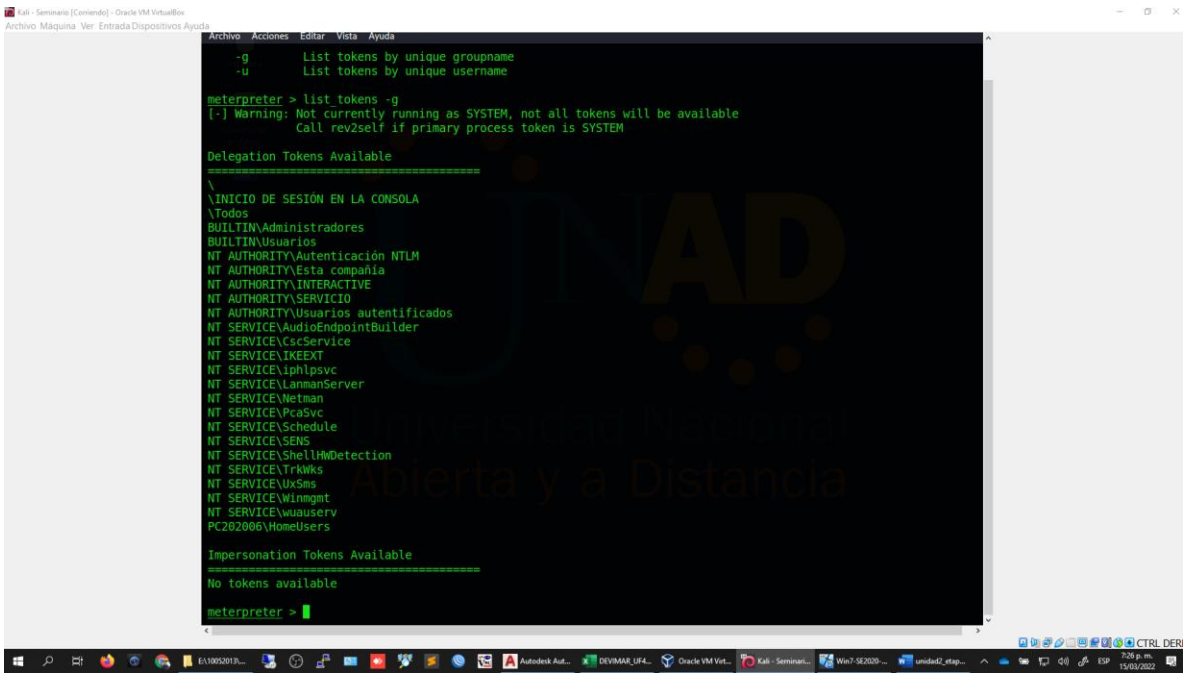
Fig. 20. Listado de comandos del payload Meterpreter



Fuente: Jean Polo Cequeda Olago

El uso del plugin incognito de meterpreter permite listar los grupos existentes en la maquina víctima, tal como se observa en la siguiente imagen.

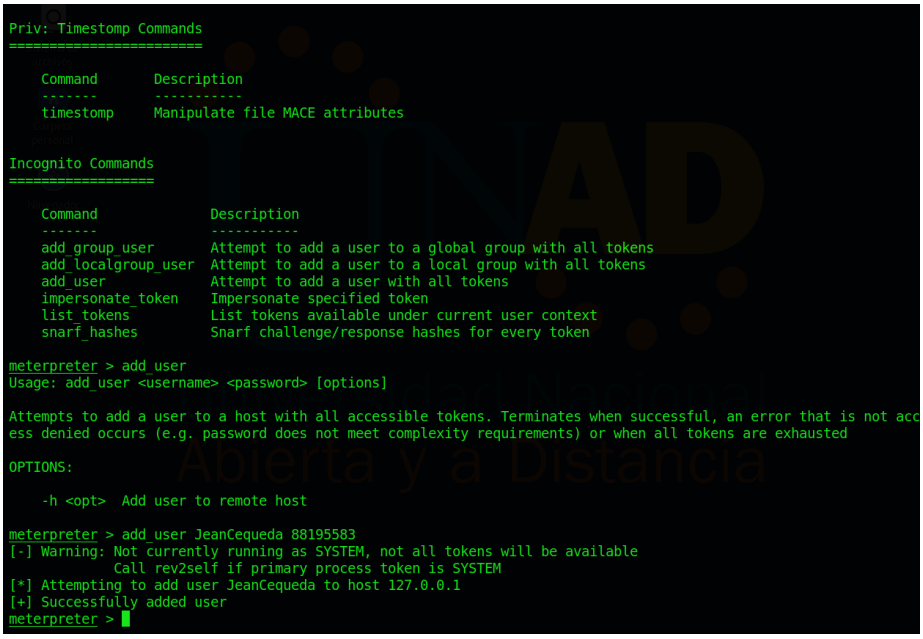
Fig. 21. Listado de grupos en el sistema operativo victima



Fuente: Jean Polo Cequeda Olago

En la siguiente imagen se evidencia que se puede agregar un usuario en el sistema operativo victima mediante el comando add_user, dándole un nombre y un password.

Fig. 22. Creación de usuario en el sistema operativo victima



Fuente: Jean Polo Cequeda Olago

Luego de agregar un usuario al sistema víctima se puede asignar ese usuario a un grupo, en este caso, al grupo de administradores, para tener todos los privilegios que pueda tener este nuevo usuario, tal como se evidencia en la siguiente imagen.

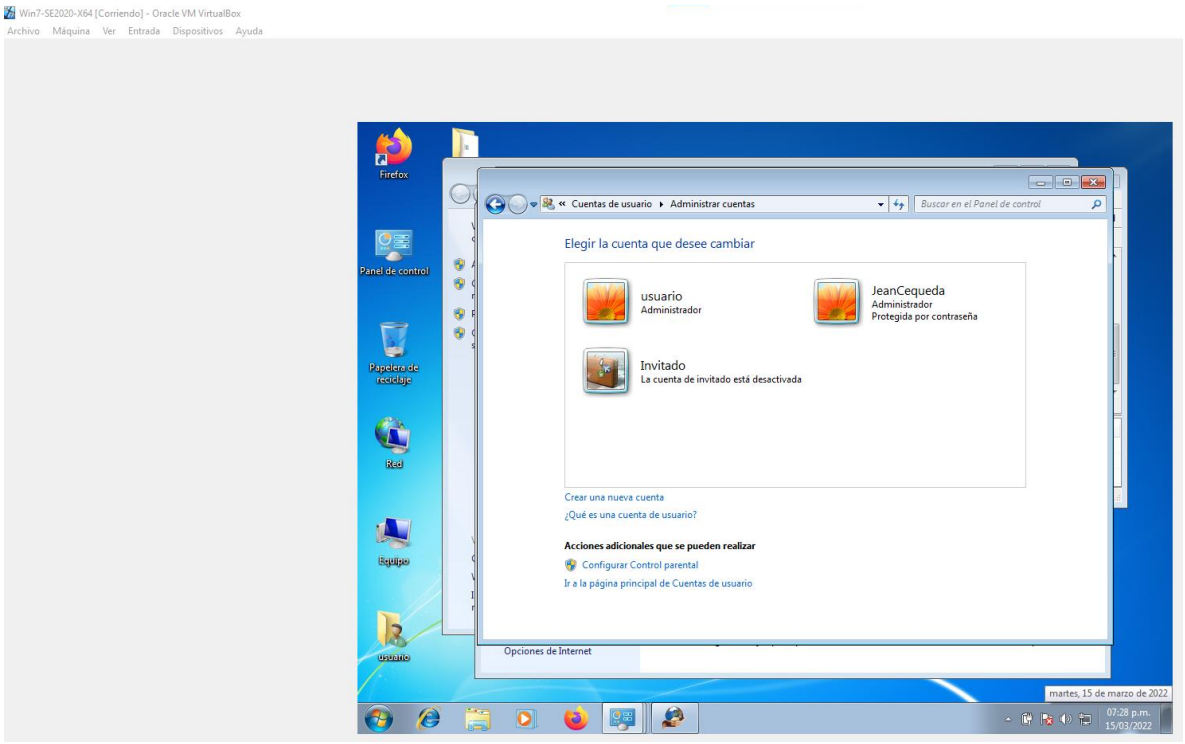
Fig. 23. Asignación del usuario creado al grupo administradores

```
meterpreter > add_localgroup_user "Administradores" "JeanCequeda"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[*] Attempting to add user JeanCequeda to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
meterpreter >
```

Fuente: Jean Polo Cequeda Olago

La siguiente imagen muestra la evidencia del usuario creado mediante la explotación de la vulnerabilidad rejetto versión 2.3 y con la ayuda del payload meterpreter como puerta trasera.

Fig. 24. Listado de usuarios en Windows 7 vulnerado



Fuente: Jean Polo Cequeda Olago

4. RESPUESTA A INCIDENTES

4.1. Respuesta ante incidente

Ante un incidente lo primero que se debe hacer es aplicar los procedimientos establecidos, es decir, si la empresa u organización tiene definido como actuar ante situaciones que se pudiesen presentar y la actual situación estuviese entre esas posibles situaciones contempladas, se debe aplicar dicho procedimiento. Si por el contrario, no se contempló esta situación y mucho menos se estableció el proceder se debe actuar con cautela y definitivamente la experiencia del administrador es crucial, ya que una mala acción puede generar un impacto negativo más grande que el mismo ataque.

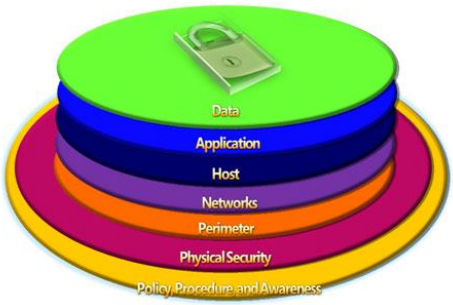
Normalmente los ataques informáticos alteran el normal funcionamiento de los sistemas que intentan afectar, es muy importante conocer el funcionamiento normal de la infraestructura, en días normales o en días especiales, es decir es importante establecer la línea base de la infraestructura, para poder comparar en un determinado momento contra esta línea base y concluir si hay o no alguna alteración en el normal funcionamiento; Hoy en día, incluso para pequeñas infraestructuras, son muchos los factores a considerar, anchos de banda, carga de CPU, utilización de memoria, entre otros muchos, y esto multiplicado por la cantidad de puertos, servidores, estaciones, etc. Convirtiéndose en procesos engorrosos y de nunca terminar, pero existen herramientas que ayudan en este proceso, pueden contemplar muchos factores, de muchos sistemas, por largos periodos de tiempo, algunos son más complejos, otros más fáciles de gestionar, hay con licencias privadas y otras software libre. Estos sistemas de monitoreo, no solo establecen la línea base de funcionamiento de los dispositivos monitoreados, sino que permiten el establecimiento de alarmas y notificaciones ante situaciones que pueden ser consideradas incidentes cuando sobre pasen o umbrales máximos o mínimos.

Como primer respondiente, ante la falta de equipo de respuesta a incidentes, ante la falta de procedimientos, ante la falta de alarmas tempranas y dándome cuenta de que se está accediendo al servidor con privilegios escalados de un superadministrador y pudiéndose estar fugando información importante, lo primero seria aislar el server del resto de la red, desconectado el cable de red. Si no hay información importante, se debe considerar que desde este sistema informático se puede estar accediendo a otros sistemas, de acuerdo a las relaciones de confianza que tenga, lo cual también llevaría a una desconexión de la red. Se debería realizar un proceso forense sobre el servidor e intentar recolectar la mayor cantidad de evidencia, para procesos legales y más importante aún, aprender del incidente para evitar que vuelva a suceder.

4.2. Hardening

El proceso de endurecimiento de sistemas informáticos pretende desmotivar a un atacante de lograr un incidente informático. Un esquema de defensa en profundidad, como se ve en la siguiente figura, siempre ha dado buenos resultados, cada capa, en diferentes niveles, ofrece controles para contrarrestar los ataques.

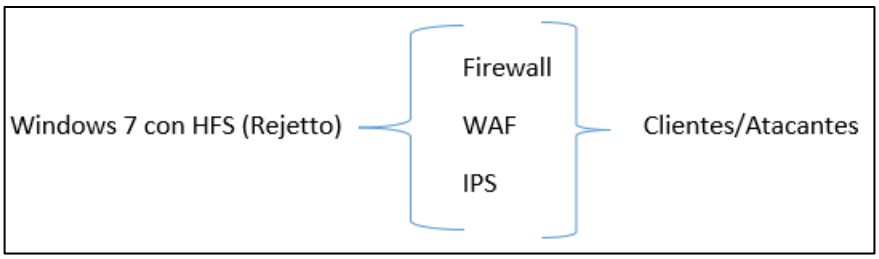
Fig. 25. Modelo de defensa en profundidad



Fuente: https://guardnet.wordpress.com

Como primera medida se puede considerar la actualización del software a la última versión, incluso en el cambio del paquete utilizado si es posible o quitar ese software si no se requiere. Se puede considerar activar y configurar el firewall de Windows para permitir la conexión solo desde los clientes de confianza, si es posible delimitarlos; Se puede pensar en implementar un WAF opensource en otra máquina, ModSecurity, IronBee, NASXI, entre otros para que valide las conexiones, permitiendo o no cierto tipo de conexiones o peticiones; se puede considerar implementar un sistema de prevención de intrusiones en otra máquina, SNORT, CrowdSec, etc, para intentar prevenir que se conexiones o peticiones sospechosas se puedan establecer, estas dos últimas alternativas, WAF e IPS requieren complementarse con creación de VLAN o segmentación de la maquina con HFS (Rejetto) para evitar el acceso directo.

Fig. 26. Esquema herramientas hardening - Windows 7 rejetto



Fuente: Jean Polo Cequeda Olago

4.3. Equipo de respuesta a incidentes vs Blueteam

La diferencia radica en que el equipo BlueTeam actúa para prevenir, busca alternativas para evitar o mitigar los incidentes, es decir la seguridad defensiva, mientras que el equipo de respuesta a incidentes se contempla para actuar cuando ya sucede el incidente, pero la realidad es que el equipo BlueTeam, RedTeam e incluso se habla de PurpleTeam, YellowTeam, OrangeTeam y GreenTeam, todos aportando a la seguridad informática de la organización.

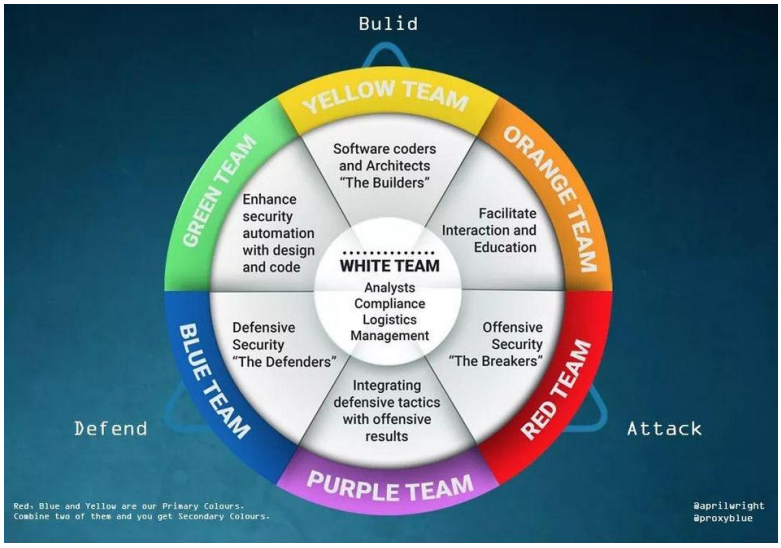
Tabla 1. Listado equipos de seguridad informática

Equipo	Descripción
Red	Seguridad Ofensiva, utiliza herramientas, emular ataques, explota vulnerabilidades.
Blue	Seguridad Defensiva, Mejora continua.
Yellow	Construye herramientas y procesos para mejorar los equipos Blue y Red
Purple	Apoyo a BlueTeam con conocimientos de atacantes desde RedTeam y viceversa.
Orange	Apoyo por parte de RedTeam a YellowTeam para la construcción de herramientas y procesos
Green	Apoyo por parte de BlueTeam a YellowTeam para la construcción de herramientas y procesos

Fuente: Jean Polo Cequeda Olago

La siguiente figura muestra el modelos de equipos por colores y con diferentes responsabilidades por parte de InfoSec

Fig. 27. Equipos de respuesta a incidentes



Fuente: InfoSec

4.4. Center For Internet Security - CIS

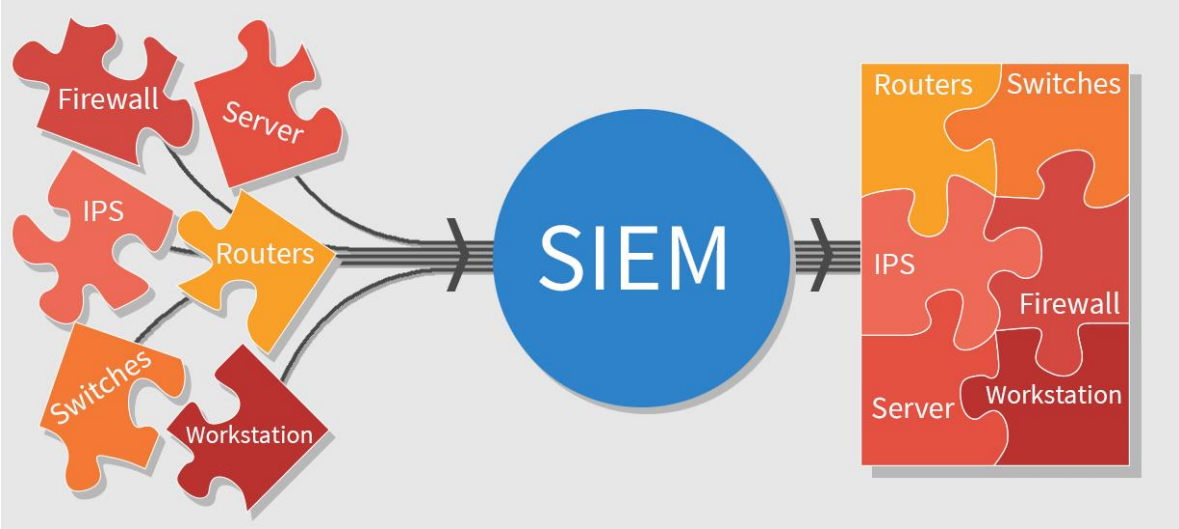
El CIS por sus siglas en Ingles, es una organización si ánimo de lucro que tiene como misión velar por un internet más seguro, desarrollando, validando y promocionando mejores prácticas de seguridad informática. El aplicar las mejores prácticas y controles de seguridad de CIS le permite ganar la experiencia de la comunidad que hace parte de CIS. Se pueden implementar controles básicos como gestión continua de vulnerabilidades, configuración segura de servidores, gestión de logs, entre otros; controles fundamentales como control de puertos, configuración segura, protección perimetral; controles organizacionales como gestión de incidentes, pruebas de penetración y de equipo rojo, entre otros.

4.5. SIEM

Los Security Information and Event Management – SIEM, son los sistemas informáticos que permiten gestionar rápidamente los incidentes de seguridad, permite analizar, identificar, calificar, determinar, cuantificar y más acciones sobre la información que se obtiene de múltiples herramientas de seguridad, por ejemplo los logs, brindando una visión integral de los eventos de una infraestructura computacional.

Como se observa en la siguiente figura, el SIEM organizar, toda la información que múltiples dispositivos puedan generar, permitiéndole al equipo de gestión y de respuesta a incidentes a reaccionar más rápidamente. Finalmente SIEM facilita la gestión de incidentes.

Fig. 28. Información de seguridad y gestión de eventos.



Fuente: https://www.ifixed.cl

Como características relevantes, los SIEM, puede determinar amenazas reales de falsos positivos, centraliza la monitorización de todas las amenazas, designa los incidentes al personal correspondiente, aporta la experiencia para resolver más rápidamente eventos recurrentes o similares, documenta cada incidente para futuras consultas, cumple la legislación de datos personales.

4.6. Herramientas de contención

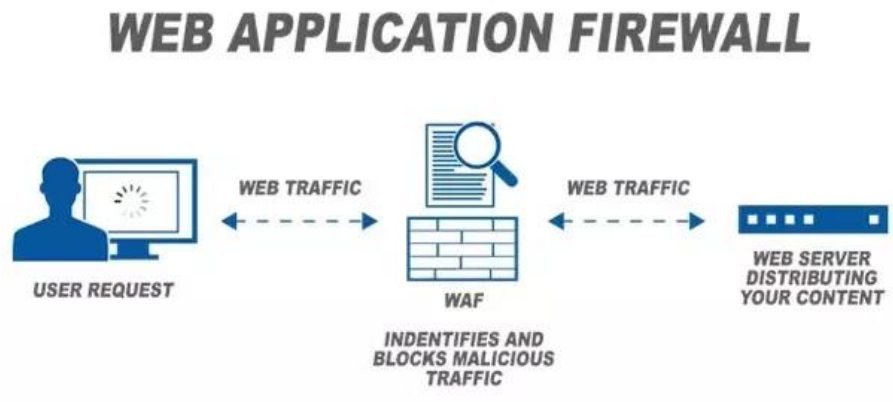
4.6.1. IPS

El sistema de Prevención de Intrusiones, intenta prevenir que se materialicen amenazas, que se exploten vulnerabilidades, que se tomen decisiones de mitigación si existe un comportamiento anormal. Un claro ejemplo de IPS es SNORT, esta herramienta nació como IDS, un sistema de solo detección pero evoluciono, permite la aplicaciones de reglas para intentar mitigar el impacto.

4.6.2. WAF

Los cortafuegos de aplicaciones web, son herramientas especializadas en servicios web, es decir, filtra, aplica restricciones, determinar la amenaza que puede darse mediante una petición al servidor web que se quiere proteger. La siguiente imagen muestra el rol de intermediario que tiene el WAF entre el servidor web y el cliente, toda petición que intente llegar al servidor es analizada por el WAF, según sus reglas, permitirá o no que la petición llegue al servidor web.

Fig. 29. Esquema WAF



Fuente: https://blogs.ugr.es/seguridadinformatica

4.6.3. UTM

La Gestión unificada de amenazas o en ingles Unified Threat Management, son sistema informáticos que cuentan con múltiples herramientas para intentar prevenir, detectar y contener ataques informáticos. Tiene funciones como el filtrado de tráfico, inspección de paquetes, establecimiento de VPN, antispam, antiphishing, antispyware, filtrado de contenidos, antivirus, IDS, IPS, entre otras. Sus funcionalidades se aplican en casi todas las capas del modelo OSI/ISO. Estas herramientas permiten de manera unificada, en una sola consola, aplicar múltiples políticas y controles, permitiendo tener más control de la comunicaciones. Endian es una alternativa opensource o también licenciada de UTM, su gestión es muy sencilla y su confiabilidad muy alta.

CONCLUSIONES

Se debe considerar las implicaciones legales ante la firma o prestamos de servicios profesionales, las altas remuneraciones no lo eximen de la responsabilidad civil y penal de su actuar.

Las actividades profesionales desarrolladas en los quehaceres diarios para cumplir con sus funciones contratadas no pueden ir en contra de la legislación nacional.

No se puede disfrazar delitos, en desarrollo de actividades en contratos laborales.

Los jueces de la república pueden facultar a autoridades competentes en realizar actividades que sin orden judicial se pueden tipificar como delito.

El primer respondiente ante un incidente informático debe considerar que una mal procedimiento puede impactar más negativamente el sistema afectado que el mismo ataque.

Se deben establecer procedimientos para actuar ante cualquier escenario posible que genere un incidente informático.

El proceso de endurecimiento del sistema informático se debe realizar antes de poner en producción y periódicamente se debe realizar pruebas de intrusión sobre dicho sistema.

El modelo de defensa en profundidad permite aplicar múltiples controles sobre un activo para intentar desmotivar al atacante.

Un equipo de respuesta a incidentes es el producto de la sinergia que los equipos Blue, Red y Yellow, el intercambio de conocimientos genera equipos como el Orange, Green y Purple. La comunicación es muy importante.

Existen organizaciones sin ánimo de lucro que consolidan el conocimiento sobre seguridad informática en pro de Internet.

Los SIEM son herramientas que por el alto volumen de información de gestión e incidencias cada día aumento su importancia.

Existen múltiples herramientas para intentar prevenir, detectar y mitigar ataques informáticos, su implementación es indispensables.

En Colombia existe legislación para proteger los activos informáticos, pero se requiere más reglamentación y hacerla cumplir.

Las pruebas de intrusión son una de las herramientas más importantes para un buen funcionamiento de la seguridad informática de una empresa u organización, se cuentan con muchas herramientas pero la experticia del pentester es crucial.

Un entorno controlado es idea para el aprendizaje de pruebas de intrusión.

Se debe considerar las implicaciones legales ante la firma o prestamos de servicios profesionales, las altas remuneraciones no lo eximen de la responsabilidad civil y penal de su actuar.

Las actividades profesionales desarrolladas en los quehaceres diarios para cumplir con sus funciones contratadas no pueden ir en contra de la legislación nacional.

No se puede disfrazar delitos, en desarrollo de actividades en contratos laborales.

Los jueces de la república pueden facultar a autoridades competentes en realizar actividades que sin orden judicial se pueden tipificar como delito.

RECOMENDACIONES

Leer y comprender cada una de las cláusulas escritas en los contratos para prestar servicios profesionales, ningún contrato está por encima de la ley Colombiana.

Se debe conocer la legislación aplicable a la profesión, no conocerla no lo exime de responsabilidades.

Todo sistema informático debe someterse a un proceso de endurecimiento, contemplando múltiples controles para desmotivar a los atacantes.

Toda organización con infraestructura computacional debe considerar el establecimiento de equipos para respuesta a incidentes, si no posible por costos, se puede considerar la contratación por servicios externos.

Se debe considerar la implementación de herramientas que faciliten las actividades de monitoreo y gestión de la seguridad.

BIBLIOGRAFÍA.

Informática Jurídica. (2022). Legislación Informática de Colombia. https://www.informatica-juridica.com/legislacion/colombia

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://www.informatica-juridica.com/legislacion/colombia/

NMAP. (2022). Description. https://nmap.org/

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

IBM. (2022). Why is SIEM important? https://www.ibm.com/topics/siem

NIST. (2022). ¿Qué es SIEM en seguridad informática? Alcance e implementación. https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Blog Jorge Hurtado, Global CTO at Cipher (2019). Beyond the Red and The Blue: Meet the "Rainbow Team" https://www.linkedin.com/pulse/beyond-red-blue-meet-rainbow-team-jorge-hurtado

SQA Consulting (2020). InfoSec Colour Team Structure. https://sqa-consulting.com/infosec-colour-team-structure

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de

seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Policía. (2009). Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4).

https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3npara-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

URL VIDEO SUSTENTACIÓN

https://youtu.be/qHgRGrOkg_Y