Capacidades Técnicas, Legales y de Gestión para equipos Blueteam y Redteam

JULIO MIGUEL PEREZ HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTACIA -UNAD

ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

CARTAGENA

2021

Capacidades Técnicas, Legales y de Gestión para equipos Blueteam y Redteam

JULIO MIGUEL PEREZ HERNANDEZ

Informe Técnico para optar por el título de Especialista en Seguridad Informática

Asesor

ING ALEXANDER LARRAHONDO N

Director

M.Sc. John F. Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTACIA -UNAD

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA-ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team.

CARTAGENA

2021

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Cartagena, 10 de Octubre de 2021

INDICE

Contenido Pag

Lista de Figuras **Pag**

Lista de Tablas **Pag**

Lista de Anexos **Pag**

GLOSARIO

BlueTeam: “Los Blue Team son equipos multidisciplinares de expertos en ciberseguridad especializados en analizar el comportamiento de los sistemas de una empresa y estudiar cómo se comportan sus usuarios y equipos para poner al descubierto de forma rápida cualquier incidente que pueda haber pasado inadvertido para el resto de sistemas de seguridad”[1].

Redteam:” Es un equipo humano, que realiza ataques (siempre controlados) a un objetivo, que ha sido definido anteriormente por parte del cliente y bajo un contrato de confidencialidad y de alcance del mismo”[2].

Pentesting: “Es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas”[3].

Vulnerabilidad:” Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma”[4].

CVE: “Son los puntos vulnerables y las exposiciones comunes (CVE) conforman una lista de fallas de seguridad informática que se encuentra disponible al público en general”[5].

---

[1] It Digital security. 30 de mayo de 2018. ¿Qué es un Blue Team y cómo trabaja? [en línea]. Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja.

[2] ESIC BUSINESS & MARKETING SCHOOL. 01 de febrero de 2018. Red team: qué es, estrategias y ejemplo de un caso real. [en línea].Disponible en:https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

[3] Incibe. 04 de Julio de 2019. ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. [en línea]. Disponible en:https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

[4] Incibe.20 de marzo de 2017. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [en línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

[5] Red hat. 08 de octubre de 2021. El concepto de CVE. [en línea]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve.

Phishing:" Consiste en el envío de mensajes, bien a través del correo electrónico, de SMS (conocido como smishing), mensajería instantánea o, incluso, de redes sociales, en los que los delincuentes cibernéticos suplantan la identidad de cualquier organización conocida para obtener nuestra información más confidencial (contraseñas, datos bancarios, etc.) incitándonos a hacer clic en un enlace que redirige a una página falsa"[6].

Malware:" Palabra compuesta por «malicioso» y «software», es un programa o aplicación informática que se ejecuta en los equipos de los usuarios con la intención de robar información o tomar el control del sistema"[7].

Vishing (Voice phishing):" A un tipo de estafa en la cual el atacante se comunica con la víctima, por teléfono o mensaje de voz, haciéndose pasar por alguien más"[8].

Metaexploit: "Es un Framework desarrollado para ejecutar exploits de manera remota contra un objetivo en particular. Un exploit es un trozo de código el cual permite explotar ciertas vulnerabilidades"[9].

Firewall: "Es un programa informático o un hardware que brinda protección a una computadora (ordenador) o a una red frente a intrusos"[10].

---

[6] Iberdrola, S.A. 08 de octubre de 2021. 'Phishing': un clic marca la diferencia. [en línea]. Disponible en: https://www.iberdrola.com/innovacion/phishing

[7] BORRMART, S.A. ¿Qué es el malware? Tipos y maneras de evitar ataques de este tipo. [en línea]. Disponible en: https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html.

[8] Jaimovich, D. 11 de mayo de 2021. Qué es el "vishing", la estafa telefónica de moda utilizada para robar datos del homebanking. [en línea]. Disponible en https://www.infobae.com/america/tecno/2021/05/11/que-es-el-vishing-la-estafa-telefonica-de-moda-utilizada-para-robar-datos-del-homebaking/

[9] Esteban, S. 07 de febrero de 2016. Metasploit: Atacando a Windows. [en línea]. Disponible en: https://backtrackacademy.com/articulo/metasploit-atacando-a-windows

[10] Merino, J. P. 01 de enero de 2017. Definición de Firewall. [en línea]. Disponible en: https://definicion.de/firewall/

RESUMEN

En el desarrollo del presente informe nosotros como a través de los distintos escenarios planteados cuales son las acciones que se deben realizar desde el punto de vista técnico y legal, ya que es algo de lo que hay que tener muy en cuenta para el análisis y contexto de cada una de las situaciones que se plantearon en el desarrollo del seminario.

Por medio de las distintas herramientas de pentesting pudimos explorar las fallas en los distintos sistemas informática, además de investigar el origen y causa de los mismos.

INTRODUCCION

En el presente informe técnico vamos a conocer o a dejar en evidencia los aspectos que se desarrollaron entorno a los equipos Redteam y Blueteam, dentro de la organización planteada como ejemplo y de cómo esos equipos son fundamentales para mejorar la ciberseguridad en cualquier organización ya sea pública o privada.

Como estamos en la actualidad la mayoría de las personas de una u otra forma interactuamos en el ciberespacio ya sea para nuestras actividades académicas o profesionales y de cómo es de escarnio público los peligros y riesgos que encontramos en el día a día por medio de estos equipos especializados podemos lograr la mejor contención que se puede obtener dentro de las empresas, basándose en buenas prácticas de seguridad de la información y en herramientas de software y hardware que nos ayudan a contener o en ciertos caso evitar las vulneraciones a los sistemas informáticos.

1 DEFINICION DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad los delitos informáticos van en alza en todo el mundo y a raíz de todos los cambios que se dan día a día y de las brechas de seguridad que se encuentran o localizan en los Sistemas informáticos sin duda alguna son los motivante para buscar las mejores practica y minimizar el impacto en las organizaciones.

Por lo cual la empresa WhiteHose Security diseño anexos con situaciones que se les presentan en la empresa por lo cual nosotros como expertos debemos tratar de ayudarlos a resolver.

1.2 PLANTEAMIENTO DEL PROBLEMA

¿Como podemos mejorar desde el punto de vista legal y técnico las estrategias y herramientas para los equipos Redteam y Blueteam?

1.3 FORMULACION DEL PROBLEMA

En virtud de lo que se requiere en el presente informe vamos a analizar a través de los distintos escenarios que se plantearon el desarrollo del seminario empezando las herramientas técnicas a utilizar, la legislación aplicable en Colombia , la realización de pruebas de intrusión y luego ver de qué forma podemos contener los ataques se presentaron en las distintas situaciones planteadas, para así permitirnos llegar a conclusiones y sugerencia para por llegar a una óptima aplicación de las estrategias de los equipos Redteam y Blueteam.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Conocer con el informe las capacidades técnicas y legales con que cuentas los equipos Blueteam y Redteam, para hacer frente a los ataques de los ciberdelincuentes con el fin de lograr la mejor defensa a las vulnerabilidades y lograr una adecuada defensa.

2.2 OBJETIVOS ESPECÍFICOS

1. Evaluar desde el punto de vista ético y legal las acciones de los equipos Blueteam y Redteam.
2. Realización de Prueba de Pestesting para demostración de vulnerabilidades en la empresa WhiteHose Security.
3. Descripción, análisis de medidas de contención y de hardenizacion ante ataques informáticos.

3 JUSTIFICACIÓN

Actualmente sin duda alguna hemos visto como el auge de la utilización de los medios digitales para trabajar, estudiar, realizar compras, pagos y transacciones bancarias han subido exponencialmente en el mundo, por lo cual las empresas requieren o es casi una necesidad tener medidas de ciberseguridad eficientes, ya que con un simple antivirus no sería suficiente.

En la actualidad hay muchas empresas que todavía es la hora y no le dan importancia al tema de la ciberseguridad, en Colombia las principales modalidades a corte de 2020 de los incidentes reportado al caí virtual de la policía son[11]:

- ✓ Estafa por compra y/o venta de productos - 2.391
- ✓ Phishing -1.753
- ✓ Suplantación de identidad -1.776
- ✓ Vishing (Voice phishing) -1.087
- ✓ Malware -1.045
- ✓ Amenazas a través de redes sociales -972
- ✓ Injuria y/o calumnia a través de redes sociales -676

Por lo cual vemos que es necesario que las empresas deben estar preparadas para afrontar los peligros que se encuentran en el ciberespacio.

[11] Policía nacional. 08 de noviembre de 2020. [en línea]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

4 MARCO DE REFERENCIA

4.1 MARCO TEÓRICO

En razón del presente informe debemos tener claro las tendencias que se están presentado en el mundo como son las distintas amenazas y vulnerabilidades que más se registran en la actualidad, por ejemplo, en el 2020 las 5 principales vulnerabilidades fueron[12]:

- ✓ ZEROLOGON (CVE-2020-1472).
- ✓ CITRIX ADC / GATEWAY / SDWAN WAN-OP (CVE-2019-19781).
- ✓ VPN SSL SEGURA DE PULSE CONNECT (CVE-2019-11510).
- ✓ 4. FORTINET FORTIGATE SSL VPN (CVE-2018-13379).
- ✓ 5. F5 BIG-IP (CVE-2020-5902).

Analizando las tendencias mundiales donde los equipos de ciberseguridad de las empresas deben estar preparados para cualquier intento de vulneración por eso es común que se mencionen el equipo BlueTeam y RedTeam, cuando hablamos de ciberseguridad y el desarrollo de este informe vemos de manera practica como actúan.

[12] Redacción CIO México. 20 de enero de 2021. ¿Cuáles fueron las principales ciberamenazas en 2020?, una retrospectiva. [en linea]. Disponible en: https://cio.com.mx/cuales-fueron-las-principales-ciberamenazas-en-2020-una-retrospectiva/

4.2 MARCO LEGAL

Tabla 1. Normatividad Aplicable en Colombia

Nombre	Descripción	Link de Documento
Documento Conpes 3854 de 2016	Política Nacional de Seguridad Digital	https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf
Ley Estatuaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la ley 1581 de 2012	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las	http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

	comunicaciones, entre otras disposiciones	
Decreto 1078 de 2015	Decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones.	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888
Ley Estatutaria 1266 del 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones	http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
Decreto 2693 de 2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras	https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51198

	disposiciones"	

Fuente: el autor

5 METODOLOGIA

Para la comprensión del presente informe vamos a iniciar conociendo la estructura que se requirió para realizar las practicas o casos, como además ir conociendo la legislación colombiana en cuanto a los delitos informáticos, tener claridad del código de ética de los ingenieros, conocer las etapas del pestenting y de las herramientas con que se cuenta para poder realizarlos y las herramientas de contención que podemos utilizar.

Todo esto basados en la metodología de casos de uso de acuerdo a los anexos que fueron presentados por la empresa WhiteHose Security.

6 DESARROLLO DEL INFORME

6.1 DESARROLLO OBJETIVO ESPECÍFICO 1

En el país contamos con herramientas legales y constitucionales por medio de las cuales están tipificados los delitos informáticos y la protección de datos personales en nuestro país, como es la ley 1273 de 2009, Ley Estatuaria 1581 de 2012 y Decreto 1377 de 2013.

Donde podemos encontrar los artículos que tipifican los castigos contra los atentando contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.

Donde tácitamente castigan los accesos no autorizados a un sistema informático, el obstaculizar los sistemas informáticos, interceptar informacion,realizar daños , el uso de software malicioso, la suplantación de sitios web, los hurtos por medios electrónicos, donde esgrimen condenas desde 48 meses hasta 120 meses dependiendo de la gravedad del delito, por lo cual estas son herramientas que podría contar el equipo para denunciar a los ciberdelincuentes los cuales se podría enfrentar a las penas anteriormente descritas.

Pero sin duda alguna estos hechos van de la mano con conductas punibles si se tratan de ingeniero en su ejercicio profesional por lo cual la entidad rectora en nuestro país es COPNIA, donde expresa en los deberes como profesionales “Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones”[13].

En lo que respecta a la ley de datos personales sin duda es una herramienta útil para la debida protección legal de los datos de las personas que en esta brinda los

[13] COPNIA. 09 de octubre de 2021. Código de ética. [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

principios que deben cumplir las personas naturales o jurídicas para el tratamiento, manipulación, custodia y divulgación de la cual es responsable.

Por medio del decreto 1377 de 2013, este reglamente la ley 1581 donde tipifican en algunos lo siguiente:

1. Aviso de privacidad: “Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales”[14].

2. Dato público: “Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva”[15].

3. Datos sensibles: “Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido

[14] Senado de la Republica. 27 de 06 de 2013. [en línea]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

[15] Senado de la Republica. 27 de 06 de 2013. [en línea]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos" [16].

4. Transferencia: "La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país" [17].

5. Transmisión: "Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable" (Senado de la Republica, 2013).

Es de anotar que el desarrollo de las actividades nos permitió analizar el caso particular del contrato de trabajo establecido por la compañía donde sin duda alguna insta al profesional a la falta de ética y del ejercicio profesional con el animo de que sea cómplice y a la vez responsable de la información que se obtuvo por los distintos medios ilegales tratando de motivarlo con un alto honorario, pero esto con el fin de que asumiera todas las responsabilidades.

6.2 DESARROLLO OBJETIVO ESPECÍFICO 2

Como se expresó en la metodología usada para el desarrollo del seminaria a través de escenarios supuestos de situaciones que se podrían dar en el contexto de las empresas como es el tener equipos vulnerables en la red y de que nosotros como

[16] Senado de la Republica. 27 de 06 de 2013. [en línea]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

[17] Senado de la Republica. 27 de 06 de 2013. [en línea]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

profesionales en seguridad podríamos en primera instancia indagar y realizar todas las fases del pestesting como son:

a. Recopilar información

En esta etapa inicial trataremos de conocer lo más que podamos la empresa, la red, los sistemas informáticos que posee la empresa o el objetivo del pestenting, con el fin de saber por dónde nos vamos a ubicar o tratar de validar los baches de seguridad.

En esta fase podemos usar herramientas como es Nmap para escanear los puertos de la red, FOCA[18] para conseguir la mayor cantidad de metadatos para así lograr recopilar la mayor cantidad de información que nos pueda servir para nuestras pruebas.

b. Buscar vulnerabilidades

En esta fase vamos a tomar como base la información recopilada y manualmente o con herramientas automáticas buscamos las vulnerabilidades; aquí podemos usar herramientas como Nessus o Acunetix.

c.Explotación de las Vulnerabilidades

Luego de haber identificado las vulnerabilidades de los distintos sistemas o en la red de datos, se procede a ingresar o aprovecharse de la información para hacer cambios o extraer información de esas brechas encontradas.

Podríamos usar herramientas como SQL inyector o Metasploit.

d.Post-Explotación

Luego de lograr el acceso a los sistemas en esta etapa demostramos los ingresos, podemos cambiar los roles o privilegios de los usuarios para que la persona o la empresa tenga la invidencia de las falencias de seguridad de sus sistemas o redes.

[18] Telefónica Cybersecurity & Cloud Tech, S.L.U. 09 de octubre de 2021. [en línea]. Disponible en:https://www.elevenpaths.com/es/innovacion-laboratorio/tecnologias/foca

e. Informé

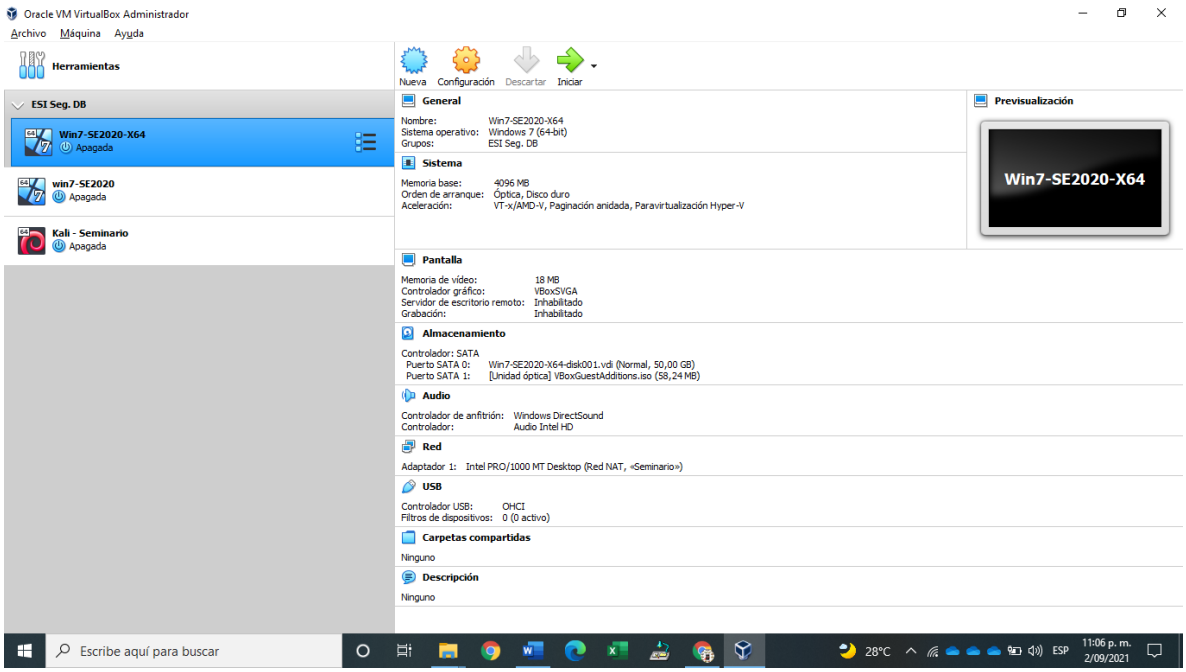
Al final de las etapas, se entregará como producto un informe de las vulnerabilidades encontradas, evidenciar las brechas de seguridad encontradas, evidenciar las principales falencias y recomendar las acciones a realizar, estos informes pueden ser uno técnico y otro más gerencial donde se exponga de manera clara lo evidenciado.

En primera instancia debemos tener un espacio virtual de trabajo el cual esta constituido de la siguiente forma:

1. Maquina Kali Linux
2. Maquina Windows 7 32 bits
3. Maquina Windows 7 64 bits

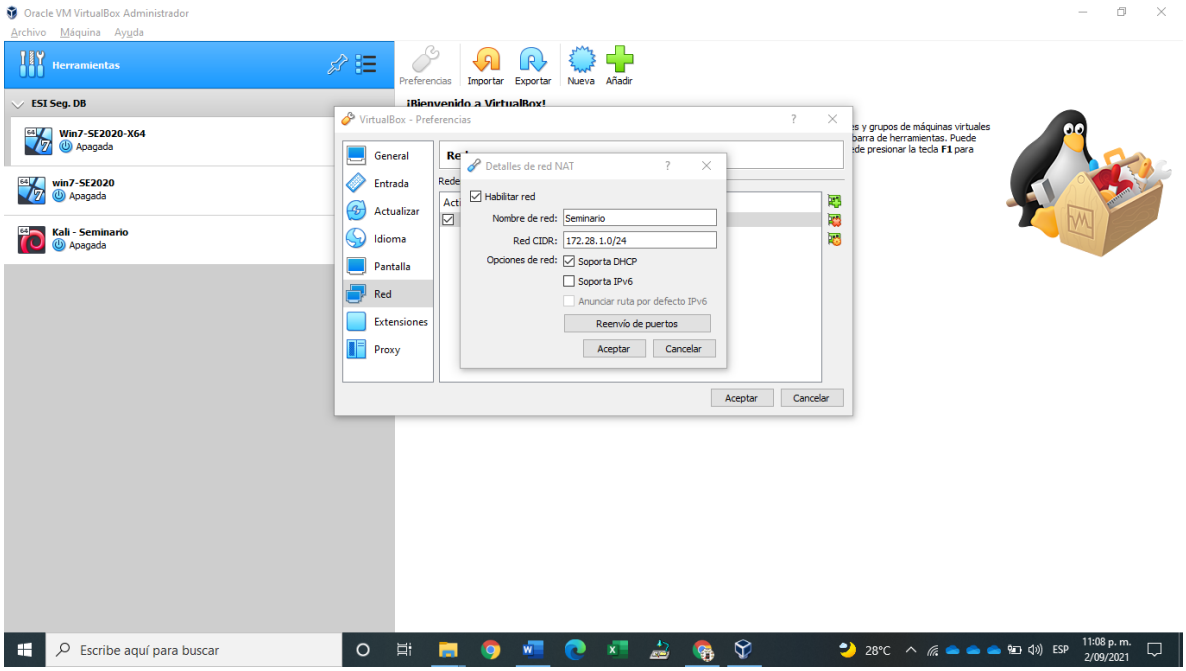
Las cuales van a estar conectadas en un mismo segmento de red

Ilustración 1 Estructura virtual de Pruebas pestesting



Fuente: el autor

Ilustración 2 Configuración segmento de red

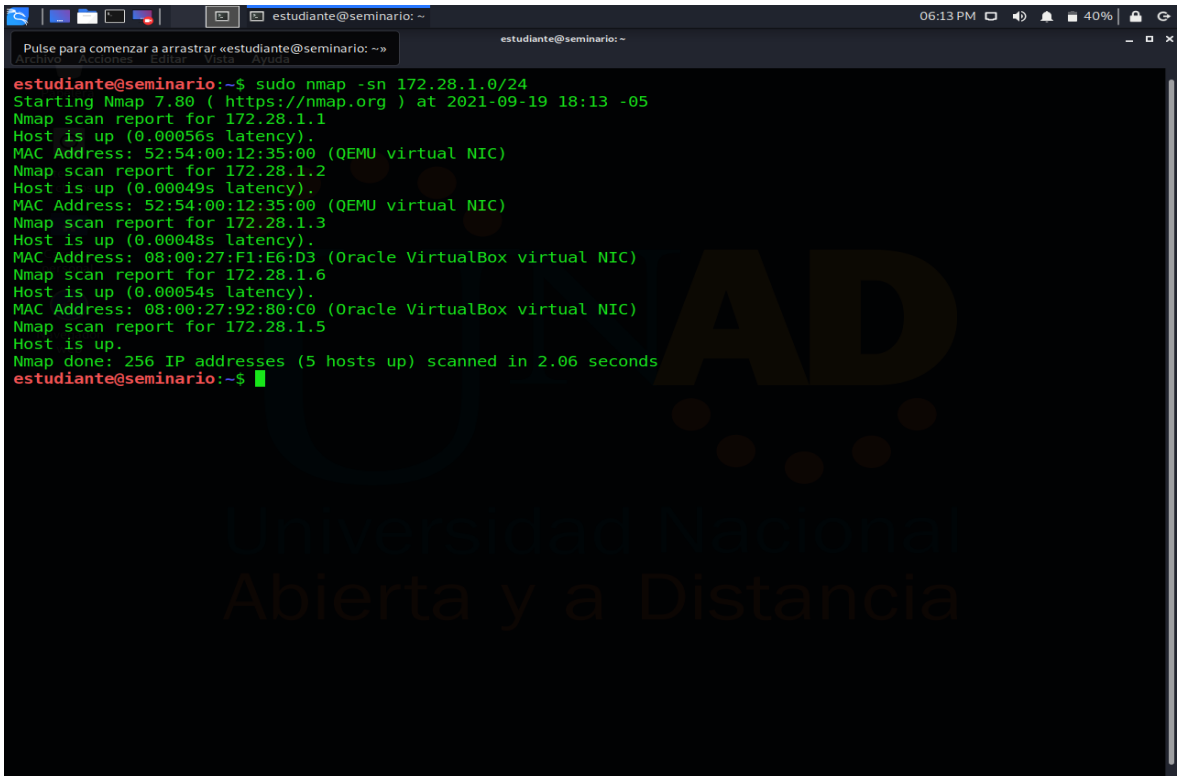


Fuente: el autor

Al iniciar el desarrollo de las actividades de Pestesting se procede de acuerdo a las etapas o fases donde se evidencia en la etapa de recopilación de información los equipos que se encuentran en la red de la empresa donde se indaga de la siguiente forma:

Inicialmente buscamos los hosts activos dentro de nuestra red por medio de nmap a través del siguiente comando

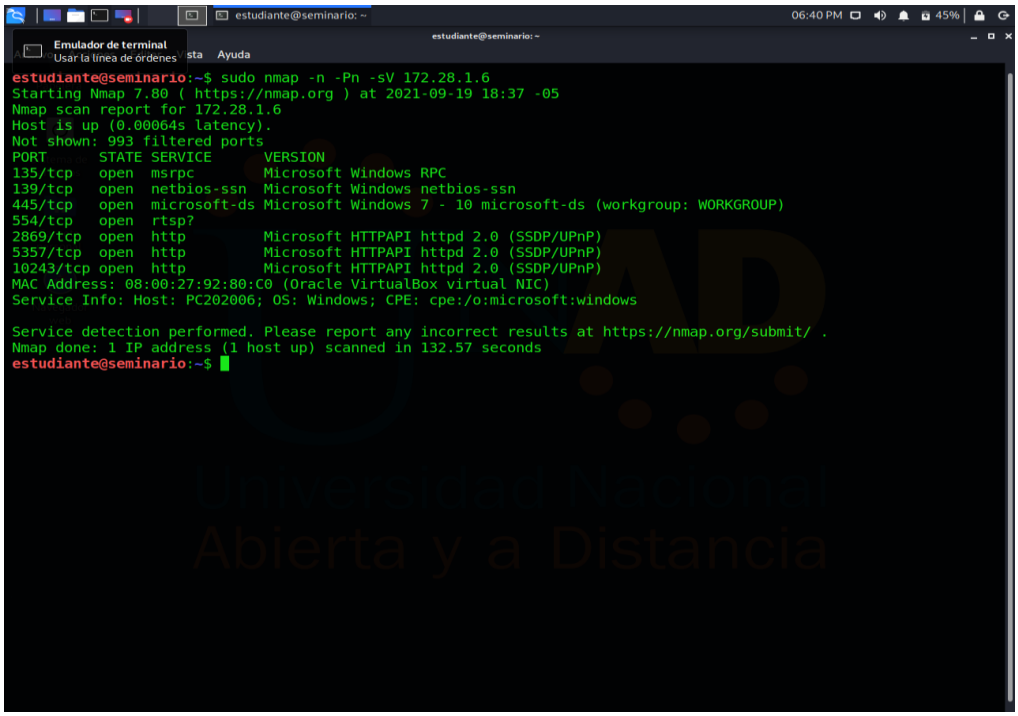
Ilustración 3 Equipos activos en la red



Fuente: el autor

Luego de la realización de la recopilación de la información de los equipos que se encontraron en la red se procede a uno a uno en buscar las vulnerabilidades que estos podrían presentar para así tratar de explorarlas a través de los distintos comandos y utilidades que podemos usar en Kali Linux.

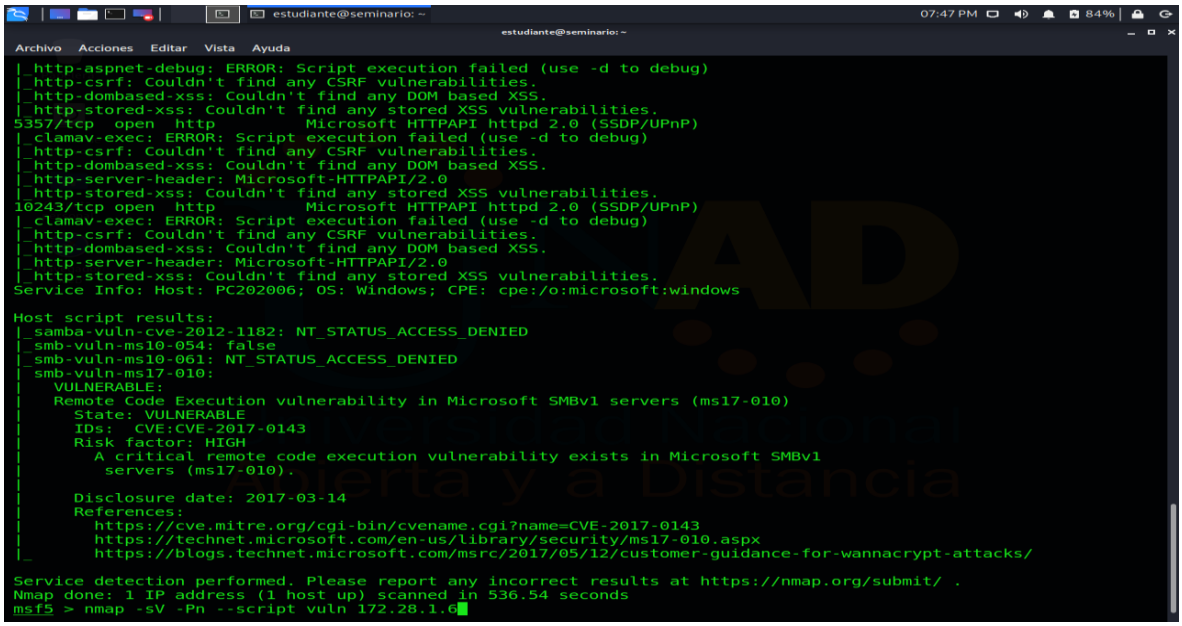
Ilustración 4 Puertos abiertos



Fuente: el autor

Luego de conocer los puertos vamos a ver que vulnerabilidades puede presentar la maquina la cual es el objetivo a través de nmap -sV -Pn --script vuln 172.28.1.6, por la cual nos muestra una vulnerabilidad la CVE-2017-0143 la cual permite a los atacantes remotos ejecutar código arbitrario a través de paquetes diseñados, también conocidos como "Vulnerabilidad de ejecución remota de código SMB de Windows"

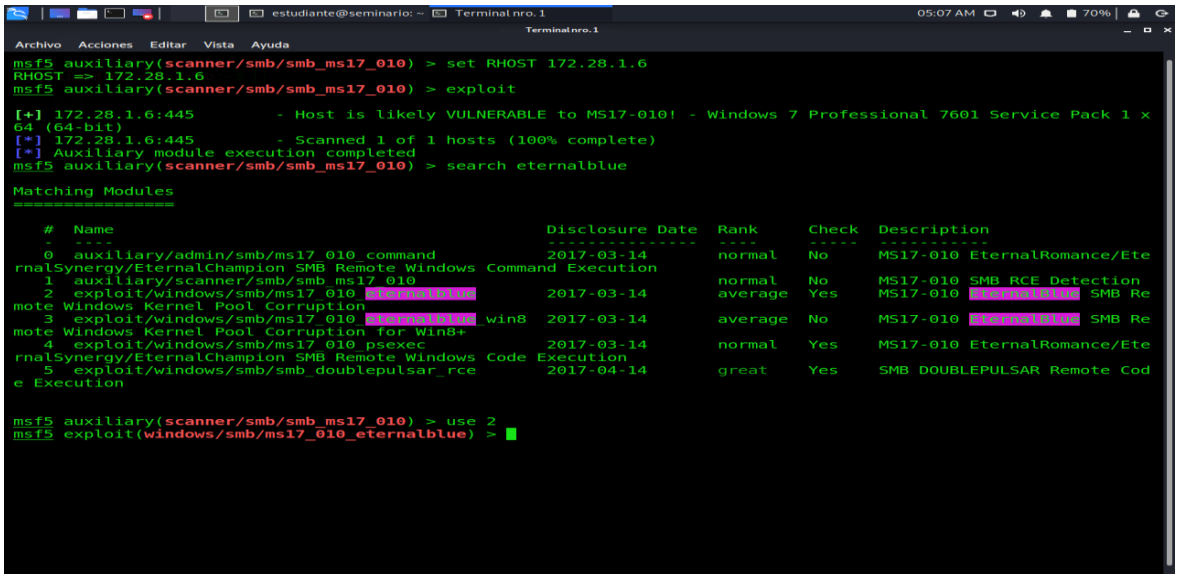
Ilustración 5 Vulnerabilidad descubierta en maquina a atacar



Fuente: el autor

Luego de tener el conocimiento de cuál es la vulnerabilidad que posee a través de un metaexploit llamado eternalblue el cual no va a permitir explorar la maquina objetivo.

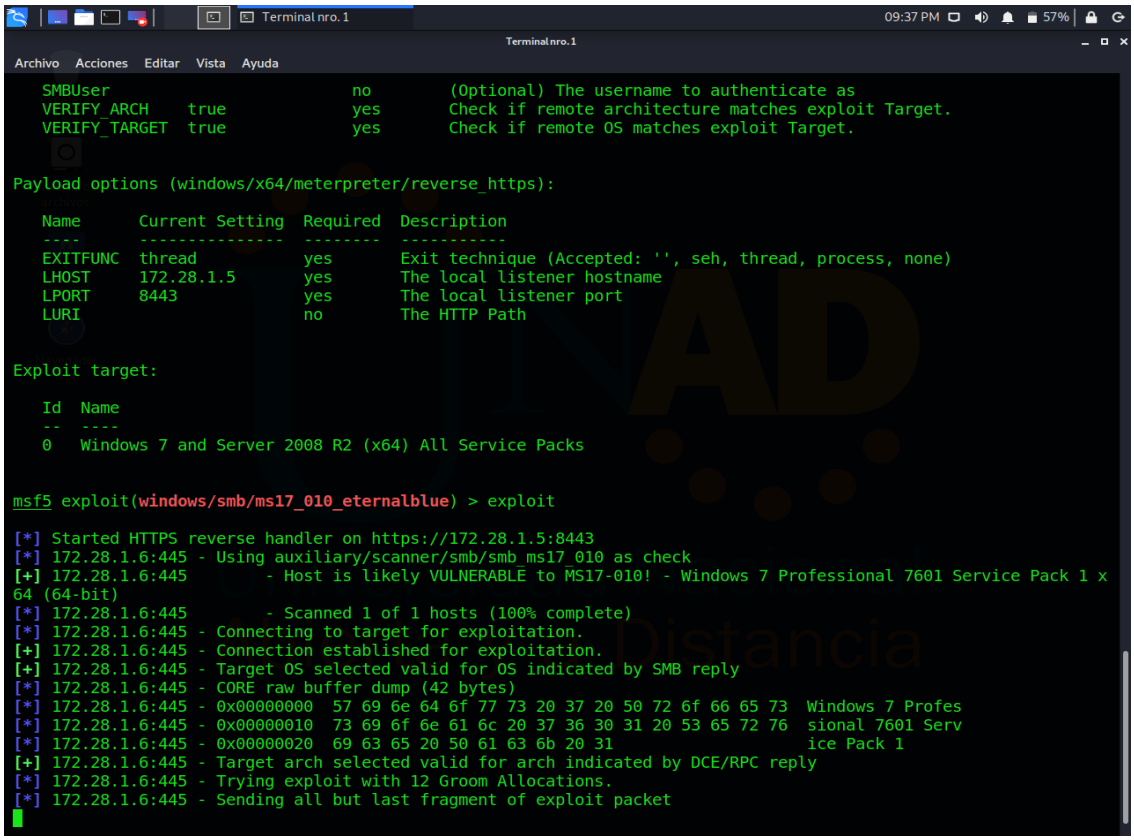
Ilustración 6 Uso de metaexploit eternalblue



Fuente: el autor

Ya al saber cuál es el metaexploit que vamos a utilizar se procede a ejecutarlo para así lograr tener acceso a la maquina objetivo

Ilustración 7 Ejecución de metaexploit



Fuente: el autor

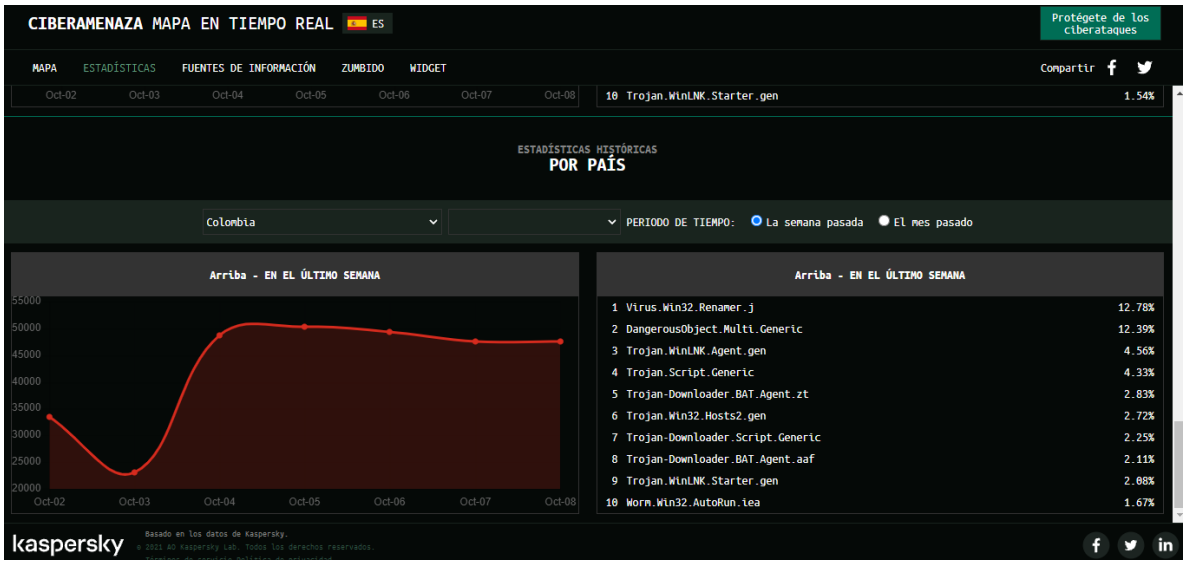
Donde por medio de este fallo en el sistema podemos demostrar que se puede tomar el control de la maquina donde se afectó la integridad de la misma pudiendo así obtener los ciberdelincuentes información privilegiada de la empresa o persona afectada.

Por lo cual es de vital importancia tener los equipos en lo posible lo más actualizado que se pueda.

6.3 DESARROLLO OBJETIVO ESPECÍFICO 3

Teniendo en cuenta lo desarrollado en el seminario vemos como cada día estamos más y más expuestos a los peligros que encontramos en el ciberespacio, primero que todo nos referiremos a los ataques en tiempo real, donde vemos en la actualidad como cada segundo en el ciberespacio en cualquier país del mundo se esta efectuando un ataque a cualquier sistema de información o servicios a las empresas. Nuestro país no es la excepción en la siguiente grafica podemos observar los ataques que más se dieron en la última semana.

Ilustración 8 Ciberataques en Colombia



Fuente: https://cybermap.kaspersky.com/

Por ende las empresas deben estar preparadas para reaccionar en cualquier momento para atender estos incidentes, donde cobra vital importancia los equipos Blueteam, el cual podemos describir como un equipo que se encarga de monitorear constantemente los servicios tecnológicos de la empresa para ver si hay algún comportamiento anormal en la red o el uso de los servicios de la empresa y que analiza en tiempo real los fallos o vulnerabilidades que se pueden presentar los softwares de la empresa para ir corrigiéndolos inmediatamente que son detectados.

Además de este equipo las empresas deben contar mínimo con otro equipo que de respuestas a estos incidentes más desde el punto de vista procedimental como son los llamados CSIRT, “Un equipo de respuesta a incidentes de seguridad

informática (CSIRT, por sus siglas en inglés) es una entidad organizativa concreta (es decir, con uno o más miembros del personal) que tiene la responsabilidad de coordinar y respaldar la respuesta a un evento o incidente de seguridad informática"[19].

Además de estos equipos en el escenario ideal debe integrarse el equipo redteam, que va a ser el encargado de tratar de vulnerar los sistemas informáticos de la organización o empresa.

En virtud de mejor las capacidades de reacción de los sistemas se debe tratar en lo posible antes estos ataques en tiempo real En primera instancia verificaría mi firewall o IDS a ver cuál es tráfico de la red que se está presentando en el momento y así localizar alguna IP que con mayor tráfico o si hay IP sospechosa tratando de entrar a nuestra red, empezando por los servicios críticos de la organización para así bloquear la IP y los puertos que no estes atacando o si no se puede por el software sin duda se procedería a desconectar el equipo afectado de la red.

Además de esto también la consola de antivirus a ver que ha detectado en las últimas 24 horas a ver si hay algún equipo en riesgo.

Al ser consecuente del ataque realizado a la maquina con Windows 7, inicialmente se procedería a actualizar o parchar el sistema operativo del equipo, luego a revisar los puertos que estén abiertos innecesariamente y cerrarlos todos, solo dejando operativo los que se necesiten y requieren dentro de nuestra red corporativa y actualizar o contar con un endpoint eficiente en los equipos terminales.

Además de esto revisar integralmente las configuraciones de los equipos empezando por los más críticos, con el fin de verificar si tienen usuarios por defecto activos, no están actualizados, si tienen instalados software no necesario o sin licencias, si los puertos USB de los equipos están habilitados para lectura-escritura y fortalecer las sensibilizaciones en pedagogía para el uso adecuado de los equipos y seguridad en la web.

En la actualidad se pueden tomar como referencia estándar los que sugiere CIS "Center For Internet Security"[20],el cual sugiere controles de seguridad mínimos con que deben contar las empresas.

---

[19] Ed Moyle.ISACA. 02 de julio de 2019. CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia? [en línea]. Disponible en: https://www.computerweekly.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia

[20] Centro para Internet Security®. ¿Lo que hay en un nombre? Controles de seguridad críticos de CIS. [en línea]. Disponible en: https://www.cisecurity.org/blog/whats-in-a-name-cis-critical-security-controls

Es fundamental en el ámbito empresarial contar con herramientas que nos permitan tener nuestros datos monitoreados y que nos brinden servicios de detección y contención efectivos.

Por lo cual es necesario que por lo menos se cuenta con sistemas SIEM[21],que actualmente es una herramienta que le ayuda a los administradores de seguridad a tener de una forma centralizada la información de los eventos y log de lo que está aconteciendo en los sistemas en su organización o empresa donde por medio del registro y análisis de todos los eventos que suceden puede detectar algún comportamiento inadecuado o fuera de la cotidianidad de la empresa o entidad.

Sus principales características son:

1) Identificar amenazas

2) Monitorear en forma centralizada las amenazas

3) Aprender de los incidentes presentados

4) Se documentan todos los procesos de detección de anomalías

Las funciones que debe cumplir un sistema SIEM son:

1) Automatizar las tareas

2) Dar respuestas automáticas cuando detecte algún fallo o anomalía

3) Emitir alertas

4) Realizar seguimiento a los eventos que se detecten

5) Manejar los riesgos

6) Evaluar las vulnerabilidades

7) Monitorear el comportamiento de las fallas

Siendo consecuente con estas herramientas de detección podemos además contar con herramientas de contención que nos permitan reaccionar

[21] Pachón, C. 09 de junio de 2021. ¿Qué es SIEM en seguridad informática? Alcance e implementación. [en línea]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

adecuadamente cuando es detectada o se está viendo afectada la integridad de nuestros sistemas.

Podemos usar las herramientas de Cisco, Cisco FireSIGHT, por medio de la cual se detecta alguna actividad inusual o no autorizada y le notifica a Cisco TrustSec, el cual nos permite aislar en la red un dispositivo que este con sospecha de estar infectado, colocando en una red virtual aislado de los demás componentes de la red y de todos los servicios brindados.

Otra herramienta que se podríamos utilizar es SolarWinds, la cual nos permite a través de sus herramientas de monitoreo, verificar eventos sospechosos y en tiempo real responder a los mismos conteniendo así los daños.

Finalmente podemos tener en cuenta la nueva generación de firewall NGFW de Fortinet, los cual nos permiten además de detectar e identificar los ataques, bloquear los ataques a través de la inspección y prevención de intrusiones a través sus poderosas características como son FortiAnalyzer, Web Filtering y Desarme y reconstrucción de contenido.

7 CONCLUSIONES

En el desarrollo del presente informe por medio del cual, con estudios de situaciones puntuales y ejercicios prácticos, además del análisis de las leyes colombianas para la protección de datos personales y de la protección de los datos e información; podemos decir que no es solo proteger con herramientas informáticas los distintos sistemas de informacion,redes,equipos sino que además de esos componentes importantes esta los deberes y obligaciones como ingenieros para un ejercicio adecuado de nuestra profesión siguiendo al pie de la letra nuestro código de ética, porque en mi entender si todos los ingenieros o personas con altos conocimientos técnicos reflejaran eso valores y deberes para con la sociedad no tendríamos en la actualidad la necesidad de tener robustos sistemas de seguridad, equipos como Blueteam y Readteam , CSIRT, para estar monitoreando la seguridad de la empresas.

Por lo cual insto a mis colegas a que por muy onerosos que sean los honorarios no prestarse para practicas indebidas o si conocen de delitos que se estén ejecutando denuncien ante las autoridades competentes, debemos dignificar nuestra profesión para el buen ejemplo de las nuevas generaciones y cada día más cerrar esa brecha entre los cibercriminales y las personas o empresas de bien.

Pero como la realidad es otra debemos cada día más estar preparados y tratar de llevar a cabo las mejores prácticas para lograr unos efectivos controles de seguridad informática en el seno de nuestras empresas y en el ámbito personal, ya que unido podemos lograr vencer a estos ciberdelincuentes que día a día buscan la forma de afectar nuestra sociedad.

8 RECOMENDACIONES

En el análisis de las situaciones presentadas y en virtud de lo que se presenta en la actualidad en mi parecer lo principal es que las empresas grandes, pequeñas o medianas con sus diferentes objetos sociales, sean conscientes de los riesgos y que son vulnerables en cualquier momento, ya que a veces por tener un antivirus licenciado o un firewall creen que ya están protegidos, los cual es un error común para muchos de los gerentes o presidentes de empresas u organizaciones.

Las recomendaciones o pautas que se deben seguir son la siguientes:

- ✓ Diseñar, implementar y monitorear plan de capacitación en ciberseguridad y seguridad de la información para todos los empleados.
- ✓ Socializar periódicamente los artículos de la ley 1273 de 2009 y la ley 1581 de 2012, para el conocimiento de todos
- ✓ Velar por que los sistemas operativos de los equipos clientes y servidores estén actualizados.
- ✓ Para los equipos de seguridad y de respuesta a incidentes recordarles la importancia de cumplir con el código de ética.
- ✓ Realizar pruebas periódicas de métodos de ingeniería social (controlados) al personal interno con el fin de cuantitivamente los indicadores de que tipo de empleados o persona son los más vulnerables a estos ataques.
- ✓ Instar a los diseñadores y desarrolladores de software usar plugins o paquetes de desarrollo avalados y aprobados a nivel mundial como seguros, no usar estas herramientas o bajarlas de sitios de dudosa reputación o en la red oculta.
- ✓ Mantener los sistemas de seguridad perimetral actualizados y con contratos de soporte ante cualquier eventualidad.
- ✓ Aunque parezca lógico, pero se deben contar con Endpoint eficientes, licenciados y que estes actualizados constantemente.
- ✓ Hacer cumplir los controles de seguridad documentados en las políticas de seguridad informática de la entidad y que estén en constante análisis y retroalimentación.

BIBLIOGRAFÍA

BORRMART, S.A. *¿Qué es el malware? Tipos y maneras de evitar ataques de este tipo*. [en línea]. Disponible en: https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html

Centro para Internet Security®. *¿Lo que hay en un nombre? Controles de seguridad críticos de CIS*. [en línea]. Disponible en: https://www.cisecurity.org/blog/whats-in-a-name-cis-critical-security-controls

COPNIA. 09 de octubre de 2021. *Codigo de etica.* [en línea]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Ed Moyle.ISACA. 02 de julio de 2019. *CERT vs. CSIRT vs. SOC: ¿Cuál es la diferencia?*.[en línea]. Disponible en: https://www.computerweekly.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia

ESIC BUSINESS & MARKETING SCHOOL. 01 de febrero de 2018. Red team: qué es, estrategias y ejemplo de un caso real. [en línea], Disponible en: https://www.esic.edu/rethink/tecnologia/red-team-experiencia-en-ataque

Esteban, S. 07 de febrero de 2016. *Metasploit: Atacando a Windows*. [en línea]. Disponible en: https://backtrackacademy.com/articulo/metasploit-atacando-a-windows

Iberdrola, S.A. 08 de octubre de 2021. *'Phishing': un clic marca la diferencia*. [en línea]. Disponible en: https://www.iberdrola.com/innovacion/phishing

Incibe.20 de marzo de 2017. *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?.* [en línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Incibe. 04 de julio de 2019. *¿Qué es el pentesting? Auditando la seguridad de tus sistemas*. [en línea], Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

It Digital security. 30 de mayo de 2018. ¿Qué es un Blue Team y cómo trabaja? .[en linea], Disponible en: https://www.itdigitalsecurity.es/actualidad/2018/05/que-es-un-blue-team-y-como-trabaja

Jaimovich, D. 11 de mayo de 2021. *Qué es el "vishing", la estafa telefónica de moda utilizada para robar datos del homebanking*. [en línea]. Disponible en https://www.infobae.com/america/tecno/2021/05/11/que-es-el-vishing-la-estafa-telefonica-de-moda-utilizada-para-robar-datos-del-homebaking/

Merino, J. P. 01 de enero de 2017. *Definicion de Firewall*. [en línea]. Disponible en: https://definicion.de/firewall/

Pachon, C. 09 de junio de 2021. *Qué es SIEM en seguridad informática? Alcance e implementación*. [en línea]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Policia nacional. 08 de noviembre de 2020. [en línea]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Red hat. 08 de octubre de 2021. *El concepto de CVE*. https://www.redhat.com/es/topics/security/what-is-cve

Redacción CIO México. 20 de enero de 2021. *¿Cuáles fueron las principales ciberamenazas en 2020?, una retrospectiva*. [en linea]. Disponible en: https://cio.com.mx/cuales-fueron-las-principales-ciberamenazas-en-2020-una-retrospectiva/

Senado de la Republica. 27 de 06 de 2013. [en línea]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

Telefónica Cybersecurity & Cloud Tech, S.L.U. 09 de octubre de 2021. [en línea]. Disponible en: https://www.elevenpaths.com/es/innovacion-laboratorio/tecnologias/foca

Anexo A Video Sustentación A

Aquí encontraran el link de video con la sustentación:

Link youtube: https://youtu.be/aITaRAZ4Uys

Anexo B Resultado Turnitin 1

Aquí encontraremos el resultado del escaneo por medio de la herramienta anti plagio.