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

WILLIAM EDUARDO VARGAS DOMINGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2022

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

WILLIAM EDUARDO VARGAS DOMINGUEZ

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
LUIS FERNANDO ZAMBRANO HERNANDEZ
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2022

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

GLORARIO

Blueteam: grupo de personas con amplios conocimientos en seguridad informática, implementado al interior de las empresas con el fin de proteger los activos de información de la entidad.

CVSS son métricas que evalúan las vulnerabilidades y según FIRST[1] la puntuación refleja la gravedad.

Eternalblue nombre dado a una serie de vulnerabilidades que presenta el software de Microsoft.

Exploit es un bloque de código, secuencia o comandos que aprovecha error o vulnerabilidad un programa informático.

ExploitDB es una página web que alberga base de datos públicas de exploit.

Explotar hace referencia a ganar acceso de manera satisfactoria de un fallo de seguridad.

Firewall herramienta informática que mediante comando permite o deniega acceso a un equipo o red por motivos de seguridad.

Framework esquema o marco de trabajo que ofrece una estructura, para a partir de él se continúe con la elaboración de un proyecto.

[1] FIRST. Common Vulnerability Scoring System v3.0: Specification Document. [Sitio Web]. [Consulta 3 octubre de 2022]. Disponible en: https://www.first.org/cvss/v3.0/specification-document#:~:text=1.1.&text=CVSS%20is%20composed%20of%20three,time%20and%20across%20user%20environments.

Hacker ético nombre dado a personas con conocimientos en seguridad informática que ayudan a las empresas a identificar fallos en infraestructuras de TI con el fin de protegerse de piratas informáticos.

Hardenizar termino dado al proceso para reducir fallos de seguridad que presente una infraestructura de TI.

HTTP protocolo de comunicación que permite la transferencia de información en internet.

HTTPS protocolo de comunicación que permite la transferencia de información en internet de manera segura.

IDS herramienta implementada en infraestructuras TI, que detecta acceso no autorizados.
IPS herramienta implementada en infraestructuras TI, que protege a los sistemas de ataques o intrusiones.

ISSAF framework que brinda una metodología de testeo.

Kali sistema operativo de distribución Linux diseñada para temas de seguridad informática.

Metasploit herramienta enfocada en seguridad informática constantemente implementada por auditores de ciberseguridad.

Nessus programa para escanear vulnerabilidades en infraestructura TI.

Nmap es un programa gratuito que es implementado por auditores en seguridad informática para exploración de la red y rastreo de puertos.

Parche hace referencia a las actualizaciones de un software con el fin de corregir errores del sistema.

Pentesting es el testeo que se le hace una infraestructura de TI con el fin de detectar fallos o vulnerabilidades para posterior mitigación.

Redteam grupo de personas con amplios conocimientos en seguridad informática, implementado al interior de las empresas que intentan superar los controles puestos por el equipo blue a los activos de información.

Shell interfaz de usuario en la cual ejecutan comandos que interpreta la máquina para controlar el sistema operativo.

RESUMEN

El manejo de la información digital ha tenido gran relevancia desde hace unos años, es por ello que nos hemos visto en la necesidad de crear leyes, implementar medidas, elaborar herramientas de hardware y software con el fin cumplir los pilares de la ciberseguridad, (confiabilidad, integridad, y disponibilidad).

Es por ello que se desea compartir un compendio de las leyes colombianas que a la fecha castigan el delito de acceso abusivo a sistemas informáticos, por otra parte, de sea resaltar la magnífica labor que realizan los equipos RedTeam y BlueTeam uno en busca de vulnerabilidades para su posterior explotación y el otro trabajando arduamente en pro de mitigar fallos de seguridad haciéndole cada vez más difícil el trabajo al equipo red.

ABSTRACT

The management of digital information has had great relevance for a few years, which is why we have seen the need to create laws, implement measures, develop hardware and software tools in order to meet the pillars of cybersecurity, (reliability , integrity and availability).

That is why we want to share a compendium of Colombian laws that to date punish the crime of abusive access to computer systems, on the other hand, to highlight the magnificent work carried out by the RedTeam and BlueTeam teams one in search of vulnerabilities to its subsequent exploitation and the other working hard to mitigate security flaws, making it increasingly difficult for the network team to work.

INTRODUCCIÓN

Con el desarrollo del presente trabajo se desea conocer y la legislación colombiana que penaliza los delitos informáticos, de igual manera se desea hacer mención de algunas herramientas con que cuentas los equipos RedTeam y BlueTeam para atacar y proteger respetivamente de las posibles brechas de seguridad que pueda llegar a tener una infraestructura tecnológica.

OBJETIVOS

OBJETIVOS GENERAL

Diseñar un informe que plantee estrategias de contención mediante el análisis de riesgos y vulnerabilidades de una infraestructura TI.

OBJETIVOS ESPECÍFICOS

- Conocer las leyes colombianas que tipifican y sancionan los delitos informáticos con el fin de evitar sanciones al realizar auditoría de seguridad informática.

- Recopilar y analizar la información sobre la red de la empresa Hackers Security con el fin de ejecutar tareas del equipo redteam.

- Formular medidas de hardenización a los equipos comprometidos y de esta forma minimizar brechas de seguridad para lograr robustecer la seguridad informática.

1. CONCEPTOS EQUIPOS DE SEGURIDAD

1.1 MARGEN LEGAL EN COLOMBIA SOBRE DELITOS INFORMÁTICOS Y PROTECCIÓN DE DATOS PERSONALES.

En Colombia existen una ley que sanciona delitos informáticos tipificados en la ley 1273 del 2009 tales como: acceso abusivo a sistemas de informáticos, obstaculizar sistemas, interceptación, destruir o dañar información, utilización distribución o portar software malicioso, violación de datos personales y suplantación de sitio web el infringir cualquiera de los anteriores será castigado con cárcel y multa, estipulado en el artículo 269 y sus variables.

Por otra parte, existe la ley de protección de datos personales o ley 1581 del 2002, esta ordenanza pretende la protección de los datos personales que estén almacenados en empresas publicas y/o privadas.

1.2 ETAPAS DEFINICION Y HERRAMIENTAS DEL PENTESTING

Para habla de los pentesting o auditorias de seguridad informática, se debe saber que son pruebas que se realizan a la entidad para saber cuan expuestos están ante un eventual ataque, según Campus Internacional de Ciberseguridad[2] existen tres tipos de pruebas de penetración, que son:

[2] Campus Internacional de Ciberseguridad. ¿QUÉ ES EL PENTESTING? [Sitio web]. [Consultado 25 de agosto 2022]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

Caja negra. No conoce ninguna característica de la infraestructura o no tiene información alguna a cerca de la red o dispositivos a ser auditados, Este tipo de auditorías analiza los sistemas verificando únicamente entradas y salidas de cada funcionalidad.

Caja blanca. Se realizan con acceso a la información interna de la empresa, por ejemplo: mapa de red, firewall, sistemas operativos, segmentación de la red, para ello el auditor asume un rol dentro del a empresa, de igual forma se deben descubrir activos.

Caja gris. La caja gris es como una mezcla entre la caja blanca y la caja negra, pues el auditor asume un rol dentro de la corporación con pocos privilegios, y este debe escalarlos, de acuerdo a los equipos o software a auditar.

Una vez mencionado los tipos de auditorías existentes, debe saber que Junta de Andalucía[3] menciona existen diferentes metodologías y framework para realizar pentesting, como lo son: OSSTMM, OWASP, ISSAF, PTES, CVSS.

Dependiendo la metodología o persona que realice en la auditoria estos pasos pueden llegar a variar, pero en general todos llegaran a la misma conclusión.

1.2.1 Contacto

Este es considerado el paso más importante, pues es el acuerdo que se hace entre contratista y contratante, dando límites al proyecto, de igual manera que tipo de prueba se ara caja blanca, caja negra o caja gris. Es de mucha utilidad realizar un contrato firmado por ambas partes (empleador y hacker etico), ante notaria.

[3] Junta de Andalucía., Metodología y Frameworks de testeo de la seguridad de las aplicaciones. [Sitio web]. [Consultado 25 de agosto 2022]. Disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html

1.2.2 Recolectar de información

Fase dedica a recopilar información de la empresa, para lo cual es requerida cierta destreza para buscar información en la web, también se puede verificar información en redes sociales de los empleados de la empresa, pues estos en ocasiones publican información relevante, se astuto por ejemplo podrías acudir a la página de la empresa en la misma prodria encontrar información incluso podrías utilizar nmap aqui, buscar entre los papeles desechados de la institución y por qué no tratar de tener información desde la misma persona de soportes TIC, por medio de la ingeniería social.

1.2.3 Búsqueda de vulnerabilidades

Algunos la llaman análisis de vulnerabilidades, es aquí donde se traza el posible o los posibles vectores de ataque, partiendo desde la información recolectada.es aquí donde dará resultado el esfuerzo hecho en la fase anterior, con toda la información recolectada se iniciará una búsqueda de vulnerabilidades e identificando posibles vectores de ataque.

1.2.4 Explotación de vulnerabilidades

Muchos mencionan que es la fase preferida de los auditores. Es aquí donde se obtienen resultados tangibles de los anteriores pasos, se consigue o no acceso a los sistemas del contratista, por lo general se realizan exploit contra las vulnerabilidades encontradas y también se utilizan credenciales obtenidas con el fin de ganar mayores privilegios. Es aquí donde se implementan muchas herramientas, por ejemplo, puede iniciar con NMAP para saber puertos, servicios y versiones de los servicios abiertos, seguido a ello puede utilizar herramientas como NESSUS y METASPLOIT para explotar la vulnerabilidad y ganar acceso a la máquina.

1.2.5 Post-explotacion.

Se intenta llegar lo más lejos posible dentro de la penetración del sistema vulnerado, es decir conseguir los privilegios de administrador, aquí depende mucho la habilidad

del auditor y la información recolectada del administrador del sistema, en algunas ocasiones los administradores al instalar nuevos equipos o software dejan las credenciales de acceso por defecto, que es un grave error.

1.2.6 Informe

Es el momento de realizar el informe, se sugiere hacer dos, uno técnico y otro gerencial. Es importante que paso a paso quede registrado por medio de capturas de pantalla, con de fin de presentar información veraz y clara, de la auditoria de seguridad realizada, en ella se detalla el proceso, herramientas utilizadas, técnicas o metodología implementada y por último y no menos importante las vulnerabilidades descubiertas.

1.3 HERRAMIENTAS DE CIBERSEGURIDAD

1.3.1 Metasploit

Framework abiertos desarrollo en la actualidad en ruby, orientada a auditores de seguridad, con el fin de explotar las vulnerabilidades de los sistemas y de esta forma robustecer la seguridad. Según ciberseguridad[4] esta herramienta la compro rapid7 y cuenta con 2 versiones gratuita metasploit y paga metasploit pro que incluye:
explotación manual, evasión de antivirus e IPS / IDS, pivote de proxy, módulos posteriores a la exploración, limpieza de sesión, reutilización de credenciales, ingeniería social, generador de carga útil, VPN pivotante, validación de vulnerabilidades, pruebas de aplicaciones web.

[4] ciberseguridad., ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio web]. [25 de agosto 2022]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

1.3.2 Nmap

Algunos lo denominan herramienta de recolección de información fingertprinting, que hace referencia a conseguir de datos de un dominio con la interacción del mismo.

Esta es una herramienta que sirve para verificar puertos de un equipo, pero no solo ello de igual forma te facilita información tal como ip, todos los puertos abiertos y cerrados de un dominio, de igual forma muestra detalle del servicio y la versión que corre por el puerto, dependiendo del comando utilizado mostrada hasta su CVE.

1.3.3 OpenVas

Esta es una herramienta que sirve para escanear e identificar vulnerabilidades, adquiere esta capacidad al escanear el objetivo y posteriormente ataca y comparar los resultados con su base de datos y de esta forma logra clasificar el nivel de gravedad de la falla. Este framework cuenta con características tales como: escáner de forma simultanea diferentes equipos, soporta SSL, soporta HTTP y HTTPS, multiplataforma.

1.3.4 ExploitDB

Para hablar de ExploitDB debes saber que exploit es una palabra inglesa que al traducir hace mención a explotar o aprovechamiento, hablando de sistemas informáticos hace referencia a fragmentos de cogido, secuencia de acciones o comando con el fin de aprovecharse de una vulnerabilidad en la seguridad de un sistema.

Dado lo anterior se puede decir que exploit-DB[5] es un repositorio con una amplia base de datos de exploit, pues muchos hackers cuelgan allí las vulnerabilidades, enseñando como se puede aprovechar de la brecha de seguridad.

[5] Exploitdb. Exploit data base. [Sitio web]. [Consultado 25 agosto de 2022]. Disponible en: https://www.exploit-db.com/

1.3.5 CVE

Esta sigla hace referencia a vulnerabilidades y explotaciones comunes, esta es una lista publica de los fallos de seguridad documentados, que a cada uno se le asigna un número de identificación.

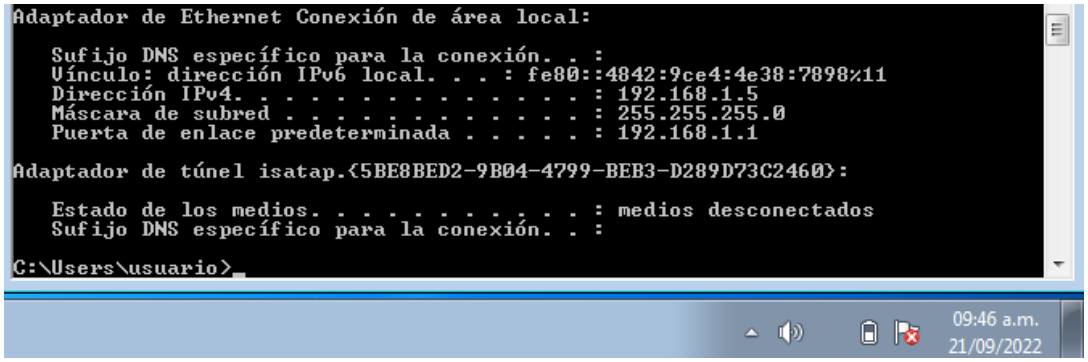
Para ello existe una organización que se encarga de supervisar la asignación del código CVE y esta es MITRE. A esta lista puedes acceder por medio de NVD National vulnerability DataBase y la CERT/CC vulnerability notes database.

2. EJECUCIÓN PRUEBAS DE INTRUSIÓN

2.1 HERRAMIENTA Y SOFTWARE UTILIZADO

Una de las fases del pentesting nos habla del reconocimiento, por ello es necesario saber la red o ips de los equipos a intervenir en la figura 1 se puede evidenciar la ip de la maquina Windows con arquitectura X64 que es 192.168.1.5/24.

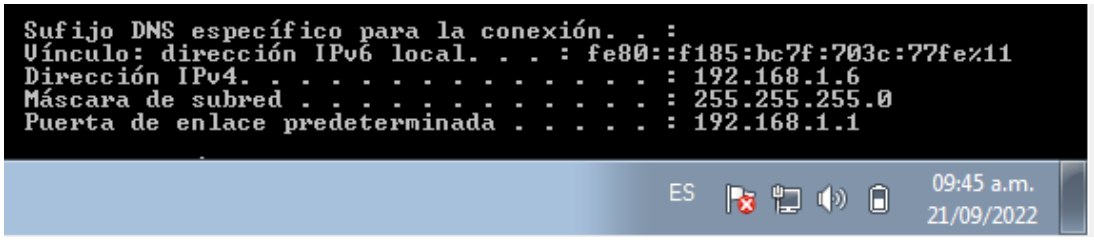
Figura 1 Ip Windows X64



Fuente: propia del autor

En la Figura que adelante se relación se puede evidenciar la ip de la maquina Windows, arquitectura X32 con ip 192.168.1.6/24

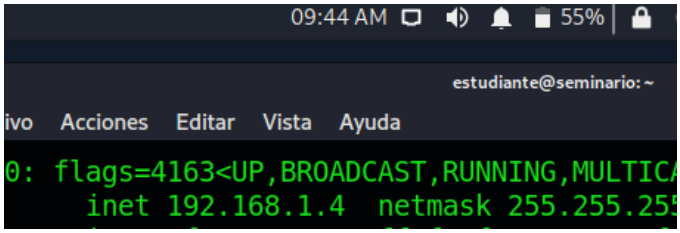
Figura 2 Ip Windows X86



Fuente: propia del autor

En la Figura 3 se puede ver la maquina kali Linux con la ip 192.168.1.4/24, para seguir con la actividad es indispensable que las maquinas se puedan ver, para ello lo puede hacer con un ping, en algunas oportunidades las maquinas Windows no contestan esta petición por una regla implementada en el firewall.

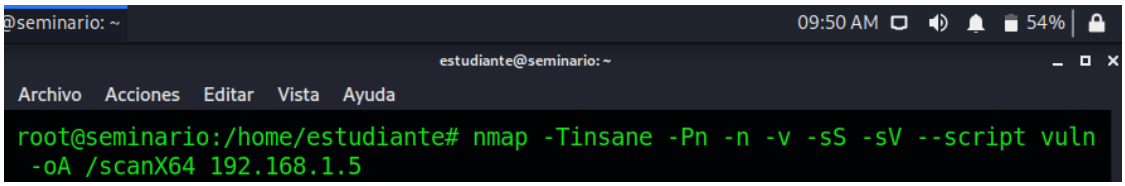
Figura 3 Ip kali linux



Fuente: propia del autor.

Siguiendo con la fase de recolección de información se lanza a cada una de las maquinas Windows desde la kali un comando con la herramienta NMAP, este comando mostrara los puertos abiertos, servicios que corren por el puerto y la versión, de igual forma mostrara si existe alguna vulnerabilidad conocida y documentada en el CVE, de igual forma mostrara si existe alguna explotación conocida o existente en MSF.

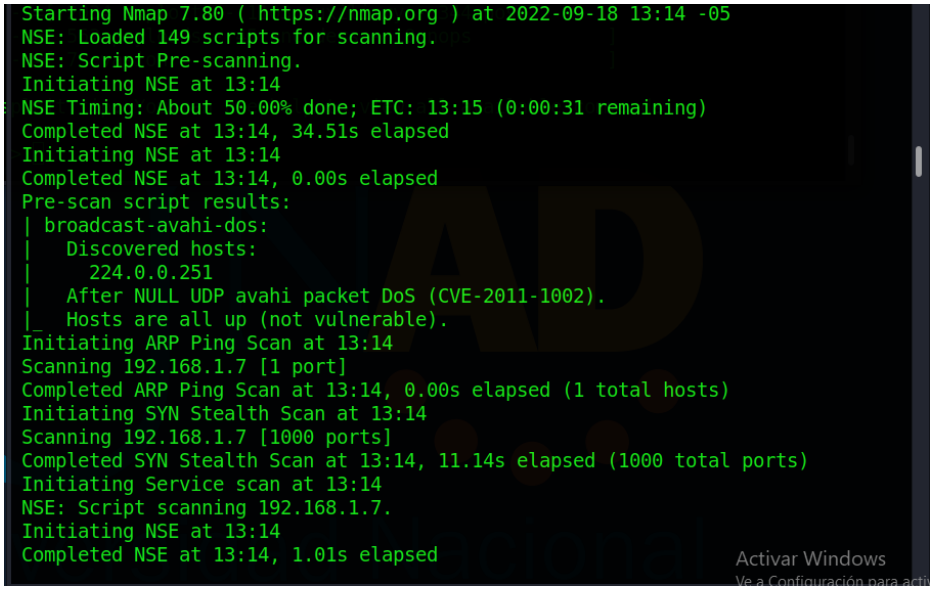
Figura 4 Comando utilizado



Fuente: propia del autor.

Lanzado la línea de comando de la Figura 4 para la maquina Windows X64, como resultados se obtiene una vulnerabilidad que muestra la Figura 5, a pesar de no tener puertos abiertos. Esto quiere decir que este equipo no tiene activo SMBv1, por lo tanto, se puede deducir, por aquí no fue la fuga de información.

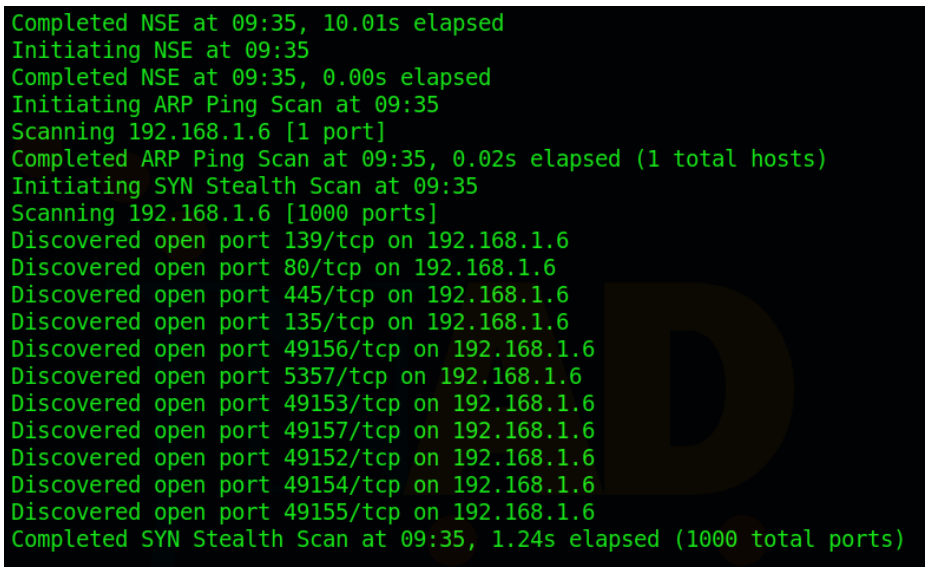
Figura 5 Identificando Windows X64



Fuente: propia del autor.

Se lanza el mismo comando de la Figura 4 pero hacia la ip del Windows X86 que tiene la ip 192.168.1.6, obteniendo como resultado 11 puertos abiertos como lo muestra la siguiente Figura.

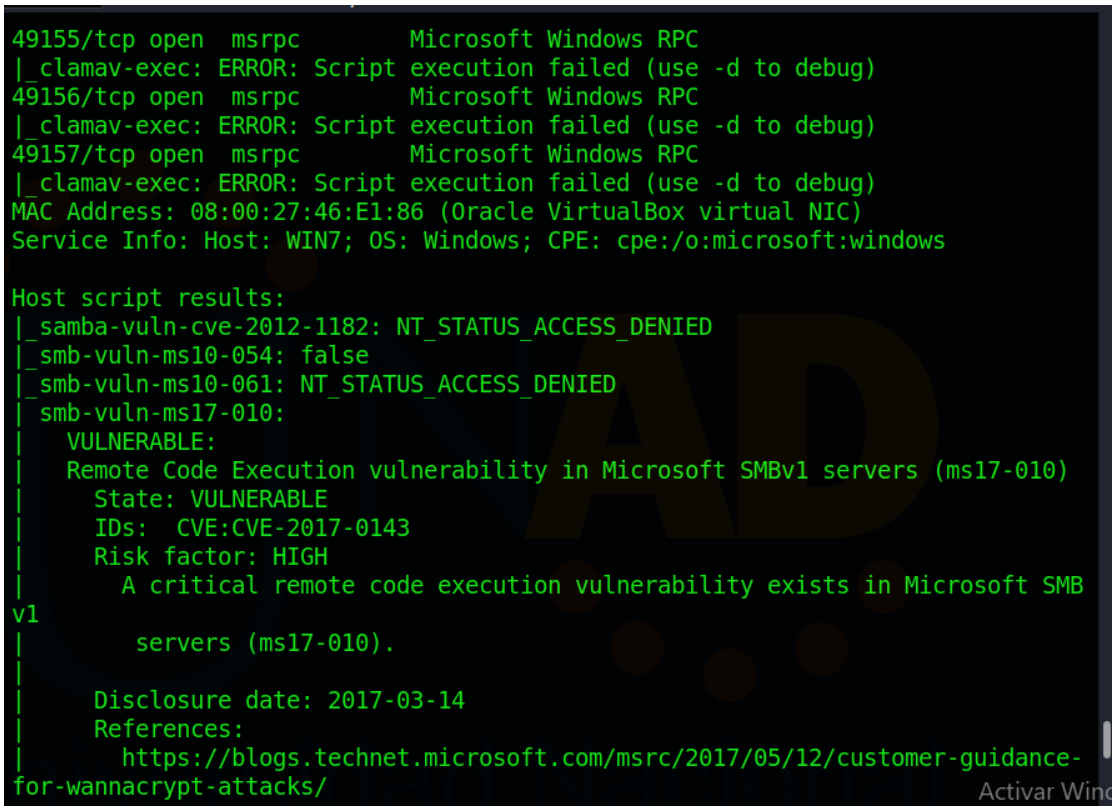
Figura 6 Identificando Windows X86



Fuente: propia del autor.

El anexo 4 escenario 3 menciona una, de las diversas vulnerabilidades que presenta la maquina Windows, esta información es corroborada por la Figura 7, fallos de seguridad identificada como los códigos CVE-2017-0143 y CVE-2017-0144. Según el reporte esta falla se presenta por servicio prestado del puerto 49157. Esto corresponde a la búsqueda de vulnerabilidades, que es otra fase del pentesting,

Figura 7 Vulnerabilidades windowsX86



Fuente: propia del autor.

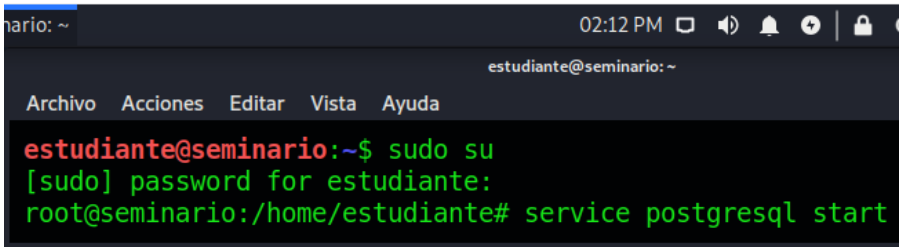
Según Microsoft[6] es un protocolo de red de esta empresa que permite compartir archivos e impresoras entre los equipos con este sistema operativo.

[6] Microsoft., Windows SMB Remote Code Execution Vulnerability. [Sitio web]. [Consulta: septiembre 21 de 2022]. Disponible en https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0144

Una vez identificadas las vulnerabilidades se procede al siguiente paso que es la explotación, esta e puede hacer de diferentes formas pero para este caso se utilizara la herramienta Mestasploit[7].

Antes de iniciar el framework mestasploit es necesario iniciar un motor de base de datos necesaria para el, para ello se ejecuta el comando q muestra la figura 8

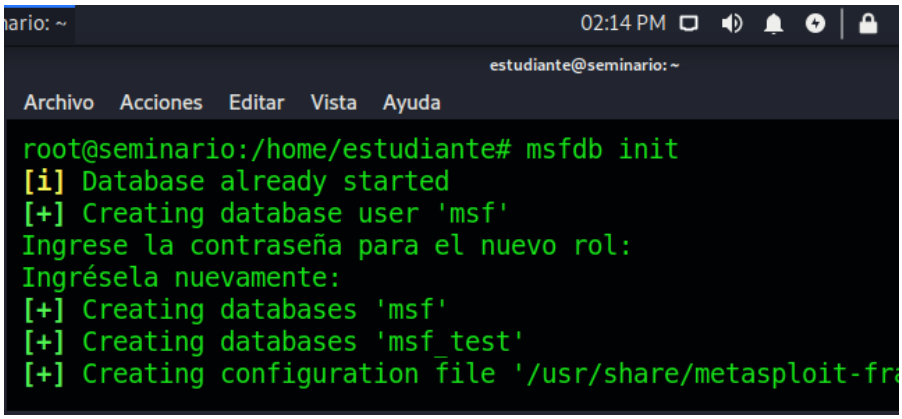
Figura 8 Iniciando prostgresDB



Fuente: propia del autor.

Una vez este arriba el motor DB, se inicializa sobre este la base de datos del framework con el comando que muestra la Figura 9.

Figura 9 Iniciando DB Mestasploit

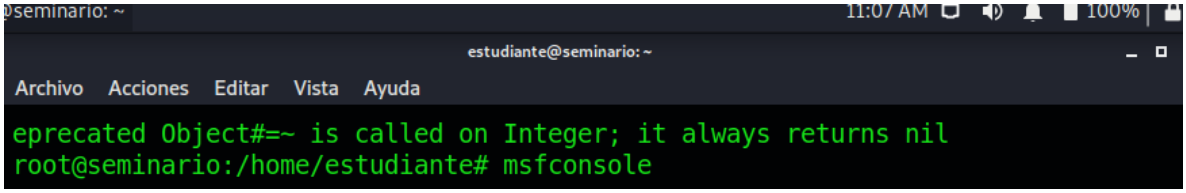


Fuente: propia del autor.

[7] Mestasploit., ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio web]. [Consulta: septiembre 20 del 2022]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Una vez realizado el paso anterior se inicia el programa con comando *msfconsole* como lo muestra la siguiente Figura.

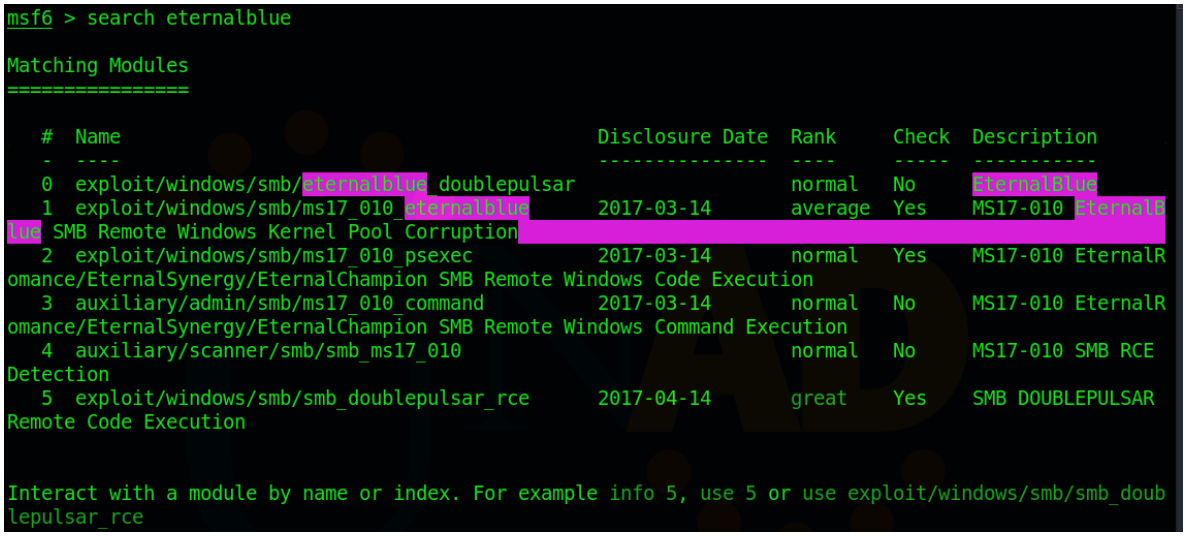
Figura 10 Iniciando MSF



Fuente: propia del autor.

Una vez iniciada la herramienta se puede buscar la explotación por el código CVE, de igual forma lo puedes hacer por el código ms17-010, en la fase de investigación me percate que fallo tiene que ver con el famoso eternalblue de Windows y este fue el parámetro que utilice para la busque del exploit como lo muestra la imagen.

Figura 11 Buscando exploit

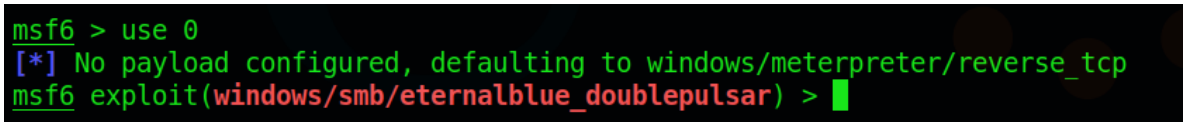


Fuente: propia del autor.

Como lo muestra la imagen y según la DB de mestrasploit existen seis exploit relacionada con el fallo de seguridad, pero entre las mismas se debe seleccionar

una de las seis opciones. Aquí se puede intentar una a una o según la información ya recopilada, para este caso selecciono la primera, para esto dentro de la consola digitamos use y el número del exploit como lo muestra la Figura

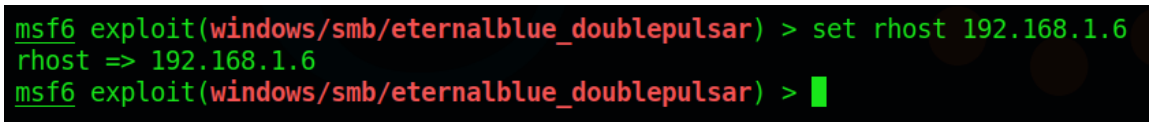
Figura 12 Selección de exploit



Fuente: propia del autor.

Una vez seleccionado el exploit se debe configurar algunos parámetros, para acceder a ellos se puede hacer por medio del comando show options, este exploit por ejemplo me pide configurar el RHOST, que es el equipo al cual se accederá, el payload que es la cargar útil para explotar el fallo de seguridad. Para ingresar la ip debe hacerlo como lo muestra la imagen.

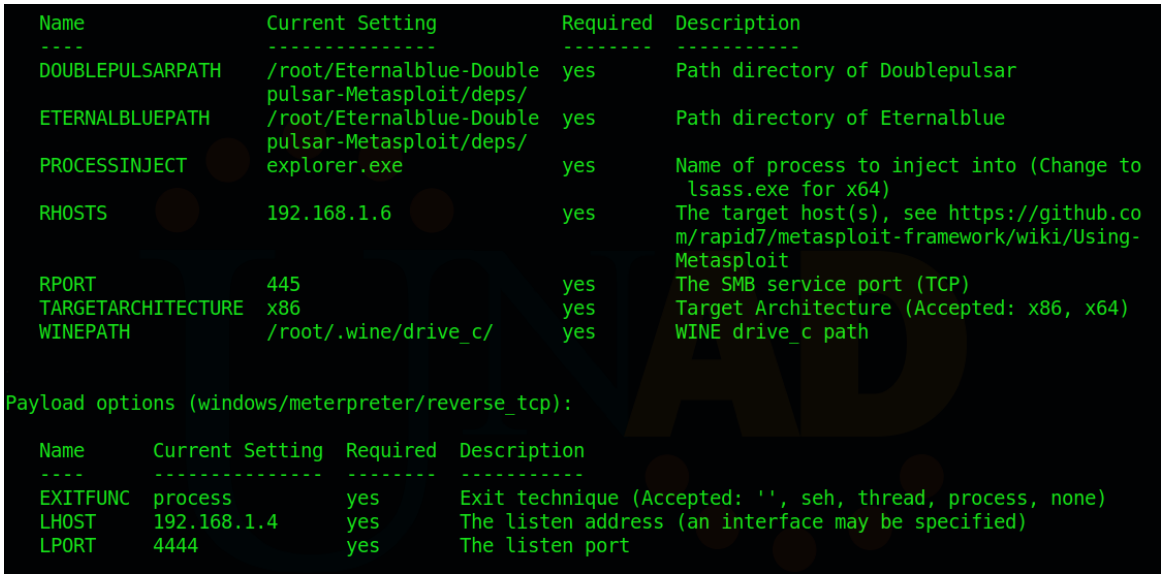
Figura 13 Editar ip



Fuente: propia del autor.

Una vez cargado los parámetros al exploit es recomendable corroborar la informacion con el comando ***show options*** como lo muestra la Figura

Figura 14 Parámetros exploit

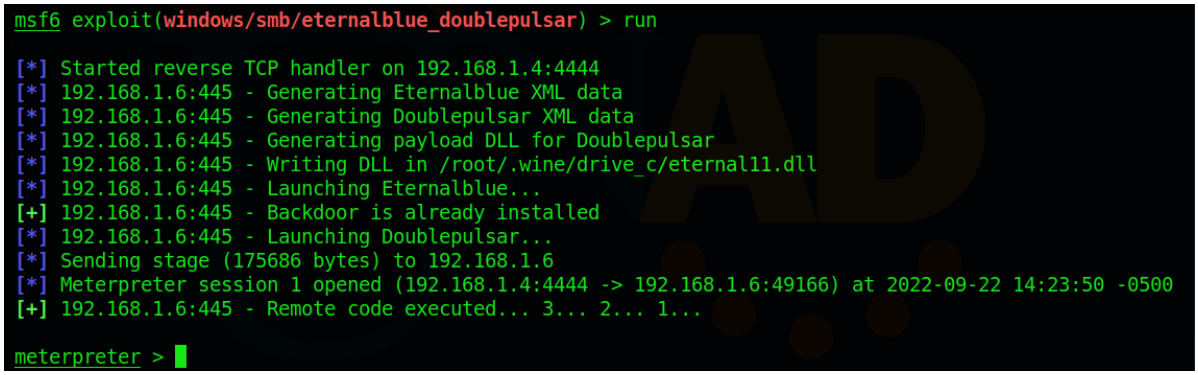


Fuente: propia del autor.

Como se puede ver en la Figura 14 los parámetros cargados son los editados, es hora de lanzar el ataque, esto se puede hacer con el comando ***exploit*** o ***run.***

Como lo muestra la siguiente Figura se tiene obtiene acceso a la maquina con el fallo de seguridad.

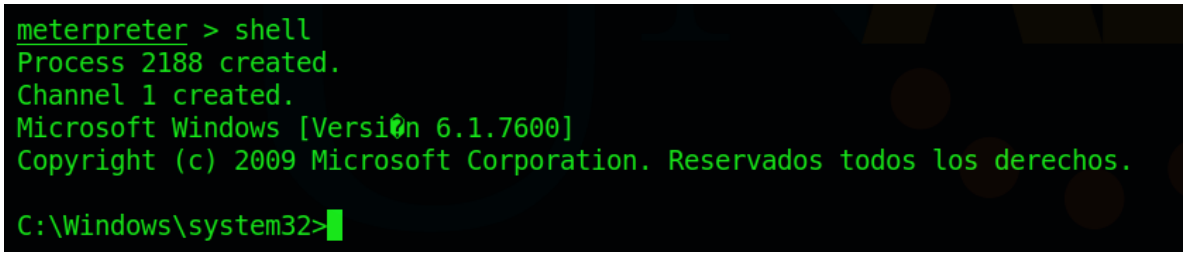
Figura 15 Obteniendo acceso



Fuente: propia del autor.

Es hora de abrir una Shell y buscar el archivo que pide el anexo 4, para ello en la conexión obtenida se escribe ***shell*** como lo muestra la figura

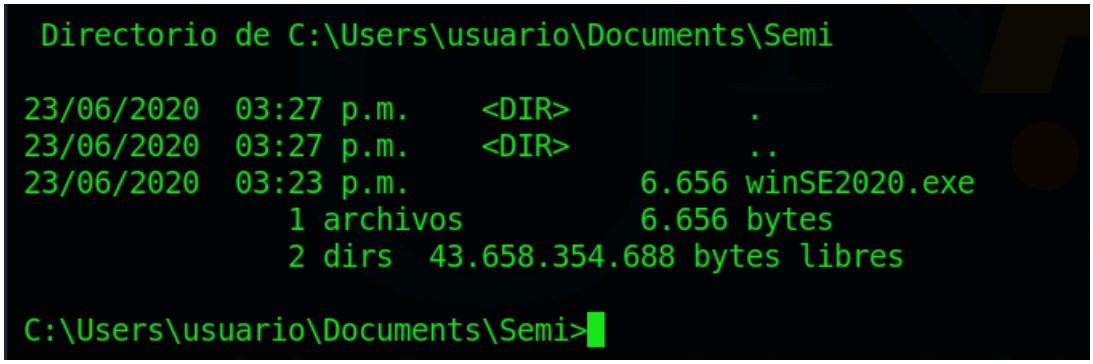
Figura 16 Obteniendo shell



Fuente: propia del autor.

Ahora debemos buscar el archivo “winse20W0.exe” y como lo muestra la imagen se ha conseguido

Figura 17 Archivo winse20W0.exe



Fuente: propia del autor.

2.2 DATOS RELEVANTE ANEXO 4

Los datos que según mi criterio fueron de gran relevancia fueron:

2.2.1 OS y Arquitectura

Esta información fue de gran ayuda pues con ella sabía que existía maquinas con sistema operativo Windows con diferente arquitectura.

2.2.2 Falta de actualización

Al saber que para la fecha no estaba actualizado o parchado algún fallo me daba indicios o pista para obtener información en la web.

2.2.3 Codigo CVE

Sin lugar a duda este es una pista muy valiosa, puesto que me indicaba de por si la vulnerabilidad del equipo solo faltaba saber cuál era.

2.2.4 Código MS

Otra pista para saber un poco más de la falla de seguridad presentada.

2.2.5 Protocolo SMB

Saber que existe un puerto abierto y sumado a ello tener la información del servicio y versión es muy importante porque esto es parte de lo que se necesita saber para explotar un fallo de seguridad.

2.3 HERRAMIENTAS UTILIZADAS

Es claro que para la fecha se vive la era digital, y gracias a la digitalización de la información se puede acceder a esta por medio de internet, se puede tener acceso desde cualquier parte del mundo a gran pedazo de esta por no decir que a toda. Con esto quiero decir que esta es una gran herramienta que puede ser utilizada por cualquier sujeto que entre en el mundo del hacking ético.

Para identificar vulnerabilidades existen muchas herramientas para ello, unas pagas otras gratuitas, en este caso utilice la herramienta ***nmap*** con el script ***vuln*** como se evidencia en las imágenes del punto 1 esta muestra puertos, servicios y versiones, vulnerabilidades y según las banderas utilizadas mucha más información de acuerdo a la necesidad o información que se quiera obtener.

Con ***nmap*** se ratificó la información brindada en el anexo 4 y se obtuvo nueva, como número 49157 que es puerto por la cual corre el servicio SMBv1.

2.4 ATAQUE A LA MAQUINA

Esta vulnerabilidad representa un fallo catalogado como crítico, puesto que una vez vulnerado se puede tener acceso total la información que en esta máquina se maneje, y si esto parece poco también se tiene acceso a la cámara, información digitada por medio del teclado, en otras palabras, acceso total de la máquina.

Aquí también se puede escalar privilegios y moverse a otros equipos dentro de la misma red, lo que comprometería no solo un equipo sino N host de la red. Por tratarse de un equipo de una empresa puede estar expuesta información de clientes y proveedores y en caso de ser expuesta y salir afectados puede llevar a grandes sanciones monetarias, perdida de reputación de la empresa y hasta el cierre de la misma esto y un poquito más puede pasar por un simple fallo de seguridad.

2.5 EVICENDIA DE EXPLOTACION

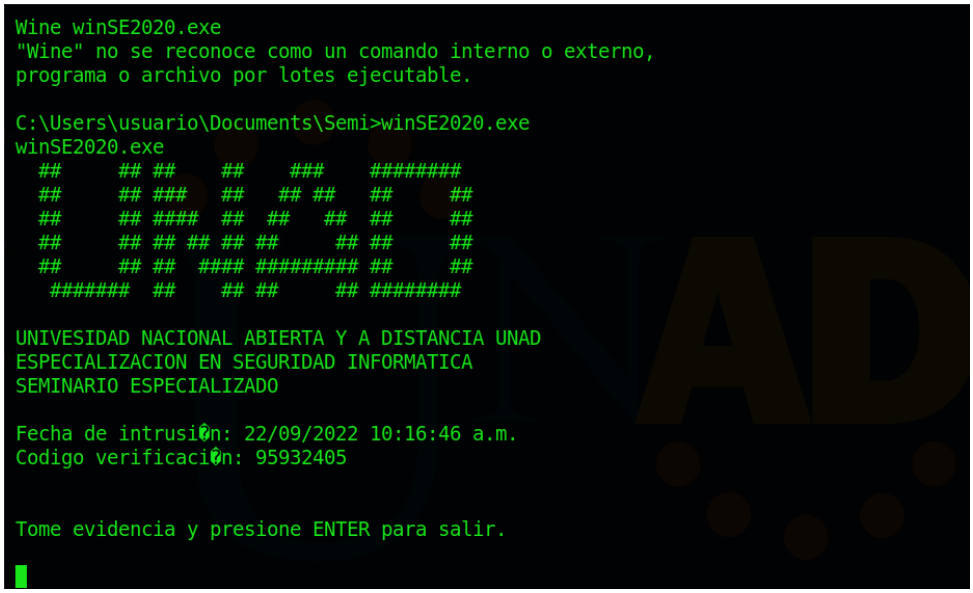
Debe tener presente que el exploit utilizado para vulnerar la maquina no es ninguno que en la actualidad tenga la herramienta metasploit, pues la cargar que tiene la herramienta es efectiva para arquitectura X64 y al ser lanzada a la máquina que presenta la vulnerabilidad, provoca un desbordamiento de buffer causando el error de pantalla azul.

El exploit utilizado fue descargado del repositorio de gitHub y lo puede encontrar con el nombre (Windows/smb/eternelblue_doublepulsar) que es el que muestro en la Figura 12, e implementarlo como indica rapid7[8] aquí también podrá obtener un poco más de información del exploit.

El aprovechamiento de la vulnerabilidad que presenta la maquina Windows X86 es evidenciada en la siguiente Figura

[8] Rapid7. SMB DOUBLEPULSAR Remote Code Execution. [Sitio web]. [consultado 22 septiembre de 2022]. Disponible en: https://www.rapid7.com/db/modules/exploit/windows/smb/smb_doublepulsar_rce/

Figura 18 Exploit completado



Fuente: propia del autor.

3. CONTENCIÓN DE ATAQUES INFORMÁTICOS

3.1 QUE HACER EN CASO DE ATAQUE

Una vez reportado el ataque considero que lo primero que haría es aislar el equipo de la red, esto con el fin de evitar la propagación del ataque en caso de ser una agresión avanzada. Posterior a ello indagaría, ¿Cómo se dio cuenta del ataque o como lo identifico? Aquí se tendría que validar la empresa que estipula en pasos para manejo de incidente o wickr[9] habla de los siete pasos a seguir durante un ataque cibernético, movilizar el equipo de respuesta, identificar tipo de ataque, contener la infección, evaluar y reparar daños, reportar el ataque, comunicarse con los clientes y aprender de la experiencia de igual forma existen varios framework, que indican el proceder ante este tipo de evento.

Independientemente del framework que se emplee es muy acertado realizar un triage al equipo o los equipos vulnerados, identificando conexiones realizadas ip de origen, registros modificados, en caso que la organización cuenta con antimalware o antivirus se realiza un escaneo con las herramientas con el amino de identificar software o código malicioso.

Se podría ejecutar por consola netstat con el ánimo de saber la o las conexiones, puertos, tiempo que duro la comunicación, ip de origen, con esta información se pude descubrir mucho más, por ejemplo la ip de origen puede indicar desde que país se perpetuo el ataque, el puerto nos indica la vulnerabilidad para saber cómo abordarla, tiempo de conexión indica la cantidad de tiempo que duro el intruso en dentro del a compañía toda esta información es indispensable documentarla para

[9] Wickr. 7 Steps to Take During a Cyber Attack. [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en https://wickr.com/7-steps-to-take-during-a-cyber-attack/

compartirla y evitar que otras entidades sufran este fallo de seguridad y en caso que lo sufra mitigarlo en el menor tiempo posible.

3.2 MEDIDAS DE HARDENIZACIÓN PORPUESTAS

El anexo 5 hace mención que la empresa no cuenta con presupuestos, partiendo de aquí, no se puede contemplar la implementación de herramientas que protejan la red que esta es una forma de hardenización, pero esta no es la única.

Debemos entrar a investigar el motivo del puerto abierto, en caso de ser solo acceso a impresora, se puede deshabilitar esta opción y reconfigurar el equipo para que tenga acceso a la impresora de red, si el motivo que este el puerto abierto es por compartir información, se puede crear una carpeta compartida con restricción de acceso, esto podría ser un plus en la seguridad de la información compartida.

En caso que esto no se puede podemos hacer un bloqueo por firewall perimetral denegar o permitir el acceso por ip. De igual forma si el puerto está abierto sin ninguna explicación ce puede cerrar, de igual forma se podría buscar el parche de seguridad que subsane la vulnerabilidad.
Sin lugar a duda debemos apoyarnos del directorio activo en caso que cuente la empresa con alguno, esto con el fin de determinar usuarios, equipos, privilegios, implementación de contraseña en los equipos y caducidad, determinar el tiempo de inactivación.

Los usuarios finales de los equipos de cómputo no deben tener privilegios de administrador esto da cabida a ejecutar código maligno que puede colocar en

situaciones complejas a la empresa, hysolate[10] hace mención al bloque de puertos periféricos.

3.3 DIFERENCIAS EQUIPO BLUETEAM Y CSIRT

Aunque visto desde algún punto de vista parecen que hicieran lo mismo, no es así, el equipo blue team es un grupo de expertos en seguridad informática que analiza la infraestructura de red, equipos (hardware y software) que la componen y locativo de la empresa con el fin de proteger cualquier tipo de información que produzca la organización, junto con sus activos. También conocido como equipo de defensa tiene una ardua labor y es día tras día debe hallar la forma de evitar la fuga de información de la empresa, unas de sus funciones son:

- Parchar software vulnerable.
- Vigilancia constante de la red
- Analizar patrones anormales dentro de la red.
- Trabajar en la mejora continua de la seguridad de la información.
- Velar por protección de los activos de la información.
- Evaluar amenazas que puedan afectar la organización.

El CSIRT es el acrónimo en inglés que al traducirlo es equipo de respuestas ante incidentes de seguridad en ordenadores, este quipo entra en operación cuando la vulnerabilidad es explotada, ayuda a la empresa a tener una recuperación por la vulnerabilidad, este equipo de expertos en seguridad informática su conocimiento se centra en como subsanar los incidentes en el menor tiempo posible, gracias a su

[10] Hysolate. System Hardening Guidelines for 2022: Critical Best Practices. [Sitio Web]. [Consultado 4 octubre de 2022]. Disponible en https://www.hysolate.com/blog/system-hardening-guidelines-best-practices/

estudios y experiencia, techtarget[11] la guía de Nist para el manejo de incidentes la cual indica preparación, detección y análisis, contención y recuperación y por ultimo actividades posterior al incidente y otros autores mencionan funciones tales como:

- Controlar y minimizar daños.
- Preservar la evidencia de lo ocurrido.
- Realizar las actividades necesarias para la recuperación rápida.
- Normalizar operación de la empresa en el menor tiempo posible.
- Documentar la información y compartirla como lección aprendida

Muchas empresas miran estos equipos como gastos innecesarios, otras por su parte no tienen como sostenerlo, el estado colombiano está enterado de ello por eso ha creado unos CSIRT, por nombrar algunos: csirt-gobierno, colcert, csirt-ponal, csirt-asobancaria.

3.4 BLUETEAM CON CIS

La CIS es el centro para la seguridad de internet, es una entidad sin ánimo de lucro coya misión es brindar soluciones en lo que respecta a ciberseguridad.

Sin lugar a duda esta organización hace un gran aporte a la seguridad informática, pues desde la pandemia muchas organizaciones optaron por el trabajo remoto, teniendo la necesidad de extender sus redes hasta ciento de hogares.

[11] TechTarget. CERT vs. CSIRT vs. SOC: What's the difference? [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

Para que los empleados puedan cumplir con sus deberes las empresas se ven obligadas a exponer sus servicios al internet. Esto de igual forma las obliga a proteger la información que puede llegar a estar expuesta, es aquí donde la CIS cobra fuerza, con la puesta en marcha de los controles que indican se puede se mejorarían en la organización la ciber seguridad.

Otra forma de beneficio o aprovechamiento seria el académico, para instruir los miembros del equipo blueteam al igual que los empleados de la empresa, ya que la CIS cuenta con una gran experiencia no solo por los profesionales que allí trabajan, también es basa en información de gobiernos, empresas y el mundo académico del globo terráqueo, toda esta información combinada con la experiencia es de inigualable ayuda para cualquier institución.

3.5 FUNCIONES Y CARACTERISTICAS DE SIEM

Es la abreviación de Security Information and Event Management, herramienta implementada en seguridad informática capaz de detectar responder y neutralizar amenazas.

Menciona nsit “objetivo principal es proporcionar una visión global de la seguridad de las tecnologías de la información”[12] esto se logra por la centralización de los log de eventos, obteniendo características como:

- Centralización de los log para su análisis.
- Respuestas automáticas a eventos y amenazas.

[12] Nsit., ¿Qué es SIEM en seguridad informática? Alcance e implementación. [Sitio web]. [Consulta: octubre 1 de 2022]. Disponible en https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

- Disminuye el tiempo de detección de ataque.
- Análisis en tiempo real.
- Monitores de comportamientos en la red.
- Identificación entre amenazas reales y falsos incidentes.

Unas de las principales SIEM según ambit[13] son:

- IBM Security QRadar.
- McAfee Enterprise Security Manager.
- LogRhythm

Este tipo de soluciones ha tenido gran éxito gracias a la reducción de costos, pues automatiza el proceso, logrando con esto optimizar el recurso humano.

3.6 HERRAMIENTAS DE CONTENCIÓN

3.6.1 Firewall Perimetral de Red.

Dedicado a escanea el tráfico de la red, según la herramienta puedes trabajar todo el modelo OSI, bloqueando o permitiendo de los mismos según las reglas implementadas por el administrador. Esta solución se encuentra tanto en software como hardware.

3.6.2 End Point Disk Encryption.

Se conoce como cifrado de punto final, se trata de un software de cifrado de disco protegiendo los datos contra accesos no autorizados, haciendo que los datos de la

[13] Ambit., ¿Qué significa SIEM y cómo funciona? [Sitio web]. [Consulta: octubre 1 de 2022]. Disponible en https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona#

empresa este complemente asegurados, ya que codifica los datos para que nadie que no tenga la clave de descifrado pueda leerlo. De igual forma protege el sistema operativo de archivos corruptos ya que bloquea los archivos almacenados en pc, servidores, laptops.

3.6.3 Escáner de vulnerabilidades.

Estas herramientas han tenido una gran acogida por las diferentes empresas ya que sirven para evaluar la eficacia y la seguridad de sus sistemas, redes y aplicaciones web. Señala helpsystems “los equipos de seguridad pueden detectar brechas, puntos débiles o una vulnerabilidad en cualquier parte del sistema, la red o las aplicaciones”[14]

[14] Helpsystems., Qué es el escaneo de vulnerabilidades y cómo funciona. [Sitio web]. [Consulta: octubre 1 de 2022]. Disponible en https://www.helpsystems.com/es/blog/escaneo-vulnerabilidades

4. RECOMENDACIONES

Es indispensable tener una lista los activos de información detallada con que cuenta las empresas para saber qué y cómo proteger.

El personal de ti debe tener control de los equipos de la red, asegurado de alguna forma el acceso al mismo me forma física.

Es una buena práctica segmentar la red por dependencias dentro de la organización.

La seguridad de la información es muy importante para cualquier corporación y esta debe ser liderada por los directivos de la misma.

El personal de redes y seguridad informática deben trabajar en sincronía y tener constante comunicación.

Microcad[15] menciona un tip muy importante de la cual ya pocos hablan y es cerrar las sesiones ya que es muy común cerrar el navegador sin terminarla.

Se debe prestar mucha atención a la procedencia de los correos electrónico por este motivo pichincha[16] indica revisar detenidamente los correos eléctricos para evitar ser víctima de phishing

[15] Microcad. 15 CONSEJOS DE SEGURIDAD INFORMÁTICA PARA EL DÍA A DÍA. [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en: https://www.microcad.es/ciberseguridad/consejos-seguridad-informatica/

[16] Banco Pichincha. Diez consejos de seguridad informática para tu día a día. [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en: https://www.pichincha.com/portal/blog/post/consejos-seguridad-informatica

CONCLUSIONES

Con la elaboración del presente trabajo se conoce las leyes colombianas que sanciones el acceso abusivo a sistemas informáticos, de igual forma se evidencia la búsqueda de fallos de seguridad que puede llegar a presentar una infraestructura TI de igual forma el aprovechamiento del mismo por parte del equipo red, que este sirve de insumo el equipo encargado de la defensa para mitigar fallos de seguridad que presenta la red dada por parte dela universidad para tal fin.

BIBLIOGRAFÍA

Ambit. ¿Qué significa SIEM y cómo funciona? [Sitio Web]. [Consulta: octubre 1 de 2022]. Disponible en https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona#

Banco Pichincha. Diez consejos de seguridad informática para tu día a día. [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en: https://www.pichincha.com/portal/blog/post/consejos-seguridad-informatica

Campus Internacional de Ciberseguridad. ¿QUÉ ES EL PENTESTING? [Sitio web]. [Consultado 25 de agosto 2022]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

Ciberseguridad., ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio Web]. [25 de agosto 2022]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Exploitdb. Exploit data base. [Sitio web]. [Consultado 25 agosto de 2022]. Disponible en: https://www.exploit-db.com/

FIRST. Common Vulnerability Scoring System v3.0: Specification Document. [Sitio Web]. [Consulta 3 octubre de 2022]. Disponible en: https://www.first.org/cvss/v3.0/specification-document#:~:text=1.1.&text=CVSS%20is%20composed%20of%20three,time%20and%20across%20user%20environments.

Helpsystems. Qué es el escaneo de vulnerabilidades y cómo funciona. [Sitio Web]. [Consulta: octubre 1 de 2022]. Disponible en https://www.helpsystems.com/es/blog/escaneo-vulnerabilidades

Hysolate. System Hardening Guidelines for 2022: Critical Best Practices. [Sitio Web]. [Consultado 4 octubre de 2022]. Disponible en https://www.hysolate.com/blog/system-hardening-guidelines-best-practices/

Junta de Andalucía. Metodología y Frameworks de testeo de la seguridad de las aplicaciones. [Sitio Web]. [25 de agosto 2022]. Disponible en: http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html

Mestasploit., ¿QUÉ ES METASPLOIT FRAMEWORK Y CÓMO FUNCIONA? [Sitio Web]. [Consulta: septiembre 20 del 2022]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Microcad. 15 CONSEJOS DE SEGURIDAD INFORMÁTICA PARA EL DÍA A DÍA. [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en: https://www.microcad.es/ciberseguridad/consejos-seguridad-informatica/

Microsoft., Windows SMB Remote Code Execution Vulnerability. [Sitio Web]. [Consulta: septiembre 21 de 2022]. Disponible en https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0144

Nsit., ¿Qué es SIEM en seguridad informática? Alcance e implementación. [Sitio Web]. [Consulta: octubre 1 de 2022]. Disponible en https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Rapid7. SMB DOUBLEPULSAR Remote Code Execution. [Sitio web]. [consultado 22 septiembre de 2022]. Disponible en: https://www.rapid7.com/db/modules/exploit/windows/smb/smb_doublepulsar_rce/

TechTarget. CERT vs. CSIRT vs. SOC: What's the difference? [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

Wickr. 7 Steps to Take During a Cyber Attack. [Sitio web]. [Consultado 5 octubre de 2022]. Disponible en https://wickr.com/7-steps-to-take-during-a-cyber-attack/

Link video
https://drive.google.com/file/d/11DTQ-6f45lctviICjqdiwebeqcNnoieS/view?usp=drivesdk