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

FABIÁN DAVID CONTRERAS HERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ
2022

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

FABIÁN DAVID CONTRERAS HERNÁNDEZ

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

NOMBRE
LUIS FERNANDO ZAMBRANO HERNÄNDEZ
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ
2022

CONTENIDO

Pág.

RESUMEN
GLOSARIO
INTRODUCCIÓN 9
1 OBJETIVOS 10
1.1 OBJETIVO GENERAL 10
1.2 OBJETIVOS ESPECÍFICOS 10
2 DESARROLLO DE LA ACTIVIDAD 11
2.1 CONCEPTOS Y EQUIPOS DE SEGURIDAD 11
2.1.1 DENTRO DEL MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES QUE LEYES EXISTEN 11
2.1.2 DEFINIR CADA UNA DE LAS ETAPAS DEL PENTESTING 13
2.1.3 HERRAMIENTAS DE CIBERSEGURIDAD 14
2.1.4 BANCO DE TRABAJO 16
2.2 ACTUACION ÉTICA Y LEGAL 22
2.2.1 EVIDENCIAR PROCESOS ILEGALES Y NO ETICOS 22
2.2.2 USTED COMO EXPERTO EN CIBERSEGURIDAD APLICARÍA A ESTE TRABAJO 24
2.2.3 OPERACIÓN ANDROMEDA BUGGLY 24
2.3 EJECUCIÓN PRUEBAS DE INTRUSIÓN 25
2.3.1 HERRAMIENTAS DE SOFTWARE UTILIZADAS 25
2.3.1.1 Nmap 25
2.3.1.2 Metasploit 29
2.3.2 DATOS DEL ANEXO QUE APOYARON LA IDENTIFICACIÓN DEL FALLO DE SEGURIDAD 35
2.3.3 HERRAMIENTAS UTILIZADAS PARA IDENTIFICAR LOS FALLOS 35
2.3.4 EXPLICACIÓN DE LA AFECTACIÓN DEL ATAQUE 36
2.3.5 DOCUMENTAR CADA UNO DE LOS PASOS 36
2.4 CONTENCIÓN DE ATAQUES INFORMÁTICOS 36
2.4.1 ACCIONES A REALIZAR EN LINEA FRENTE A UN ATAQUE 36
2.4.2 QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA 37
2.4.3 DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS 37
2.4.4 SI LE INDICAN QUE DEBE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” USTED LO UTILIZARÍA PARA QUÉ FIN 38
2.4.5 FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM 38
2.4.6 DEFINA POR LO MENOS 3 HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS 39
2.4.6.1 Winpatrol 39
2.4.6.2 Snort 39

2.4.6.3 Security Onion..... 39
CONCLUSIONES 40
ANEXOS 44

Anexo A Video de Sustentación ……..45
Anexo B Prueba Turniting ……45

LISTA DE FIGURAS

Pág.

Figura 1 Máquina Virtual 17
Figura 2 Repositorio OVAS 17
Figura 3 Importación OVA Windows 18
Figura 4 Montar Máquina Virtual Kali Linux 18
Figura 5 Máquinas virtuales 19
Figura 6 Máquina Windows 7 19
Figura 7 Maquina Kali Linux Dirección IP 20
Figura 8 Ping desde Windows a Linux 20
Figura 9 Configuración Kali Linux 21
Figura 10 Configuración Kali Linux Almacenamiento 21
Figura 11 Configuración Windows 7 22
Figura 12 Escaneo de la máquina Windows 25
Figura 13 Identificación IP Máquina Windows 26
Figura 14 Identificación de puertos abiertos 26
Figura 15 Identificar Más información Vulnerable 27
Figura 16 Identificación Vulnerabilidades 27
Figura 17 Identificación Puerto y servicio para atacar 28
Figura 18 Identificación de la vulnerabilidad ms17-010 28
Figura 19 Ejecución de metasploit 29
Figura 20 Se identifica la vulnerabilidad ms17-010 29
Figura 21 Identificación información para atacar 30
Figura 22 Se identifican las variables a configurar para el ataque 30
Figura 23 Se ejecuta el comando use exploit 31
Figura 24 configuración RHOST RPORT 31
Figura 25 Ejecución del ataque run 32
Figura 26 Acceso a la máquina Windows 32
Figura 27 Creación usuario desde kali linux en Windows 33
Figura 28 Validación usuario creado desde Linux 33
Figura 29 Acceso con usuario creado 34
Figura 30 Máquina Windows 7 X86 34

RESUMEN

El presente informe pretende dar a conocer las vulnerabilidades que tanto una persona como una organización enfrentan actualmente en el ámbito social y comercial a través de la tecnología; conocer la legislación que rige para el entorno colombiano y las formas en que se pueden blindar para minimizar los ataques informáticos, las herramientas tecnológicas en las que se pueden apoyar y las técnicas a emplear para avanzar en la identificación de riesgos a través del RedTeam y el BlueTeam para así sortear los delitos informáticos.

Es importante que estos equipos cuenten con bancos de pruebas donde puedan desplegar las diferentes herramientas que permitan realizar seguimientos a los diferentes ataques o realizar los mismos con el objetivo de identificar las vulnerabilidades y realizar el endurecimiento de los mismos con el fin de evitar los ataques por parte de black hackers.

Por otra parte, la exposición a las redes sociales, son la plataforma desde la cual los Hackers se valen para atacar a los individuos del común. Estos escenarios han contribuido de gran forma para que nuestra privacidad sea expuesta de manera voluntaria. De otra parte, el sistema de globalización que dio apertura al mercado digital, generó también que las organizaciones se vieran abocadas a exponer su información para no desaparecer dentro de un mercado en constante crecimiento y trasformación.

ABSTRACT

This report aims to publicize the vulnerabilities that both a person and an organization currently face in the social and commercial field through technology; Know the legislation that governs the Colombian environment and the ways in which they can be shielded to minimize computer attacks, the technological tools that can be supported and the techniques to be used to advance in the identification of risks through the RedTeam and the BlueTeam in order to circumvent computer crimes.

It is important that these teams have test benches where they can deploy the different tools that allow them to monitor the different attacks or carry them out with the aim of identifying vulnerabilities and hardening them in order to avoid attacks by part of black hackers.

On the other hand, exposure to social networks is the platform from which Hackers use to attack ordinary individuals. These scenarios have greatly contributed to our privacy being voluntarily exposed. On the other hand, the globalization system that opened up the digital market also caused organizations to be forced to expose their information so as not to disappear within a market in constant growth and transformation.

GLOSARIO

Amenaza: Cualquier evento al que pueda estar expuesta la organización

Blue Team: Equipo azul es el encargado de estar monitoreando los sistemas de información en busca de ataques de externos.

Pentesting: El pentesting o técnica de penetración consiste en realizar ataques a diferentes activos con el fin de encontrar puntos vulnerables o posibles fallos.

Red Team: Equipo rojo, encargado de realizar ataques controlados a los sistemas de información con el fin de identificar el grado de preparación en el que se encuentra para enfrentar un ataque real.

Riesgo: Es la probabilidad de que se materialice una amenaza, explotando una vulnerabilidad del sistema.

Seguridad informática: es el conjunto de herramientas y técnicas utilizadas para garantizar la confidencialidad, integridad y disponibilidad de la información.

Vulnerabilidad: Debilidades encontradas por los atacantes extenso o internos para atacar un sistema.

INTRODUCCIÓN

El proceso de globalización y la constante evolución de la tecnología, individuos y organizaciones se han visto impulsados a exponer su entorno personal, social y comercial en la Internet. Esto, con el fin de no quedar relegados o simplemente desaparecer del mercado. Es así como se han convertido en ciudadanos 2.0.

Con la aparición del Covid-19, se produjo un proceso de aceleración frente al tema del trabajo en casa, el cual venía dando algunos pasos con moderación y que llevó a utilizar conexiones remotas, desprovistas de mecanismos de blindaje que pudieran evitar fugas de información. Esto no fue ajeno a los atacantes informáticos que ya venían haciendo de las suyas, ahora se abría un panorama más grande donde podían identificar más fácilmente las vulnerabilidades de individuos y organizaciones y poder así realizar sus ataques.

Para esto se examinarán diferentes documentos donde se identifiquen las funciones que realizan estos equipos, las leyes que enmarcan estas actividades, al igual que el concepto ético que debe ser parte integral de las personas que integren estos equipos, así como la definición de las diferentes herramientas en las que se pueden apoyar, con el fin de realizar seguimiento y monitorización a las vulnerabilidades, minimizando así posibles ataques.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Conocer las actividades a realizar por parte de los equipos Blue Team y Red Team enmarcados en la normatividad y principios éticos, apoyados en herramientas tecnológicas y metodologías para minimizar las vulnerabilidades de los activos de las organizaciones.

1.2 OBJETIVOS ESPECÍFICOS

Identificar las actividades de los equipos de Blue Team y Red Team enmarcadas en la normatividad y principios éticos vigentes, para garantizar la aplicación de buenas prácticas por parte de los mismos.

Conocer las diferentes herramientas disponibles en el mercado que apoyen a los equipos Blue Team y Red Team que permitan monitorizar e identificar intrusiones para el seguimiento, control y mitigación de incidentes o vulnerabilidades.

2 DESARROLLO DE LA ACTIVIDAD

2.1 CONCEPTOS Y EQUIPOS DE SEGURIDAD

2.1.1 DENTRO DEL MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES QUE LEYES EXISTEN

La Ley 1273 de 2009 legisla los delitos relacionados con delitos informáticos y se encuentra discriminado en dos capítulos así:

Capítulo 1 Legisla lo relacionado con los sistemas informáticos y los datos garantizando la confidencialidad, integridad y disponibilidad de éstos.
Capítulo 2 Legisla lo relacionado con atentados informáticos y otras infracciones.

Referente al capítulo1 encontramos los siguientes artículos:

Artículo 269A “Acceso abusivo a un sistema informático: La persona que acceda de forma irregular y no autorizada o sobrepase lo acordado sin autorización de quien corresponda, incurrirá en cárcel de 48 a 96 meses de prisión y tendrá una multa de 100 a 1000 salarios mínimos mensuales vigentes”.

Artículo 269B “Obstaculización ilegítima de sistema informático o red de telecomunicación: El que impida el acceso o funcionamiento a los datos informáticos de un sistema, incurrirá en cárcel de 48 a 96 meses de cárcel. Si se considera que esta acción ocasionó otros problemas, se asumirán también la sanción de este e incurrirá en pago de 100 a 1000 salarios mínimos vigentes”.

Artículo 269C “Interceptación de datos informáticos: El que en cualquiera de las etapas intercepte datos informáticos por fuera o dentro de la organización o en las ondas electromagnéticas que transporten información incurrirán en prisión de 36 a 72 meses, éste no tiene sanciones económicas”.

Artículo 269D “Daño informático: El que altere, destruya, borre destruya un sistema informático o sus componentes físicos y lógicos incurrirá en prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos mensuales vigentes”.

Articulo 269E “Uso de software malicioso: Aquel que produzca, trafique, utilice software malicioso con el fin de causar daños o robar información, incurrirá en penas de 48 a 96 meses de prisión y multa de 100 a 1000 salarios mínimos mensuales vigentes”.[1]

Artículo 269F Violación de datos personales: el que con provecho propio o de un tercero utilice información de cualquier persona si su permiso de bases de datos, ficheros o archivos para cualquier uso, incurrirá en penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos mensuales vigentes.

Artículo 269G Suplantación de sitios WEB para capturar datos personales: el que desarrolle publique, trafique con páginas web que direccionen a sitios que permitan el robo de información de datos personales y a su vez modifique la resolución de dominios direccionando a otros sitios, incurrirá en penas de 48 a 96 meses, si este es recurrente se incrementará en una tercera parte y tendrá sanción económica de 100 a 1000 salarios mínimos mensuales vigentes.

Articulo 269H Circunstancias de agravación punitiva: la pena se aumentará de la mitad a l tres cuartas partes si:

- Si se realiza sobre redes públicas del estado o entidades financieras
- Si es realizado por un empleado publico
- Si es realizado por un proveedor aprovechando las relaciones comerciales
- Con fines terroristas o que atenten contra la seguridad del estado.
- Se inhabilitará hasta tres años el acceso a sistemas de cómputo a la persona si esta es el administrador y se aprovecha de dicho estado0.

Referente al Capítulo 2 encontramos los siguientes artículos:

Artículo 269I Hurto por medios informáticos o semejantes: aquel que supere todas las medidas de seguridad y demás contemplados en el artículo 239 y suplante a la persona incurrirá en las penas mencionadas en el artículo 240.

Artículo 269J Transferencia no consentida de activos: Aquel que valiéndose de la tecnología logró realizar la transferencia de activos a un tercero o así mismo sin autorización del propietario incurrirá en penas de 48 a 120 meses de prisión y multas entre 200 y 1500 salarios mínimos legales vigentes. Se incrementará en la mitad si la cuantía de la estafa supera los 200 salarios mínimos mensuales vigentes[2].

[1] Leyes desde 1992 Vigencia expresa y control de constitucionalidad [Sitio WEB]Ley 1273 de2009 [Consulta: 29 de agosto de 2022] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[2] Leyes desde 1992 Vigencia expresa y control de constitucionalidad [Sitio WEB]Ley 1273 de2009 [Consulta: 29 de agosto de 2022] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

2.1.2 DEFINIR CADA UNA DE LAS ETAPAS DEL PENTESTING

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Las etapas para realizar la penetración a un sistema pueden variar en uno o dos pasos, pero la esencia de los pasos a seguir se mantiene entre estos, unos colocan una o dos adicionales, pero finalmente se contemplan los principales pasos.

Según OWASP se mencionan las siguientes fases:

- Reconocimiento
- Análisis de Vulnerabilidades
- Explotación
- Post Explotación
- Informes

Reconocimiento

En esta fase se indaga el inventario de los activos a los cuales se les realizará la intrusión, identificando todos los atributos encontrados con el fin de poder posteriormente identificar si se tienen vulnerabilidades

Análisis de Vulnerabilidades

En esta fase con el inventario de los activos y sus atributos se indagan en las diferentes bibliotecas de vulnerabilidades cuales aplican para la explotación de cada uno de los activos, siempre buscando cual poder explotar y penetrar el sistema.

Explotación

Identificadas las vulnerabilidades, se utilizan las diferentes herramientas con el fin de penetrar e identificar específicamente cómo se logra explotar estos hallazgos y hasta donde se pude llegar dentro del sistema al que se le realiza la intrusión.

Post Explotación
Se continua con el ataque de penetración con el fin de lograr penetrar lo más profundo que se pueda dentro del sistema para secuestrar información, encontrar información confidencial, usuarios claves que tengan accesos superiores.[3]

[3]Hiberus blog [Sitio Web] Pentesting con OWASP Fases y Metodología [Consulta 1 de septiembre de 2022] Sitio web: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

Informes

Una vez realizada la penetración se debe realizar la documentación de los hallazgos encontrado y si dentro del convenio quedo realizar las recomendaciones colocar las mismas con el fin de reducir las vulnerabilidades de las mismas.

Técnicas de auditoría de caja negra con Nmap

¿En las técnicas de auditoría de caja negra Qué función tendría el programa Nmap? ¿Qué resultados se obtiene al hacer uso de esta aplicación? Mencione los comandos principales y básicos para Nmap; deben describir que comando se puede utilizar en Nmap para hacer uso de los scripts programados para análisis de vulnerabilidades ya que es un tema avanzado.

2.1.3 HERRAMIENTAS DE CIBERSEGURIDAD

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

Metasploit

El framework metasploit permite un sin número de pruebas que permiten identificar las diferentes vulnerabilidades con las que cuenta un sistema informático, este le permite a los pentesting ejecutar un sin número de actividades orientadas a la identificación de las diferentes vulnerabilidades, esto en ambientes de pruebas que pueden simular el ambiente real y realizar los ataques correspondientes y poder definir los mecanismos de minimización de los riegos.

Obviamente por ser una herramienta d código abierto esta puede ser utilizado por los hackers éticos y los black hakers, lo que hace indispensable definir todas las medidas de seguridad con el fin de reducir la exposición de la organización frente a estos ataques.[4]

NMAP

Nmap es un sistema escáner de puertos, que se ejecuta contra un servidor. Nmap envía paquetes simultáneamente y ping TCP para obtener información de los puertos. La respuesta del ping TCP indica que el servidor de destino está en línea y se puede seguir

[4] CIBERSEGURIDAD [Sitio Web] Que e Metasploit framework y como funciona [Consulta 1 de septiembre de 2022] Sitio web: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

escaneando. Si el servidor escaneado no responde puede indicar que está fuera de línea o que está protegido por un firewall.
Usar esta aplicación, permite buscar y explorar las vulnerabilidades detectadas en una red, aplicación o servidor. Para realizar una prueba de penetración se debe tener un plan o un orden específico para realizar las exploraciones. Como ejemplo se podría decir que, si se piensa como un atacante en el mundo real, se debe obtener conocimiento del sistema que se desea atacar para saber qué puntos débiles se pueden explotar.

Comandos Nmap
Selección de objetivo en Nmap
-Escanear una IP: nmap 192.168.8.109
-Escanear un nombre de host: nmap mihost
-Escanear un rango de IP´s (en este caso de la IP 190 a la 200): nmap 192.168.8.190-200
-Escanear una subred: nmap 192.168.8.0/24 nmap escanear subred
-Escanear una lista de objetivos desde un archivo: nmap -iL lista.txt
Selección de puerto en Nmap
-Escanear un solo puerto: nmap -p 22 192.168.8.109
-Escanear un rango de puertos: nmap -p 1-30 192.168.8.109
- Escanear los 100 puertos más comunes (la opción más rápida para ejecutar un escaneo con nmap): nmap -F 192.168.8.109
- Escanear todos los puertos (65536):nmap -p 192.168.8.109
Detección de Servicios y de Sistema Operativo con nmap
- Detectar el Sistema Operativo y los servicios activos: nmap -A 192.168.8.109
- Detección estándar de servicios (detección de versiones; obtiene más info de lo que se está ejecutando una vez que se han detectado los puertos):nmap -sV 192.168.8.109
- Detección ligera de servicios (una forma más rápida de detectar servicios): nmap -sV --version-intensity 0 192.168.1.1
Ayuda e información sobre los scripts NSE de Nmap
Con la opción --script-help=nombre_script, obtendremos la ayuda de cada uno de los scripts, y algo de información acerca de la utilidad que tiene el script:
Por ejemplo: nmap --script-help=whois-domain.nse

Nmap cuenta con unos scripts predefinidos que podremos utilizar para obtener información sobre la vulnerabilidad de los sistemas ante algunos ataques, además de personalizar la ejecución de los scripts mediante los argumentos que le pasemos durante un escaneo e incluso tenemos la posibilidad de escribir scripts propios que se ajusten a nuestras necesidades mediante el lenguaje LUA.
Además, Nmap permite que se puedan añadir scripts personalizados para explotar las vulnerabilidades encontradas.
Podemos ejecutar los scripts ya sea indicando una categoría de scripts, el nombre del script específico o el directorio en donde se almacena el o los scripts que queremos utilizar.
Nmap es muy reconocida en el mundo de seguridad informática por su funcionalidad de escaneo de redes, puertos y servicios. No obstante, la herramienta ha ido mejorando con

el correr de los años, ofreciendo cada vez más posibilidades que resultan muy interesantes. Actualmente incorpora el uso de scripts para comprobar algunas de las vulnerabilidades más conocidas, por ejemplo:
Auth: ejecuta todos sus scripts disponibles para autenticación
Default: ejecuta los scripts básicos por defecto de la herramienta
Discovery: recupera información del target o víctima
External: script para utilizar recursos externos
Intrusive: utiliza scripts que son considerados intrusivos para la víctima o target
Malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors (puertas traseras)
Safe: ejecuta scripts que no son intrusivos
Vuln: descubre las vulnerabilidades más conocidas
All: ejecuta absolutamente todos los scripts con extensión NSE disponibles

OPENVAS

Es una de las herramientas más populares para el escaneo y solución de vulnerabilidades de redes, cuenta con una amplia biblioteca de casos identificados los cuales utiliza para identificar los posibles accesos, pero igualmente informa como solucionarlos, esta herramienta también tiene una versión gratuita que permite ser utilizada sin ningún tipo de licenciamiento.

ExploitDb

Esta es una base de datos donde se publica la información de las diferentes vulnerabilidades identificadas por los hackers y que puede ser utilizada por cualquier persona para realizar ataques o minimizar las vulnerabilidades.

CVE

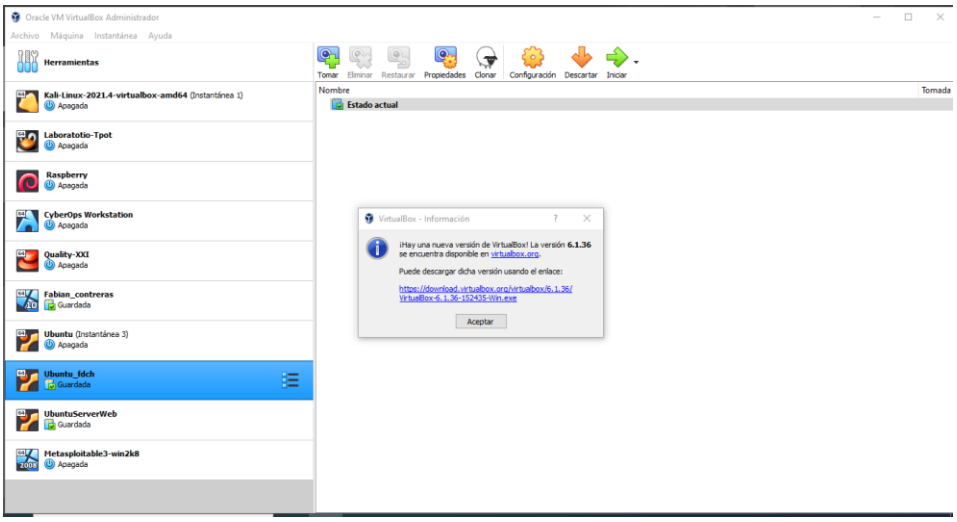
Por sus siglas en inglés Common Vulnerabilities and Exposures, es un diccionario de las diferentes vulnerabilidades encontradas y las soluciones frente a estas.

2.1.4 BANCO DE TRABAJO

Es importante que usted reconozca, analice y configure “banco de trabajo”

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

Figura 1 Máquina Virtual

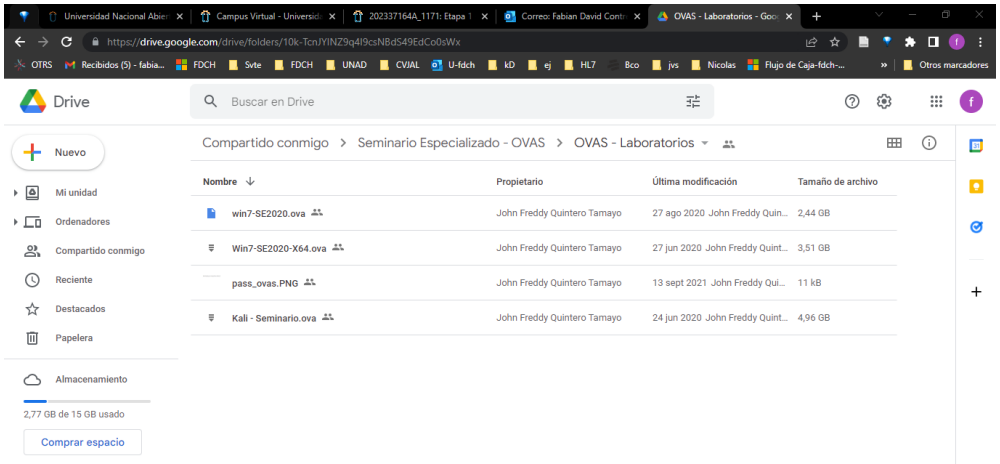


Autoría Propia

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

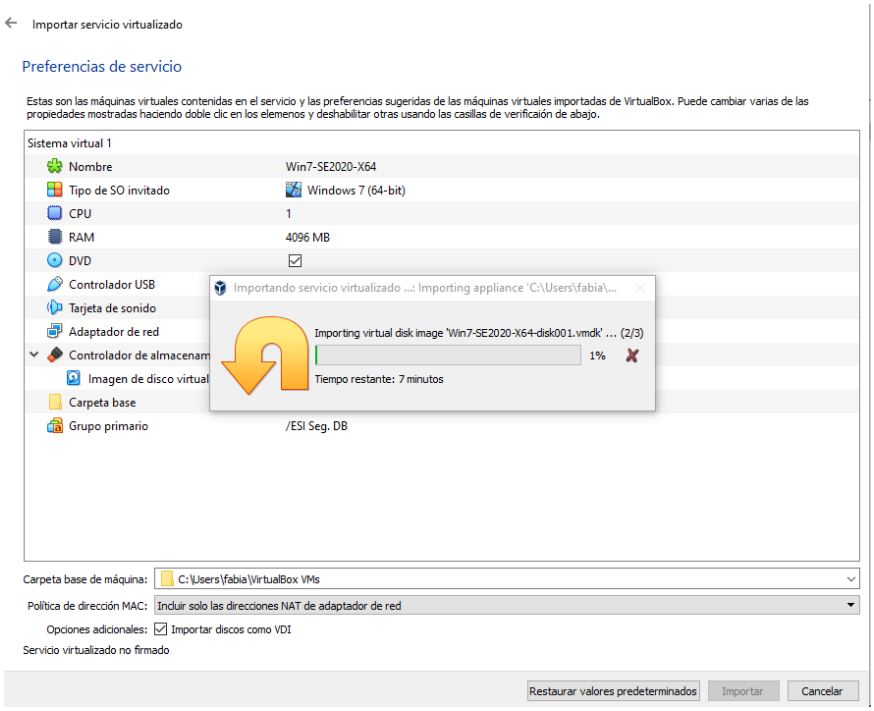
  Se procede hacer la descarga de las OVAS del link suministrado en el foro.

Figura 2 Repositorio OVAS



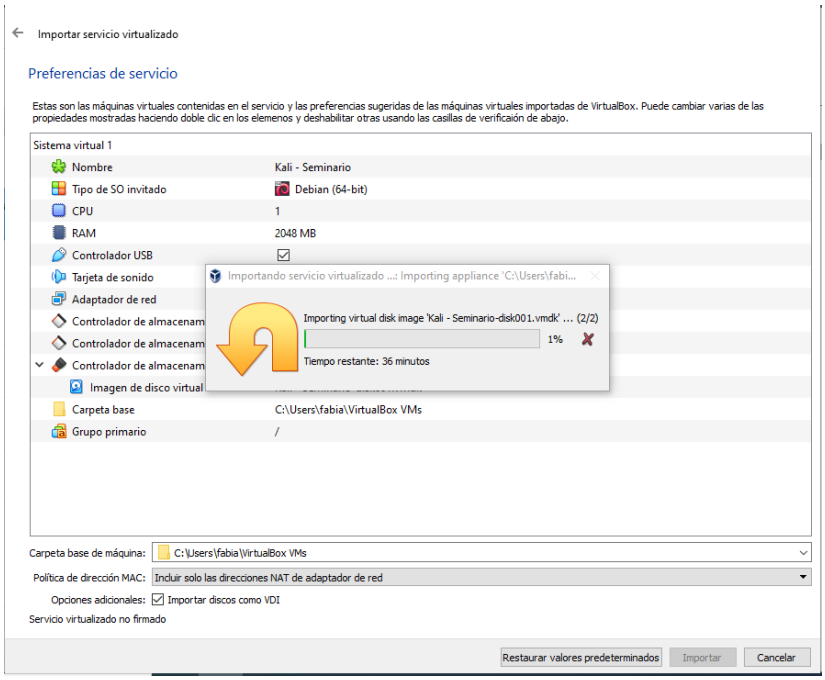
Autoría: Propia

Figura 3 Importación OVA Windows



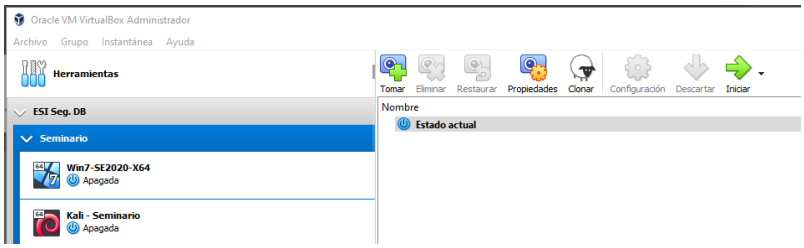
Autoría Propia

Figura 4 Montar Máquina Virtual Kali Linux



Autoría Propia

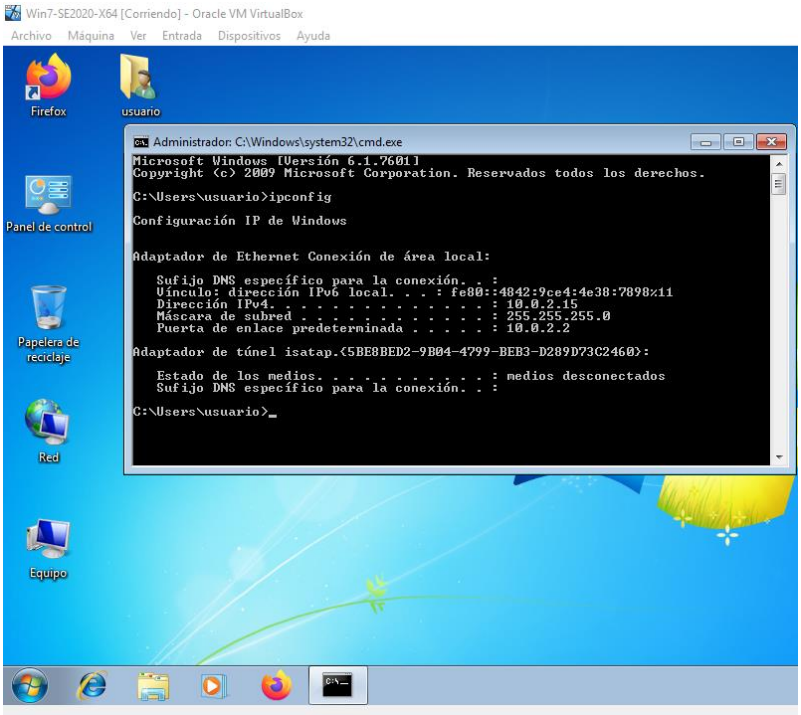
Figura 5 Máquinas virtuales



Autoría propia

- 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.

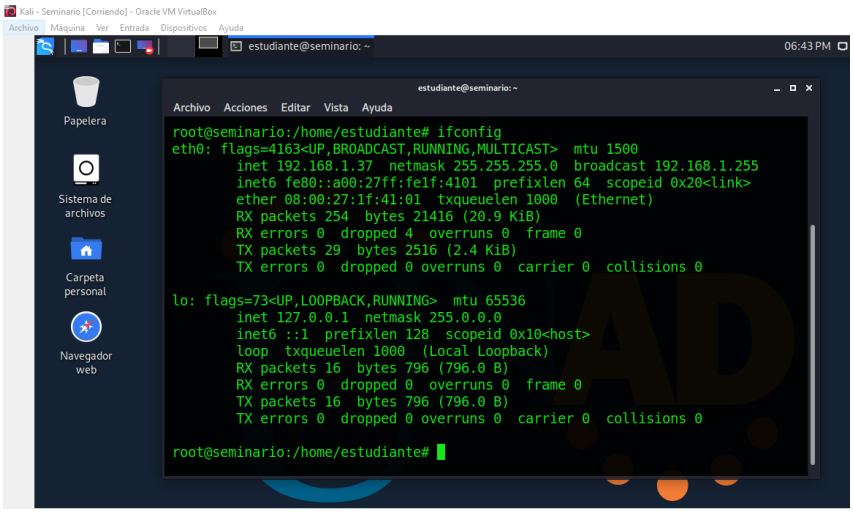
Figura 6 Máquina Windows 7



Autoría Propia

La IP del sistema operativo Windows 7 es 10.0.2.15 si realizo un ping desde la maquina local Windows 10 se recibe comunicación.

Figura 7 Maquina Kali Linux Dirección IP

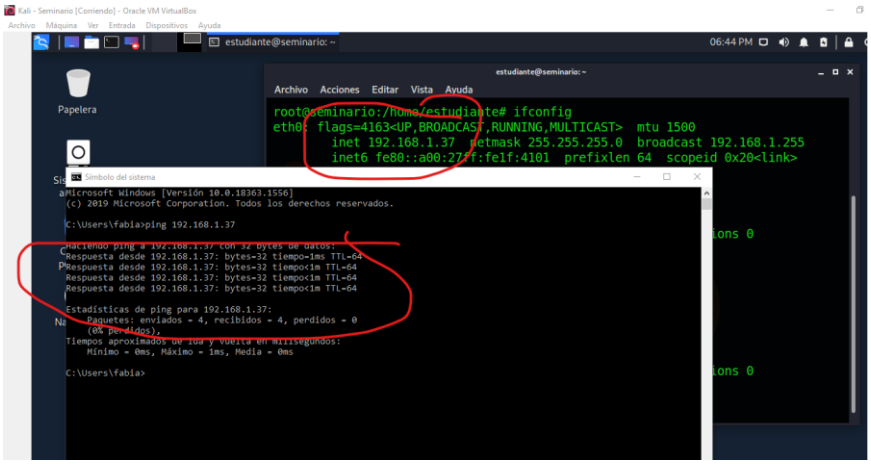


Autoría Propia

Dirección IP de la Maquina Kali Linux 192.168.1.37

Se realiza ping desde la maquina Windows a la maquina Kali Linux y se obtiene respuesta

Figura 8 Ping desde Windows a Linux

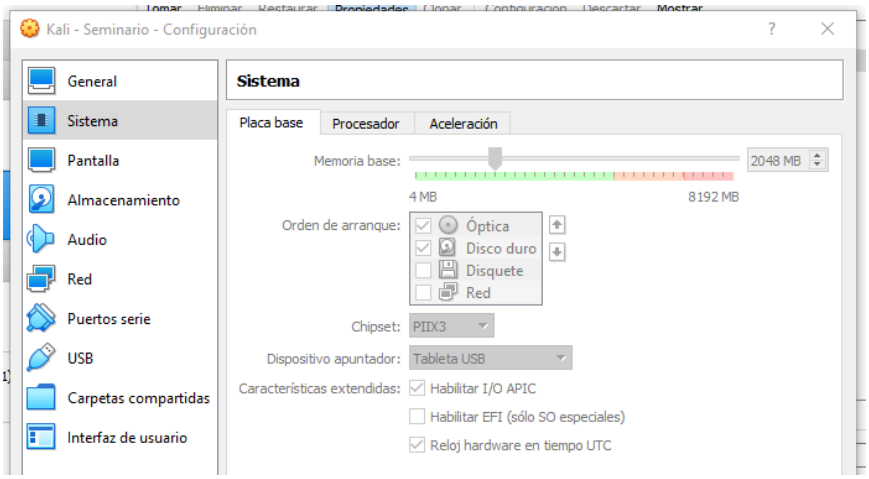


Autoría Propia

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

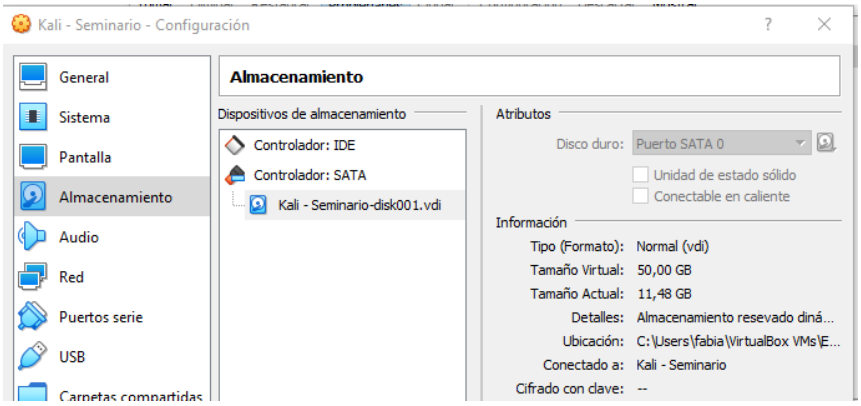
Se realiza la importación dela OVA de Kali Linux y estas son las características que se tienen.

Figura 9 Configuración Kali Linux



Autoría Propia

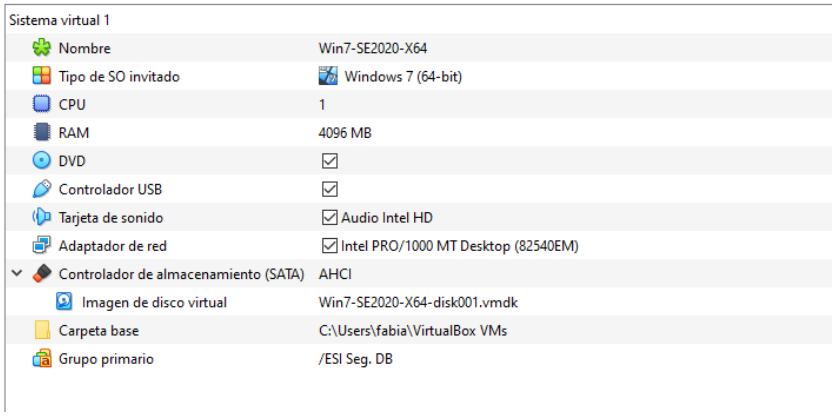
Figura 10 Configuración Kali Linux Almacenamiento



Autoría Propia

Se realiza la importación del OVA de Windows y estas son las características de la maquina

Figura 11 Configuración Windows 7



Autoría propia

2.2 ACTUACION ÉTICA Y LEGAL

2.2.1 EVIDENCIAR PROCESOS ILEGALES Y NO ETICOS

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 - Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad

- Clausula primera: referente al siguiente texto (la información confidencial o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados) la ley 842 de 2003 en su capítulo II Articulo 31 Deberes generales de los profesionales en el literal “e” habla de que se debe prestar la debida colaboración a la policía y/o representantes del consejo nacional frente a cualquier indagación que se esté realizando

- Clausula segunda: referente al siguiente texto en lo que se considera información confidencial (datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”), es de anotar que al ser información obtenida si autorización y de forma abusiva estaría incurriendo en faltas contempladas en la ley 1273 artículo 269ª acceso abusivo a un sistema informático y podría tener sanciones de 48 a 96 meses de prisión y las sanciones económicas de 100 a 1000 salarios mínimos mensuales vigentes.

- Clausula cuarta: en el texto que se cita en el numeral 3 (No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros), se puede incurrir en faltas a la ley 1273 de 2009 en el Artículo 269F Violación de datos personales

incurriendo en penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos mensuales vigentes.

- Clausula cuarta: en el texto que se cita en el numeral 7 (Responder por el mal uso que le den sus representantes a la información confidencial)Si bien aquí no se está incurriendo en ninguna falta contra el código de ética o la ley 1273 de 2009 la persona contratante no puede responder por los hechos realizados por terceros con la información entregada en su investigación, ya que la responsabilidad del mismo no llegaría hasta ese punto, a menos de que sea consiente o participe del mal uso del mismo, en dado caso podría incurrir en violación del artículo 269F Violación de datos personales incurriendo en penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos mensuales vigentes.

- Clausula cuarta: en el texto que se cita en el numeral 8. (Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento) Frente a este si la información encontrada en su poder fue obtenida de forma ilegal se debe responder por los actos correspondientes y dependiendo de la información que se encuentre y la forma como se obtuvo, este tendrá las sanciones correspondientes de la ley 1273 de 2009.

- Clausula cuarta: en el texto que se cita en el numeral 9 (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), frente al tema de la información confidencial es claro que esta no debe ser suministrada si autorización escrita por parte de la organización siempre y cuando esta no sea requerida por un ente judicial con los requisitos de ley correspondientes, frente a la información ilegal obtenida, primero éticamente no se debería obtener esta ya que incurriría en faltas a la ley 1273 de 2009 y dependiendo como se obtuvo la misma incurriría en la sanción que se le atribuya al artículo correspondiente de la misma.

- Clausula octava: frente a la solución de controversias (En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security) En caso de que se encuentre en manos de la persona información obtenida de forma ilegal, es este el que debe responder ante las autoridades correspondientes por la misma y las sanciones correspondientes serán con base en la ley 1273 de 2009 dependiendo del artículo donde se enmarque la información obtenida y como se obtuvo la misma, en caso de que sea por orden directa de Hackers Security y probatoriamente se identifique que se actuó por orden explicita de la misma, la sanción será para las dos partes.

2.2.2 USTED COMO EXPERTO EN CIBERSEGURIDAD APLICARÍA A ESTE TRABAJO

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted como experto en ciberseguridad aplicaría a este trabajo en Hackers Security, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.
Si bien el objetivo de un pentesting es el de penetrar de cualquier forma los diferentes sistemas informáticos o cualquiera utilizando las diferentes metodologías o herramientas de intrusión, es importante que estas se deben de realizar sin incurrir en ninguna infracción de la ley 1273 de 2009 o lo dispuesto en el código de ética de COPNIA, el cual se soporta en la ley 842 de 2003.
Si bien la oferta económica es muy tentadora, las diferentes cláusulas que hacen referencia a la información ilegal y las responsabilidades que debemos asumir nos hacen ver que el objeto del contrato es el de ser un Black Hacker y que muchos trabajos se realizarían de forma ilegal, lo cual a lo largo nos acarrearía problemas legales y las respectivas sanciones por parte de COPNIA.
Por tal motivo no aceptaría la propuesta de trabajo.

2.2.3 OPERACIÓN ANDROMEDA BUGGLY

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

Cuando se realiza la investigación y se contextualiza la forma como operaba esta red de hackeo, se pueden observar que las personas implicadas en la misma carecían de un sentido ético, ya que la forma como reclutaban las personas con el fin de obtener su conocimiento y entender como irrumpir en diferentes sistemas era por intermedio de una comunidad, donde se desvirtuó totalmente el sentido ya que se aprovecharon de las personas que allí asistían y se aprovecharon de su conocimiento para cometer diferentes ilícitos.
Lo más preocupante desde mi punto de vista es que esta “comunidad” era una facha montada por el propio gobierno en cabeza del ejercito con recursos ilimitados para ser utilizados en seguimientos a diferentes entidades, personalidades o instituciones para beneficiar a terceros ya hubieran sido del mismo gobierno o lo que sucedió después a terceros dependiendo del pago que este les ofreciera dándola al mejor postor.
Frente a esto se realizó un estudio de ingeniería social con el fin de identificar como se podría captar a todas estas personas que por sus conocimientos avanzados en sistemas y programación pudieran irrumpir a los diferentes sistemas informáticos para obtener de forma ilegal y abusiva diferente información. Es así como se les proporcionaban equipos de última generación, consolas de juegos que incluían torneos para posteriormente obtener lo que se buscaba de ellos. Incluso muchos de ellos ni se dieron por enterado de

lo que hicieron ya que pensaban que era algún hijo de papi y mami que le gustaba gastar el dinero en estas actividades.
Si analizamos lo ocurrido en este sitio frente a la ley 1273 del 2009 y el código de COPNIA, la conclusión es que se incurrió en sanción de todos los artículos e incluso con los agravamientos correspondientes por hacerlo a entidades del gobierno y por pertenecer al mismo.

2.3 EJECUCIÓN PRUEBAS DE INTRUSIÓN

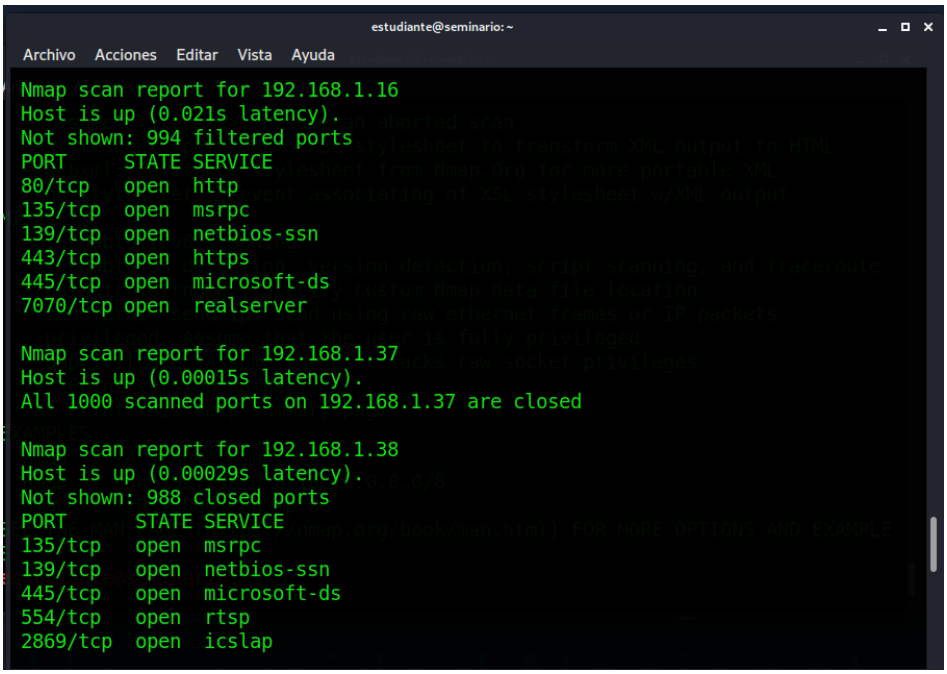
2.3.1 HERRAMIENTAS DE SOFTWARE UTILIZADAS

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting

2.3.1.1 Nmap

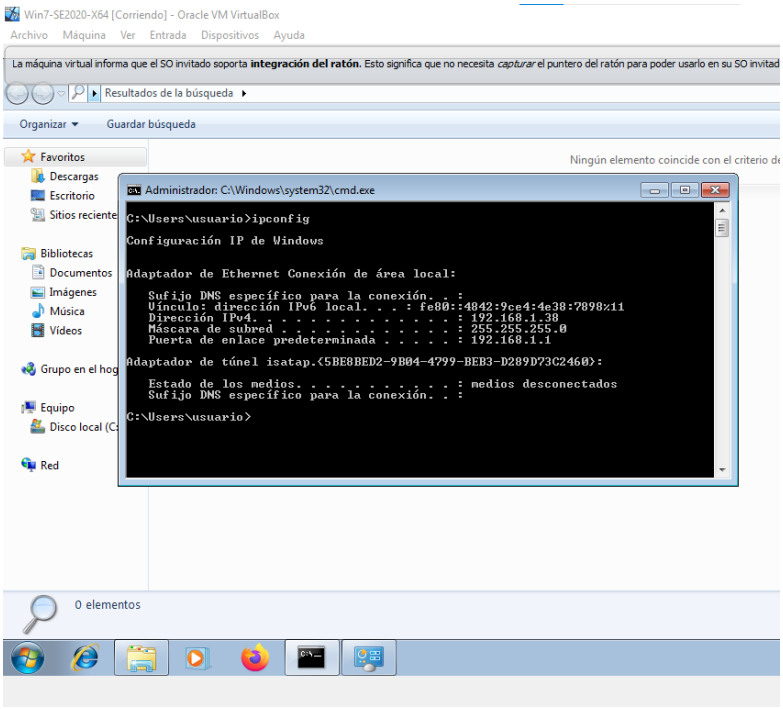
Ejecutamos el comando nmap 192.168.1.0/24 que lo que hace es buscar dentro de ese rango de red, cuales equipos encuentra y los puertos abiertos aquí logramos identificar la IP a la cual queremos atacar que es la 192.168.1.38

Figura 12 Escaneo de la máquina Windows



Fuente: Autoría Propia
Desde la maquina Windows ejecuto el comando ipconfig y me arroja la ip asignada al sistema operativo

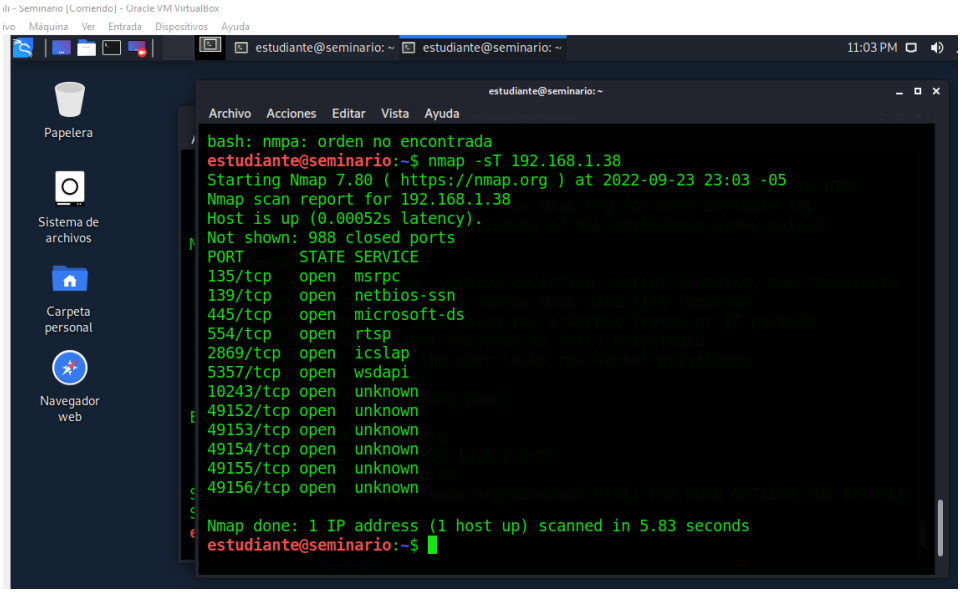
Figura 13 Identificación IP Máquina Windows



Fuente: Autoría propia

Posteriormente ejecutamos el comando nmap -sT 192.168.1.38 que es la IP del equipo Windows y nos muestra los puertos abiertos

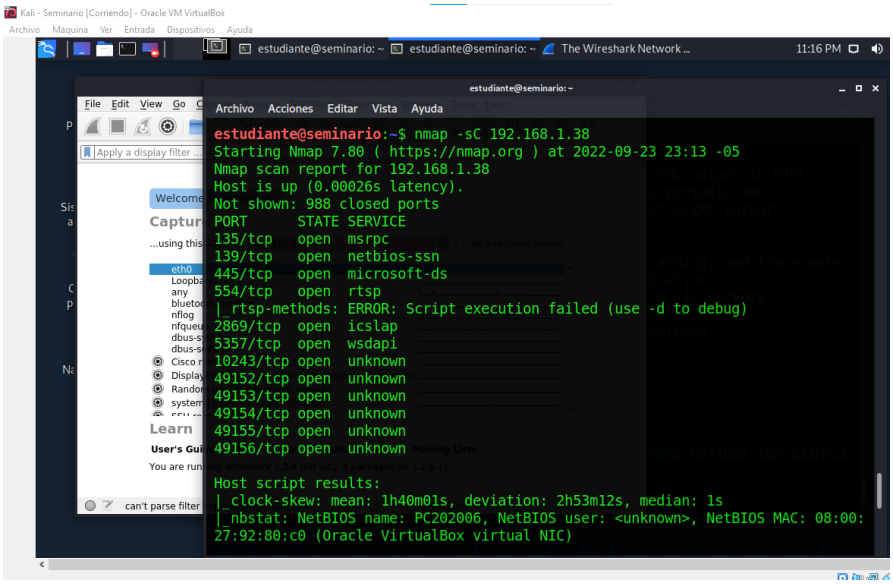
Figura 14 Identificación de puertos abiertos



Fuente: Autoría Propia

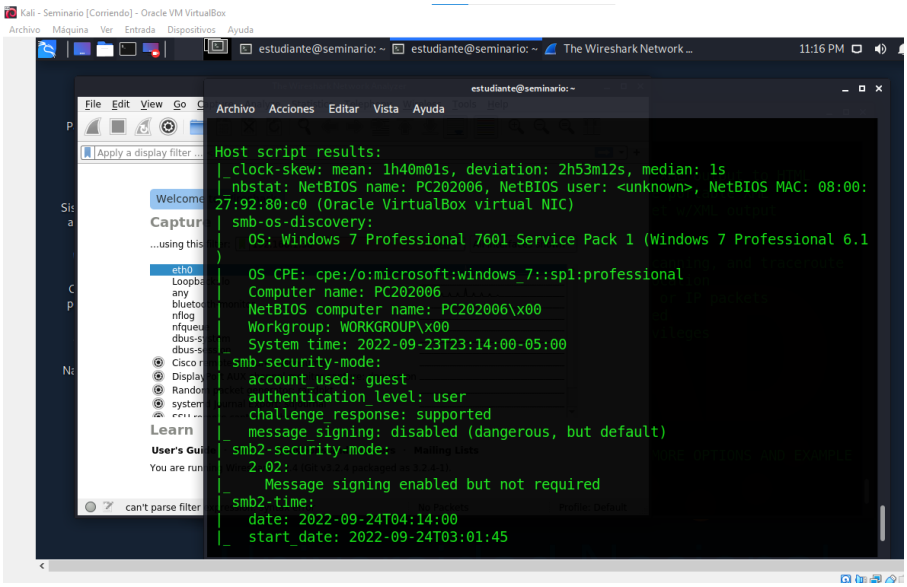
Se ejecuta el comando nmap –sC 192.168.1.38, el cual realiza un escaneo completo de todas las vulnerabilidades del equipo objetivo.
Aquí encontramos cuales son los servicios que esta abiertos, que sistema operativo es y la versión del SP, entre otros datos.

Figura 15 Identificar Más información Vulnerable



Fuente: Autoría Propia

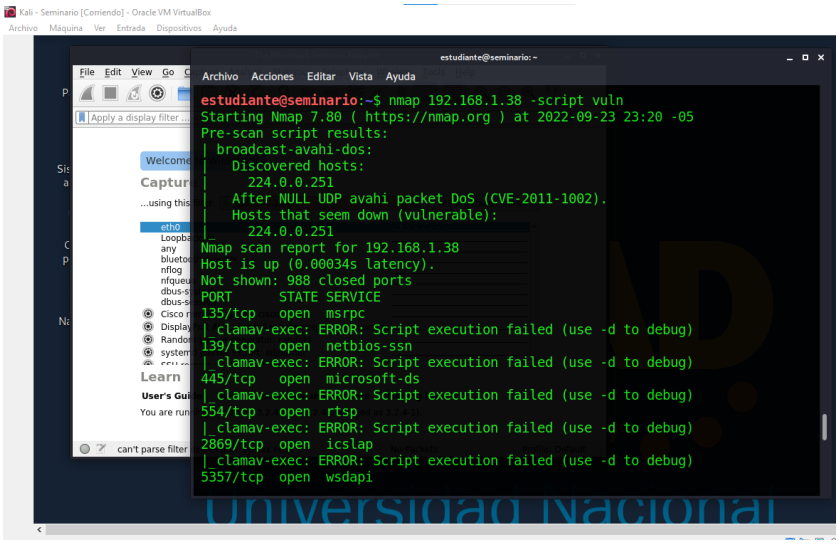
Figura 16 Identificación Vulnerabilidades



Fuente: Autoría Propia

Con el fin de identificar las vulnerabilidades ejecutamos el comando nmap 192.168.1.38 –script vuln, este comando nos informara los códigos de las vulnerabilidades para con base en esto realizar la explotación.

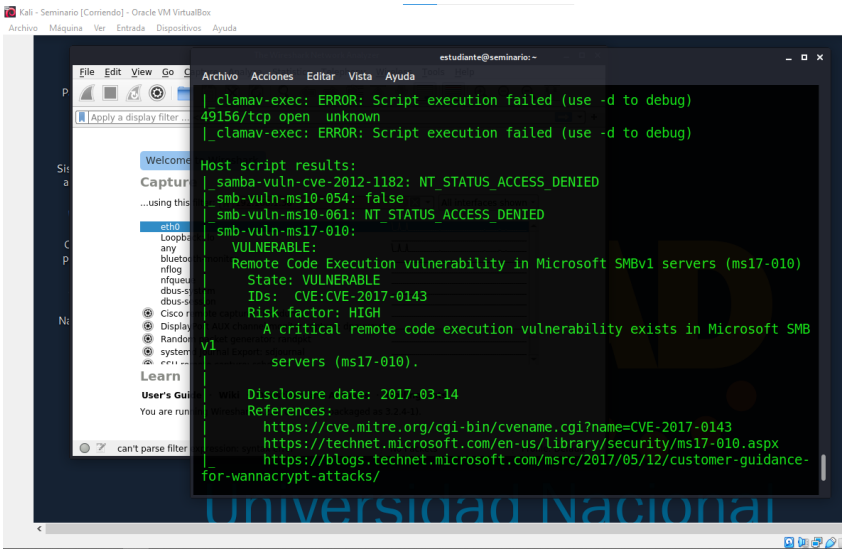
Figura 17 Identificación Puerto y servicio para atacar



Fuente: Autoría Propia

En la anterior imagen se observa el puerto 445/tcp Microsoft-ds, que es por donde podremos acceder a la maquina Windows 7.
En la siguiente imagen se observa las vulnerabilidades informadas en el anexo 4

Figura 18 Identificación de la vulnerabilidad ms17-010

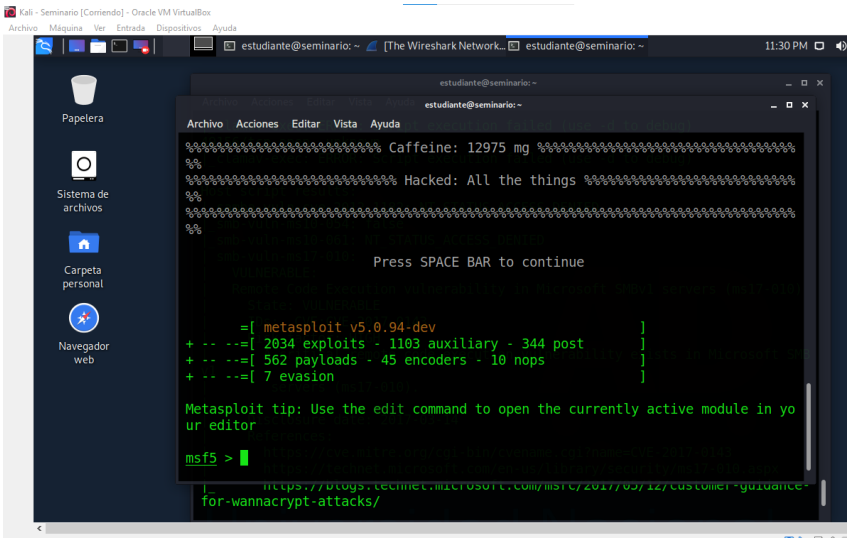


Fuente: Autoría Propia

2.3.1.2 Metasploit

Se realiza la iniciación de la funcionalidad metasploit desde una terminal de Kali Linux con el comando msfconsole para realizar desde allí el ataque.

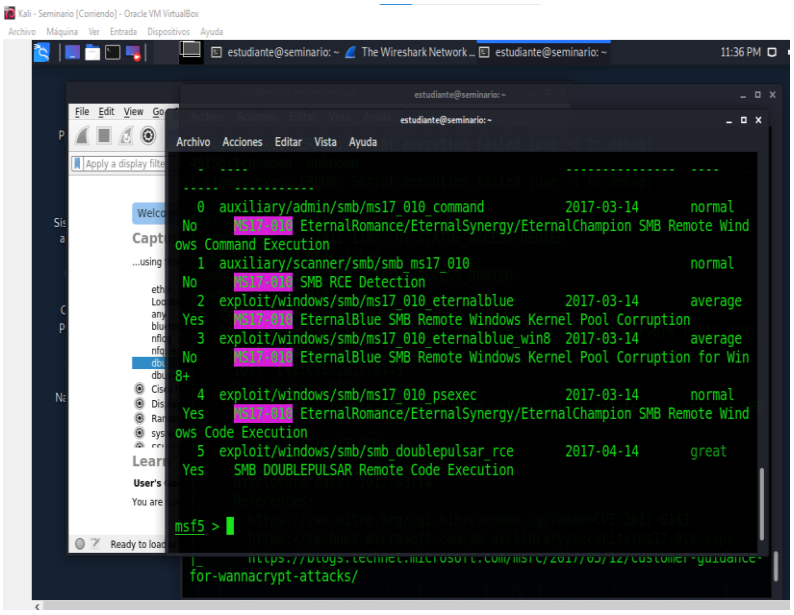
Figura 19 Ejecución de metasploit



Fuente: Autoría Propia

Hacemos la búsqueda de la vulnerabilidad ms17-010

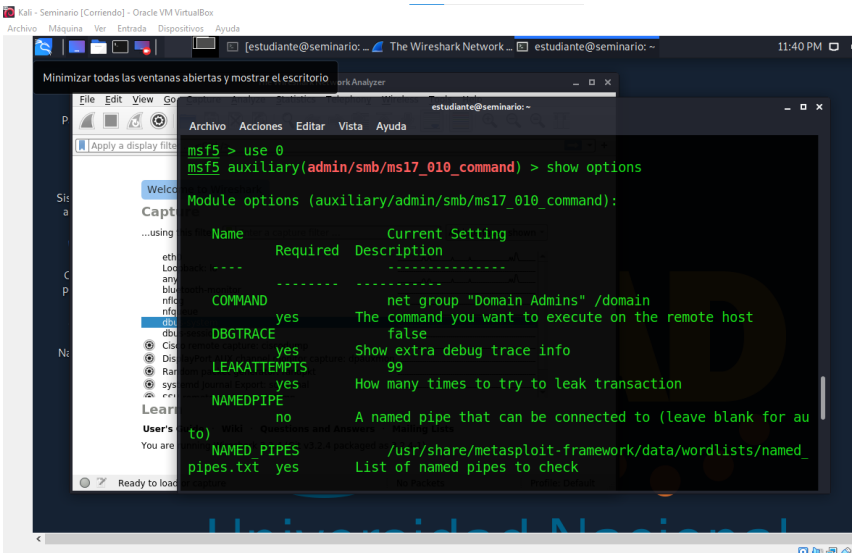
Figura 20 Se identifica la vulnerabilidad ms17-010



Fuente: Autoría Propia

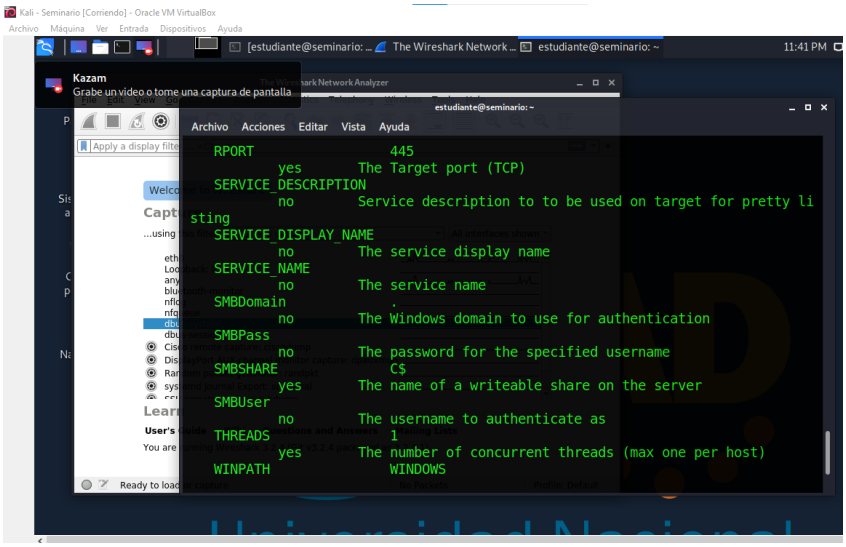
Indagamos más sobre las vulnerabilidades con el comando use 0 y al seleccionar escribimos show options y nos muestra las diferentes opciones.

Figura 21 Identificación información para atacar



Fuente: Autoría Propia

Figura 22 Se identifican las variables a configurar para el ataque

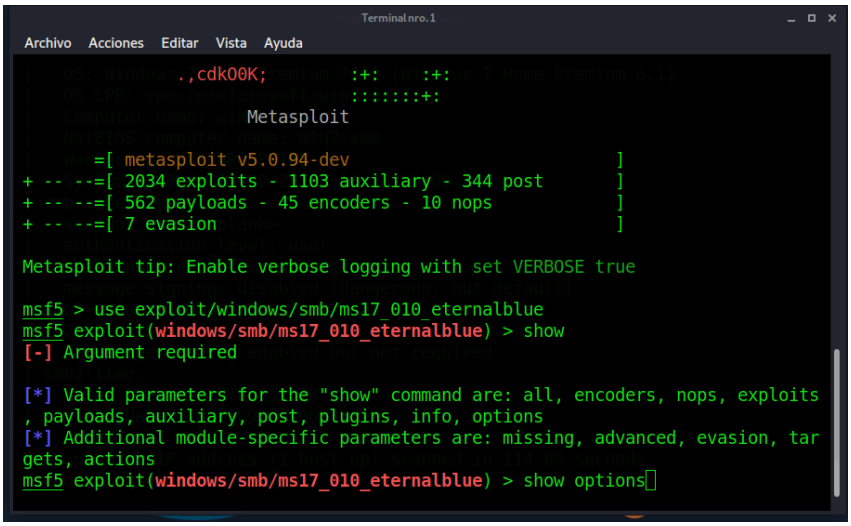


Fuente: Autoría Propia

En la siguiente figura se observa cómo vamos a acceder a la maquina Windows 7 por intermedio de la vulnerabilidad ms17-010, e así como desde el metasploit utilizamos el comando use expploit/Windows/smb/ms_017_eternalblue.

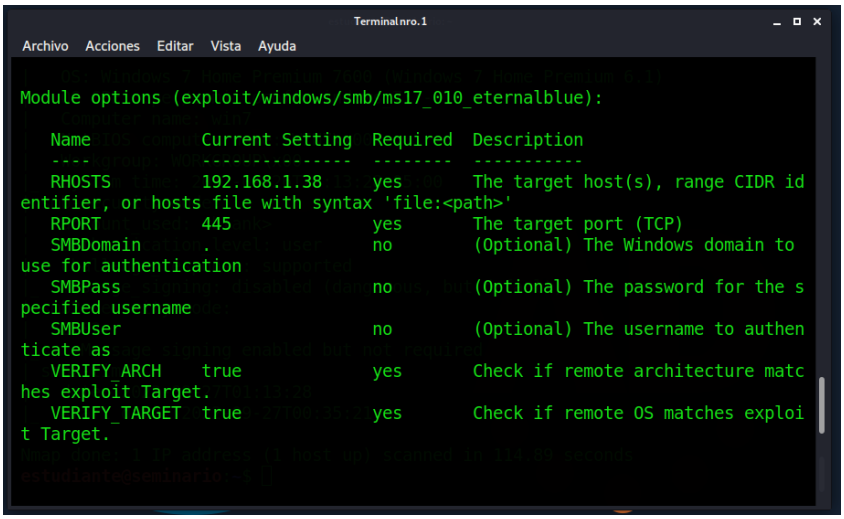
Posteriormente colocamos las diferentes variables para poder hacer el ataque como lo son:
SET LHOST Que corresponde a la IP del equipo Kali Linux desde donde realizaremos el ataque
SET LPORT que es el puerto por de la maquina Kali Linux de donde se realizará el ataque.
SET RHOSTS que corresponde a la maquina Windows 7 a donde realizaremos el ataque
SET RPORT Que es el puerto por donde se realizará el ataque a la maquina Windows y que se identificó en el escaneo de las vulnerabilidades que para este caso es el puerto 445.

Figura 23 Se ejecuta el comando use exploit



Fuente: Autoría Propia

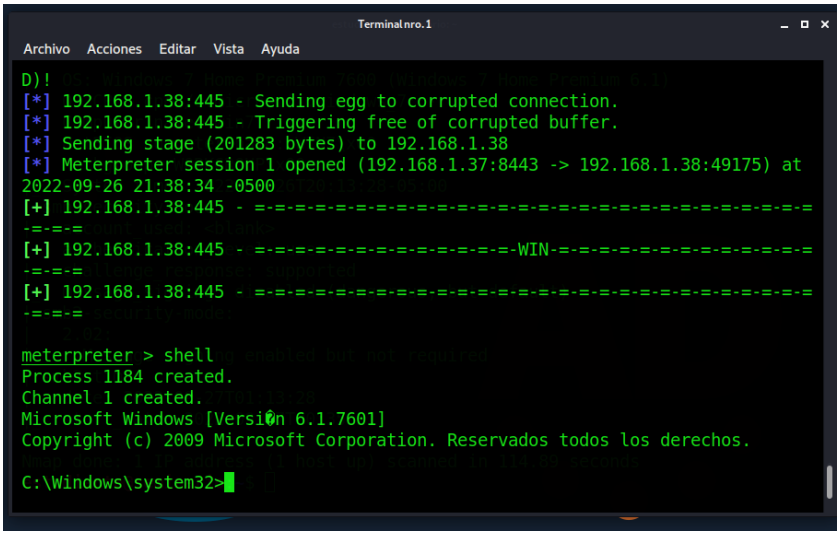
Figura 24 configuración RHOST RPORT



Fuente: Autoría Propia

Posteriormente lanzamos el ataque con el comando run y este dispara el ataque, accediendo al equipo Windows.[5]

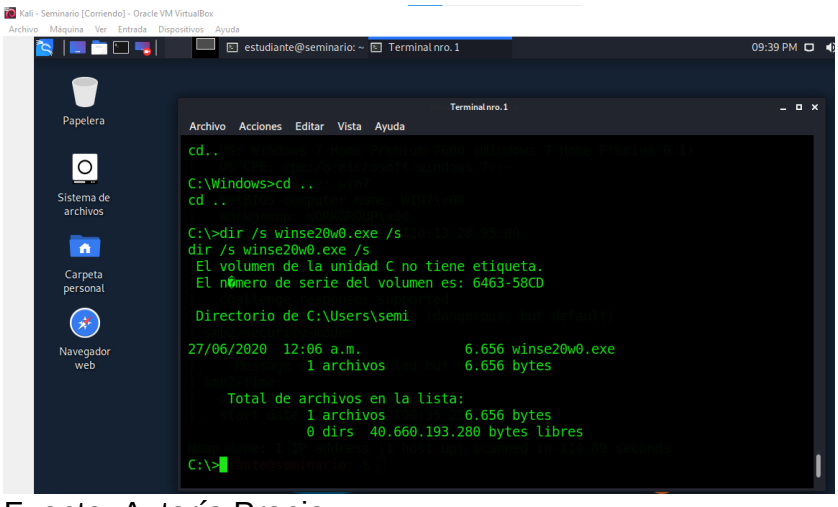
Figura 25 Ejecución del ataque run



Fuente: Autoría Propia

Ejecutamos el comando Shell y nos deja en el directorio de la maquina Windows en system32.

Figura 26 Acceso a la máquina Windows



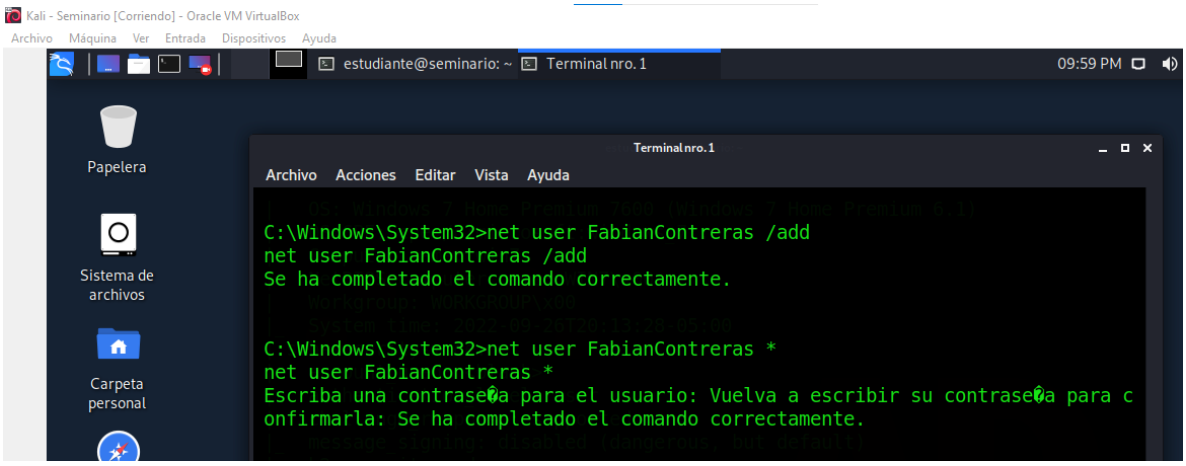
Fuente: Autoría Propia

[5] YOUTUE [Sitio Web] Conexión remota a windows 7 desde Kali Linux [Consulta: septiembre 21 de 2022] Disponible en: https://www.youtube.com/watch?v=fPqFylr3nCY

Estando en la maquina nos dirigimos a la raíz y desde allí ejecutamos el comando dir winse20w0.exe /s y él nos muestra que el archivo se encuentra ubicado en el directorio c:\users\semi.

Para crear el usuario en la maquina Windows 7 desde Kali Linux ejecutamos el comando Net user FabianContreras /add

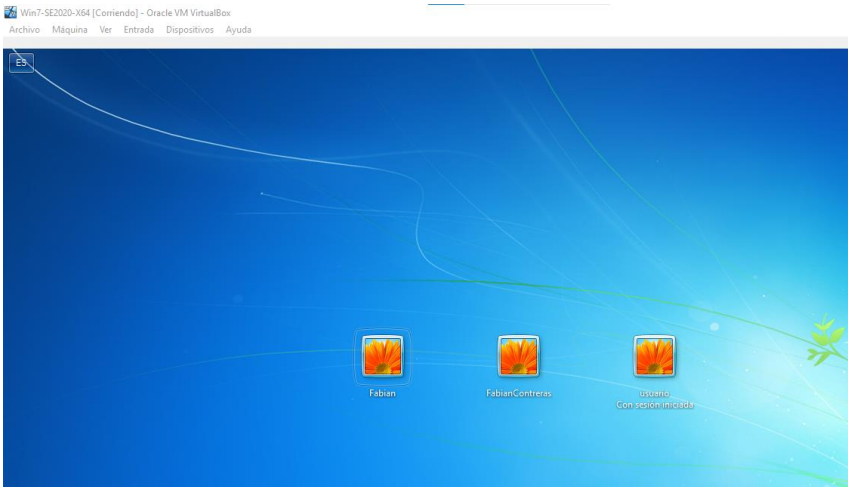
Figura 27 Creación usuario desde kali linux en Windows



Fuente: Autoría Propia

Validamos la creación desde el equipo Windows y observamos lo siguiente:

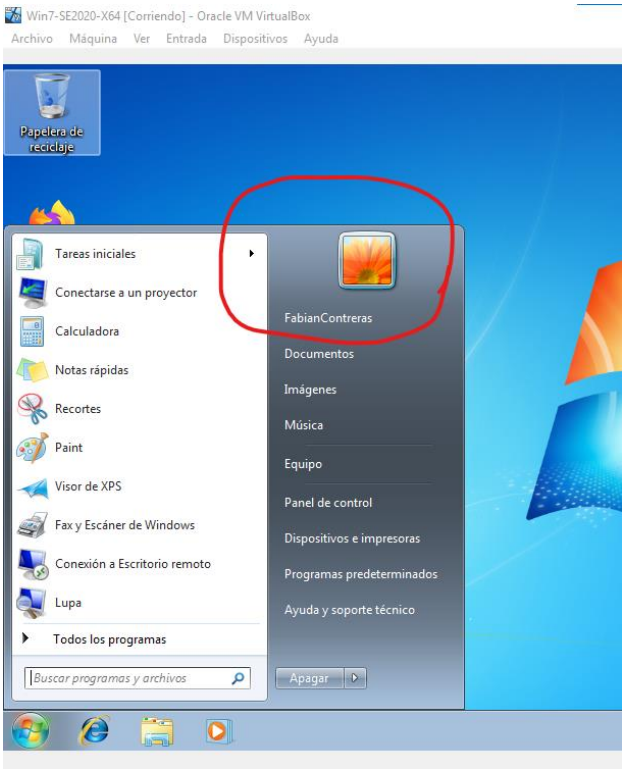
Figura 28 Validación usuario creado desde Linux



Fuente: Autoría Propia

Accedemos con el usuario creado y se observa lo siguiente:[6]

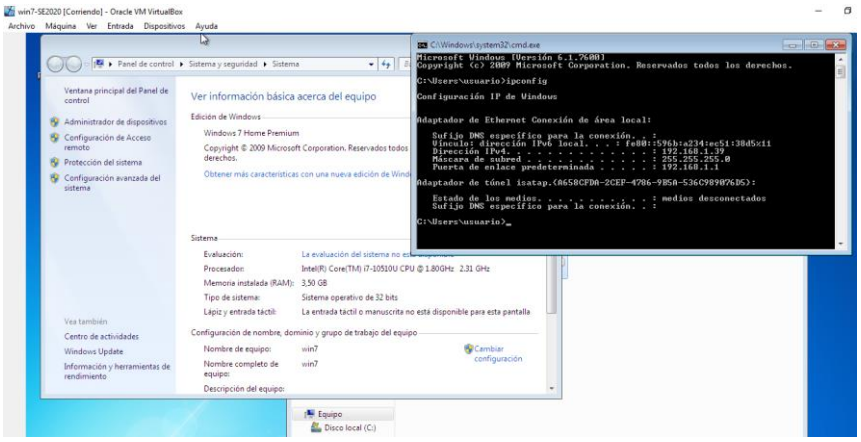
Figura 29 Acceso con usuario creado



Fuente: Autoría Propia

Windows 7 32 Bits

Figura 30 Máquina Windows 7 X86



Fuente: Autoría Propia

[6]YOUTUBE [Sitio web] Crear usuarios en Windows 7 en linea de comandos y de forma gráfica [Consulta 22 de septiembre de 2022] Disponible en: https://www.youtube.com/watch?v=YsAXuSnDiOg

Se generó la IP 192.168.1.39

Esta máquina no es la atacada ya que no permite por su sistema operativo en versión X86.

2.3.2 DATOS DEL ANEXO QUE APOYARON LA IDENTIFICACIÓN DEL FALLO DE SEGURIDAD

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows 7 X64.

al suministrar la información se describe que los equipos que pueden presentar la vulnerabilidad por sus características de sistema operativo son las maquinas Windows 7 X86 y X64, por ser este un sistema que ya no tiene soporte y a su vez un sin número de vulnerabilidades encontradas nos dan una primera pista del mismo, igualmente se habla de que no tienen los parches actualizados y que la última realizada fue en 2017 y que son factibles a que se presentara la vulnerabilidad descrita en CVE-2017-0144, igualmente se habla de que no tienen la actualización MS17-010. Adicionalmente dan una pista adicional que consiste en que el equipo vulnerado, presenta constantes errores de pantalla azul error de Windows de forma repetitiva.
Validando la vulnerabilidad CVE-2017-0144, en NIST y su base de datos de vulnerabilidad nacional hace referencia a que los atacantes pueden ejecutar código malicioso por intermedio de paquetes manipulados y es conocida como "vulnerabilidad de ejecución remota de código SMB de Windows"[7]
Adicionalmente la solución a esta vulnerabilidad fue liberada por Microsoft el 14 de marzo de 2017, como se observa en el anexo, la última actualización fue realizada el 5 de febrero de 2017.

2.3.3 HERRAMIENTAS UTILIZADAS PARA IDENTIFICAR LOS FALLOS

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 7”? ¿Qué puerto abre la aplicación específica en el anexo?

Para identificar las vulnerabilidades utilizamos nmap

Para realizar la explotación utilizamos metasploit

El puerto que se identifica y por el cual se realiza el ataque es el puerto 445/tcp

[7]NIST [Sitio Web] National Vulnerability Database [Consulta: septiembre 19 de 2022] Disponible en: https://nvd.nist.gov/vuln/detail/cve-2017-0144#vulnCurrentDescriptionTitle

2.3.4 EXPLICACIÓN DE LA AFECTACIÓN DEL ATAQUE

Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.

Una vez se alcanza a la maquina Windows 7, se pueden crear usuarios y dar permisos de administrador, permitiendo acceder con dicho usuario y realizar las configuraciones que se quieran y capturando la información para copias, borrados y alteraciones.

2.3.5 DOCUMENTAR CADA UNO DE LOS PASOS

Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Los pasos se encuentran documentados en los puntos anteriores donde se explica el comando utilizado y como se realzo el proceso de vulneración de la máquina.

2.4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

2.4.1 ACCIONES A REALIZAR EN LINEA FRENTE A UN ATAQUE

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.
Lo primero que se debe hacer cuando se identifica un posible ataque es reportar al equipo de atención de incidentes, los cuales realizarán un análisis preliminar con el fin de aislar los activos afectados con el fin de que este no se distribuya en los diferentes activos de la organización.
Una vez realizado esto se deben validar que los diferentes parches de seguridad se encuentren al día, una vez validados realizar los escaneos correspondientes con el fin de ejecutar las limpiezas correspondientes con el fin de aislar o eliminar la vulnerabilidad. Esto se debe hacer a nivel de toda la plataforma tecnológica, simultáneamente se debe advertir a los diferentes usuarios de la posible intrusión con el fin de evitar que esta se siga propagando.
Posteriormente el equipo de contención debe utilizar el kit de respuesta con el fin de indagar al detalle la forma como se realizado la intrusión y realizar la recuperación de la información y continuidad de la prestación de los servicios en toda la organización.
Para el punto anterior es importante contar con la información de la arquitectura de la organización con el fin de identificar la red, los diferentes activos de la organización, sus IPs, Puertos, servicios activos usuarios y privilegios de los mismos para con estos realizar un monitoreo de cada uno para validar su afectación o posible intrusión desde alguno de estos.

En caso de afectación de los activos se debe realizar la recuperación de backups, restauración de las imágenes de los servidores y todo lo relacionado para garantizar la continuidad de la prestación de los servicios.[8]

2.4.2 QUÉ MEDIDAS DE HARDENIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Redteam qué medidas de hardenización propondría para que el ataque no se repita?
Lo más importante para eliminar la vulnerabilidad frente a estos ataques es la de mantener el sistema operativo actualizado con las diferentes opciones entregadas
por la casa fabricante en este caso Microsoft, para este caso puntual se liberó la solución a esta vulnerabilidad con la actualización del 14 de marzo de 2017.
Adicionalmente con el fin de reducir aún más las vulnerabilidades de este equipo y a sabiendas que por temas de necesidad del aplicativo que no se puede ejecutar en otro sistema operativo actualizado se debería crear una DMZ con el fin de aislar esta aplicación frente a futuros ataques, igualmente se debe reducir el número de usuario que acceden a dicho aplicativo y reducir los permisos dependiendo del nivel de privilegios que deban tener los mismos.
Adicionalmente a esto se deben validar los diferentes puertos y servicios en ejecución con el fin de denegar los permisos a los que no se necesiten dejar habilitados para el funcionamiento de este aplicativo.
Se debe definir una política clara de revisión constante para este sistema operativo con el fin de monitorizar posibles ataques, al igual que una copia espejo de la misma, para en caso de afectación realizar una restauración del mismo.

2.4.3 DIFERENCIAS ENTRE UN EQUIPO BLUETEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

¿Describa con sus palabras las diferencias entre un equipo Blue team y un equipo de respuesta a incidentes informáticos?
El equipo blue team es el encargado de estar monitorizando los diferentes activos de la organización, utilizando diferentes metodologías apoyados en herramientas de hardware o software con el fin de encontrar movimientos o accesos fuera de lo común y que puedan ser un ataque a los activos, igualmente deben mantener al día las actualizaciones de las diferentes herramientas parches de las mismas utilizadas para reducir la vulnerabilidad de los activos.
Igualmente, el equipo blue team está en constante investigación de los diferentes ataques que se realizan en las diferentes bases de datos con el fin de evidenciar si esa vulnerabilidad se encuentra presente en la organización con el fin de realizar el parcheo o actualización de las plataformas para reducir la vulnerabilidad.

[8] KeepCoding. [Sitio Web]. Introducción al Red Teaming en Ciberseguridad. [Consulta: 27 septiembre 2022]. Disponible en https://www.youtube.com/watch?v=H2UM2sxpYIs

El equipo de respuesta a incidentes informáticos es el encargado de activar el plan de recuperación frente ataques informáticos con base en la metodología que tenga definida la organización, identificando la vulnerabilidad y por intermedio de las diferentes herramientas y acciones definidas aislar, identificar y restaurar en caso de ser necesario la configuración, información de los activos afectados con el fin de garantizar la continuidad de la prestación de servicios de la institución.
El equipo de respuesta a incidentes informáticos deberá entregar un informe de los hallazgos realizados con el fin de documentar las lecciones aprendidas y construir un base de datos de conocimiento que pueda ayudar frente a futuros ataques.[9]

2.4.4 SI LE INDICAN QUE DEBE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” USTED LO UTILIZARÍA PARA QUÉ FIN

¿Si dentro de un equipo Blue team le indican que debe trabajar con CIS “Center For Internet Security” usted lo utilizaría para qué fin?
EL CIS, es la recopilación de la mejor práctica con el fin de establecer la seguridad de internet de las organizaciones y dependiendo de los recursos y el grado de madurez de las mismas estas pueden utilizar diferentes niveles.
Yo la utilizaría para definir mi política de seguridad en la organización con el fin de identificar claramente los diferentes pasos a realizar con el fin de salvaguardar la seguridad de los diferentes activos en su exposición a internet.[10]

2.4.5 FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM

Explique y redacte las funciones y características principales de lo que es un SIEM
Por sus siglas en ingles SIEM (Security Information and Event Management), son programas encargados de realizer monitoreo constant a los activos de la organización con el fin de identificar posibles ataques o vulnerabilidades dentro de los mismos con el fin de reducir el ataque de los mismos, estos se encuentran en monitoreo constantes y dependiendo del tipo de software puede manejar IA que permitirá identificar comportamientos dentro de los activos para que al momento de encontrar alguna alteración informe inmediatamente a las personas indicadas y realice las acciones correspondientes frente a esta posible amenaza, igualmente esta información se almacena en una base de datos para posteriormente ser utilizada como base de conocimiento o lecciones aprendidas.
Dentro de sus funciones principales encontramos:

- Permite realizar la documentación del ataque en todos los momentos

[9] QUINTERO Fredy. Equipos estratégicos en ciberseguridad – red team & blue team [En Línea]. Seminario de grado. Universidad Abierta y a Distancia, 2021 [Consultado 18 septiembre 2022] Disponible en https://repository.unad.edu.co/bitstream/handle/10596/44163/mgleivap.pdf?sequence=1&isAllowed=y
[10] Telefonica Tech [Sitio web]. ElevenPaths, radical and disruptive innovation in security. Seguridad Defensiva vs Seguridad Ofensiva por Claudio Caracciolo y Jorge Rivera. [Consulta: 23 de septiembre de 2022]. Disponible en: https://www.elevenpaths.com/es/noticias-y-eventos/elevenpaths-talks/seguridad-defensiva-vs-seguridad/

- Suministrar una base de conocimiento con el fin de afrontar eficientemente el ataque.
- Identificar si se está realizando un ataque o es un movimiento normal dentro de los activos.
- Monitorización central de las diferentes amenazas y los activos.[11]
- Generar las alertas ante los responsables en caso de movimientos fuera del estándar.

2.4.6 Defina Por Lo Menos 3 Herramientas De Contención De Ataques Informáticos

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

2.4.6.1 Winpatrol

Este programa se instala en la maquina Windows y se encarga de validar las posibles alteraciones originadas por spyware o adware, no solo logra identificar algunos spyware que pasaron por el antivirus si no que adicionalmente monitoriza los diferentes programas con el fin de validar su instalación y si son pertinentes para el correcto funcionamiento de su máquina Windows.[12]3

2.4.6.2 Snort

Es catalogado como un software NIDS (Network Intrusion Detection System) por sus siglas en ingles basado en protocolos, anomalías y firmas, las diferentes reglas que se definan se deben alinear con la política de la organización y se debe definir en qué parte se configurarán estas reglas dependiendo de la vulnerabilidad de los activos.[13]

2.4.6.3 Security Onion

Este es basado en el sistema operativo Linux es uno de los más populares para la monitorización de los activos en las diferentes empresas, cuenta con un sinnúmero de funcionalidades que permiten monitorizar cualquier anomalía en los mismos.[14]

---

[11] 1 ManageEngine [Sitio Web] Qué son y cómo implementar los Controles de CIS (CIS Controls) [Consulta: 30 de septiembre de 2022] Disponible en: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

[12] VIDEOTUTOPRIAL.RO [Sitio Web] WinPatrol, nos avisa cuando suceden cosas desagradables en la PC [Consulta: 01 de octubre de 2022] Disponible en: https://es.videotutorial.ro/winpatrol-o-aplicatie-care-ne-ajuta-sa-intelegem-ce-se-intampla-in-calculator-tutorial-video/

[13] CIBERSEGURIDAD.BLOG [Sitio Web] Reglas SNORT , detección de intrusos y uso no autorizado [Consultado: septiembre 30 de 2022] Disponible en: https://ciberseguridad.blog/reglas-snort-deteccion-de-intrusos-y-uso-no-autorizado/

[14]2 Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63).
http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

CONCLUSIONES

Se conocieron las actividades a realizar por parte de los equipos Blue Team y Red Team enmarcados en la normatividad y principios éticos, apoyándolos con herramientas tecnológicas y metodologías que permiten minimizar las vulnerabilidades de los activos de las organizaciones.

Se identificaron diferentes actividades para aplicar en los equipos de Blue Team y Red Team enmarcadas en la normatividad y principios éticos vigentes, que permitirán garantizar la aplicación de buenas prácticas en dichos equipos.

Se conocieron diferentes herramientas que apoyan los equipos Blue Team y Red Team permitiendo monitorizar e identificar intrusiones que permiten el seguimiento, control y mitigación de incidentes o vulnerabilidades

RECOMENDACIONES

Todas las organizaciones y su área de tecnología, deben maximizar sus esfuerzos en la definición de estrategias que fortalezcan su seguridad informática en pro de garantizar los pilares de la misma como lo son la confidencialidad, integridad y disponibilidad.[15]

Implementar dentro de sus equipos de auditoria interna de ciberseguridad los equipos de Blue Team y Red Team, si bien estos pueden ser subcontratados con una empresa con amplio reconocimiento y con principios éticos elevados. Se debe propender por identificar las vulnerabilidades que posee la organización y así reducir el riesgo de que estas se materialicen.

Las diferentes empresas y organizaciones deben definir mecanismos que garanticen el continuo monitoreo de las infraestructuras críticas de la organización con el fin de reducir el riesgo. Esto se puede hacer con equipos permanentes de Blue Team y Red Team o con una compañía que se dedique a estas labores.[16]

Se debe garantizar una política de cultura de la ciberseguridad con el fin de capacitar a los diferentes usuarios, internos como externos, sobre los riesgos a los que pueden estar expuestos por ataques informáticos y las medidas que deben tomar para minimizarlos.

Se debe contextualizar a las personas de los equipos de TI y de ciberseguridad de la importancia y el aporte que pueden brindar los equipos blue Team y Red Team con la identificación de vulnerabilidades y sus posibles soluciones para así dar garantía en la continuidad de la prestación de los servicios por parte de las organizaciones.

Definir un escritorio de trabajo con los equipos, sistemas operativos, herramientas y frameworks necesarios para la realización de los diferentes testeos y pruebas de ataques de vulnerabilidades encontradas en las bases de datos o en los activos de la organización.

[15] Global Cibersecurity [Sitio web]. Global Cibersecurity Index 2018 [Consulta: 20 de septiembre de 2022] Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[16] IDB. [Sitio web]. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.[Consulta 8 de septiembre de 2022] Disponible: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

BIBLIOGRAFÍA

CIBERSEGURIDAD [Sitio Web] Que e Metasploit framework y como funciona [Consulta 1 de septiembre de 2022] Sitio web: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Global Cibersecurity [Sitio web]. Global Cibersecurity Index 2018 [Consulta: 20 de septiembre de 2022] Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Hiberus blog [Sitio Web] Pentesting con OWASP Fases y Metodología [Consulta 1 de septiembre de 2022] Sitio web: https://www.hiberus.com/crecemos-contigo/pentesting-owasp-fases-metodologia/

IDB. [Sitio web]. Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.[Consulta 8 de septiembre de 2022] Disponible: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

IEEE Xplore. [Sitio web]. A red team blue team approach towards a secure processor design with hardware shadow stack [Consulta: 15 de septiembre 2022] Disponible: http://ieeexplore.ieee.org/stampPDF/getPDF.jsp?tp=&arnumber=8031545&ref=aHR0cHM6Ly9pZWVleHBsb3JlLmllZWUub3JnL2RvY3VtZW50LzgwMzE1NDU=

INCIBE [Sitio Web]. RedTeam, El hacking en otra dimensión [Consulta: 28 septiembre 2022]. Disponible en: https://www.youtube.com/watch?v=__PZogK-y-Q.

Karpesky [Sitio Web], Que es la Ciberseguridad [Consulta: 27 de septiembre de 2022], Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

KeepCoding. [Sitio Web]. Introducción al Red Teaming en Ciberseguridad. [Consulta: 27 septiembre 2022]. Disponible en https://www.youtube.com/watch?v=H2UM2sxpYIs

Leyes desde 1992 Vigencia expresa y control de constitucionalidad [Sitio WEB]Ley 1273 de2009 [Consulta: 29 de agosto de 2022] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

NIST [Sitio Web] National Vulnerability Database [Consulta: septiembre 19 de 2022] Disponible en: https://nvd.nist.gov/vuln/detail/cve-2017-0144#vulnCurrentDescriptionTitle

QUINTERO Fredy. Equipos estratégicos en ciberseguridad – red team & blue team [En Linea]. Seminario de grado. Universidad Abierta y a Distancia, 2021 [Consultado 18 septiembre 2022] Disponible en

https://repository.unad.edu.co/bitstream/handle/10596/44163/mgleivap.pdf?sequence=1&isAllowed=y

Telefonica Tech [Sitio web]. ElevenPaths, radical and disruptive innovation in security. Seguridad Defensiva vs Seguridad Ofensiva por Claudio Caracciolo y Jorge Rivera. [Consulta: 23 de septiembre de 2022]. Disponible en: https://www.elevenpaths.com/es/noticias-y-eventos/elevenpaths-talks/seguridad-defensiva-vs-seguridad/

Unir la universidad en internet [Sitio Web], Red Team, Blue Team y Purple Team, ¿Cuáles son sus funciones y diferencias?, [Consulta: 01 de septiembre de 2022], Disponible en: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

YOUTUBE [Sitio web] Crear usuarios en Windows 7 en línea de comandos y de forma gráfica [Consulta 22 de septiembre de 2022] Disponible en: https://www.youtube.com/watch?v=YsAXuSnDiOg

YOUTUBE [Sitio Web] Conexión remota a windows 7 desde Kali Linux [Consulta: septiembre 21 de 2022] Disponible en: https://www.youtube.com/watch?v=fPqFylr3nCY

ANEXOS

Anexo A. Video de sustentación

https://youtu.be/DAo7GgWtGY4

Anexo B. Prueba Turniting