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

JHONNATAN GARCIA MIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD INGENIERÍA Y TECNOLOGÍAS
SEGURIDAD INFORMÁTICA
CURUMANI, CESAR
2020

RESUMEN

El presente informe técnico contiene una descripción de las acciones que se deben realizar frente a incidente de seguridad informática, estableciendo las fases para realizar una auditoría e identificar vulnerabilidades en los sistemas o en los equipos de la red. Se hará una descripción de algunas herramientas utilizadas por el equipo ReadTeam y BlueTeam con un escenario virtual con dos sistemas operativos Windows (victima) y un sistema operativo kali Linux (pentesting).

Con el fin de que toda organización consolide la seguridad información, se nombran estrategias de ciberseguridad para mitigar y contener ataques informáticos y las acciones o protocolo a implementar.

Contenido Pág.

GLOSARIO

- **Ciberseguridad:** conocida también, como seguridad de la información o seguridad informática, se ocupa de la protección de equipos, redes, sistema, red de nodos, aplicando métodos, protocolos y herramientas estándar.

- **ReadTeam:** es el equipo de expertos emulan a un atacante, está encargado de realizar pruebas de vulnerabilidad a los sistemas aplicando diferentes técnicas pivoting, exploits.

- **BlueTeam:** es el equipo de expertos encargado de proteger a las organizaciones de ataques informáticos de manera proactiva

- **Kali Linux:** es un sistema operativo basado en Debian GNU, que cuenta con un conjunto de herramientas para recopilar información, identificación de vulnerabilidades y explotación de los fallos realizando un pentesting (pruebas de penetración) en cada uno de los equipos.

- **SIEM: "**Es un tipo de software con la capacidad de detectar fallos y amenazas de seguridad en un sistema"[1], usando un procedimiento estandarizado por normas y protocolos en seguridad informática

- **CIS: "**Centro para la Seguridad de Internet, organización sin ánimo de lucro maneja las mejores prácticas a nivel mundial para proteger los sistemas y la tecnología de la información" [2] . Contiene módulos avanzados para organizaciones gubernamentales y distintas instituciones, generando un ambiente de confianza en el ciberespacio.

- **Nmap:** Analizador de red versátil y eficaz que existe como herramienta de software libre en el mercado, identifica servidores, computadoras en red realizando una lista a las que responden el ping.

---

[1] SOFECOM, blog. Qué es un sistema SIEM. Madrid: Alcobendas, 2015, p.1.

[2] CIS, Center for Internet Security. Mejores Prácticas de Ciberseguridad. EE. UU: Nueva York, 2020

1. INTRODUCCIÓN

En el presenten informe técnico para la organización WhiteHouse Security se establecen las estrategias de contención de acuerdo a un análisis de riesgo y vulnerabilidades ejecutado en una infraestructura de red. Se define aportes para fortalecer las habilidades técnicas del equipo de RedTeam y BlueTeam, a su vez recomendaciones para consolidar la seguridad de la información con herramientas de software. Para finalizar formular conclusiones que permitan fortalecer el conocimiento sobre la seguridad de la información o ciberseguridad.

2. OBJETIVO GENERAL

Formular métodos de contención por medio de análisis y vulnerabilidades en la infraestructura de red organización WhiteHouse Security.

3. OBJETIVOS ESPECIFICOS

- Enunciar el marco legal sobre delitos informáticos, protección de datos y las fases de auditoria en una infraestructura de red.

- Mostrar el análisis de riesgo y vulnerabilidad en los sistemas operativos Windows 7 de la organización WhiteHouse Security

- Sugerir herramientas para estrategias de RedTeam y BlueTeam que detengan los incidentes en la infraestructura de red WhiteHouse Security

CAPITULO 1. ENUNCIAR EL MARCO LEGAL SOBRE DELITOS INFORMÁTICOS, PROTECCIÓN DE DATOS Y LAS FASES DE AUDITORIA EN UNA INFRAESTRUCTURA DE RED

4. MARCO LEGAL

En Colombia la ley que rige los delitos informáticos está contemplada en la ley 1273 del 2009, en donde se modifica el código penal y se crea el bien jurídico tutelado de la protección de la información y de los datos.

Señalando las penas de prisión sobre el acceso abusivo a un sistema informático, la obstaculización ilegitima de sistemas o redes de comunicación, la interceptación sin orden judicial de los datos, sobre el daño informático, sin tener autorización, el uso de software malicioso que ocasione daños informáticos, en que sin estar facultado viole los datos personales para beneficio propio o de terceros y la utilización de sitios web sin autorización para capturar información.
El decreto presidencial 1377 de fecha 27 de junio de 2013, el cual reglamenta parcialmente la ley 1581 de 2012 señalando el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de nuestra constitución política.

5. ETAPAS DEL PENTESTING

"En las auditorias de pentesting, procedimientos autorizados para detectar vulnerabilidades en el sistema, es importante identificar cuál es el sistema a auditar para utilizar las herramientas correspondientes; las fases establecidas para realizar pruebas de penetración son las siguientes"[3]:

5.1 Fase 1. Recopilar información del sistema: Recopilar la mayor información del sistema auditar, definir con el cliente el objetivo del pentesting, los riesgos que podría generar una caída del sistema en consecuencias perdidas económicas, vulnerabilidad de sus bases de datos lo que conlleva a robo de información,

[3] HACKING, Pentesting. Fases de Auditoria. España, 2017, p.1.

definir el alcance de la prueba de penetración definiendo cuales serían los servicios o equipos que se van analizar, establecer en que momentos se realizará el pentest, si en su momento se usarán exploit para servicios vulnerables o solo bastará con ser identificados y definir a quien se debe informar en caso de detectar una vulnerabilidad critica en el sistema.

La información del sistema es de vital importancia, por eso es importante identificar por medio de herramientas monitoreo, **Nmap** sería una herramienta importante detecta puertos, servicios y dispositivo, identificar sistemas operativos y servicios disponibles.

5.2 Fase 2. Búsqueda de Vulnerabilidades: Una vez recopilada la información del sistema, de los servicios o equipos a auditar, se realiza una búsqueda de vulnerabilidades, una herramienta importante para esta fase es **NESSUS** es un programa de escaneo de vulnerabilidades para diferentes sistemas operativos en tiempo real, detecta errores y debilidades en las configuraciones.

5.3 Fase 3. Explotación de Vulnerabilidades: Identificadas las vulnerabilidades, se realiza una explotación para obtener acceso al sistema, ejemplo: Un cifrado débil de un password, una herramienta importante para esta fase es **Metasploit**; es un programa diseñado para explotar vulnerabilidades, metasploit maneja una serie de herramientas y programas que se ejecutan en las vulnerabilidades del sistema.

5.4 Fase 4. Post – Explotación: Consiste en una recopilación de la información en la fase de explotación para posteriormente tomar acciones para mitigar las vulnerabilidades.

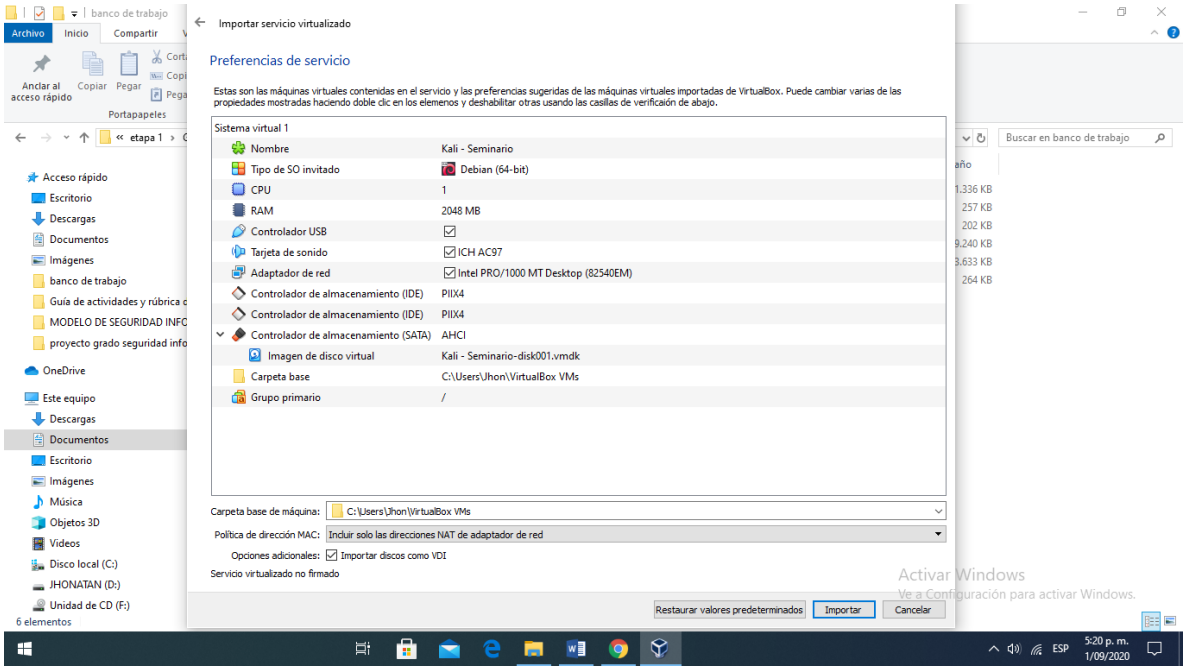
5.5 Fase 5. Elaboración de Informes: Una vez finaliza la fase de explotación se debe rendir un informe al cliente y al personal encargado de las TI, este informe debe dividirse en un informe ejecutivo; explicando las vulnerabilidades descubiertas con las acciones a tomar, resaltando aquellos puntos donde se implementó la seguridad de maneta correcta, y un informe con detalles técnicos de la auditoria que será dirigido al personal del departamento de las TI.

CAPITULO 2. MOSTRAR EL ANÁLISIS DE RIESGO Y VULNERABILIDAD EN LOS SISTEMAS OPERATIVOS WINDOWS 7 DE LA ORGANIZACIÓN WHITEHOUSE SECURITY

1. BANCO DE TRABAJO

En primer lugar para el banco de trabajo es instalar VirtualBox-6.1.12-139181-Win teniendo en cuenta las características de mi equipo, se descarga los archivos .ova ubicados en foro en un link drive. Posterior, abrimos cada uno de los discos virtuales y los importamos a nuestro VirtualBox.

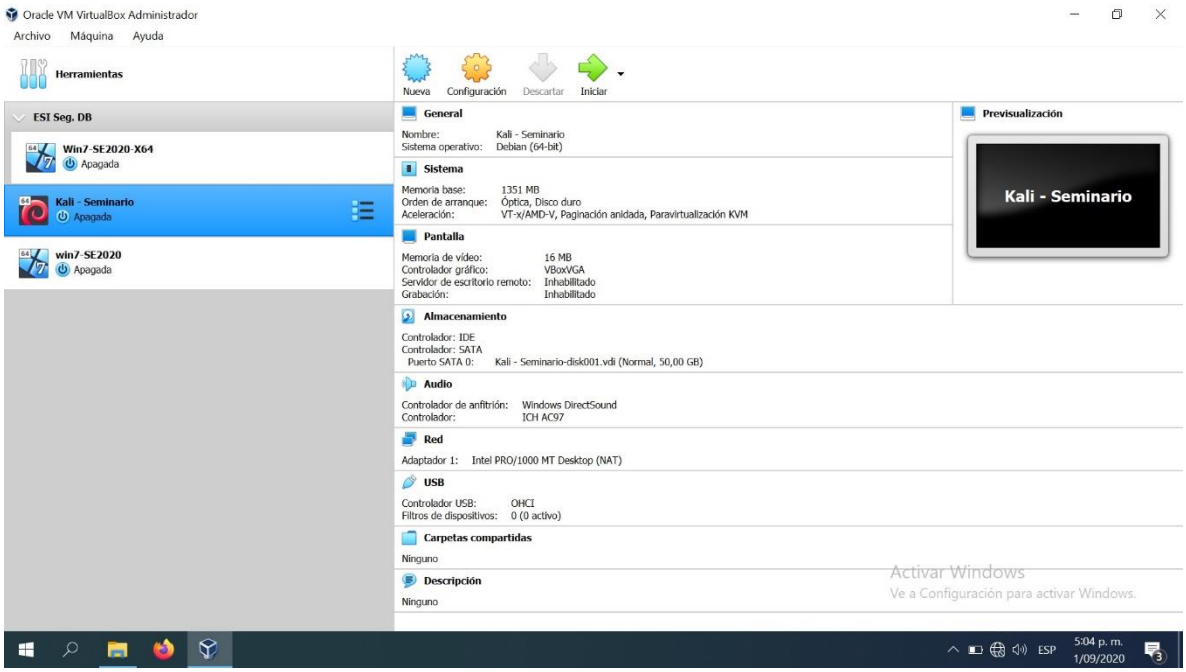
Figure 1. Importar sistema Operativo



El Autor.

La siguiente imagen muestra el sistema operativo kali Linux Debian 64bit, memoria base 1351MB importado en la máquina virtual (virtual box)

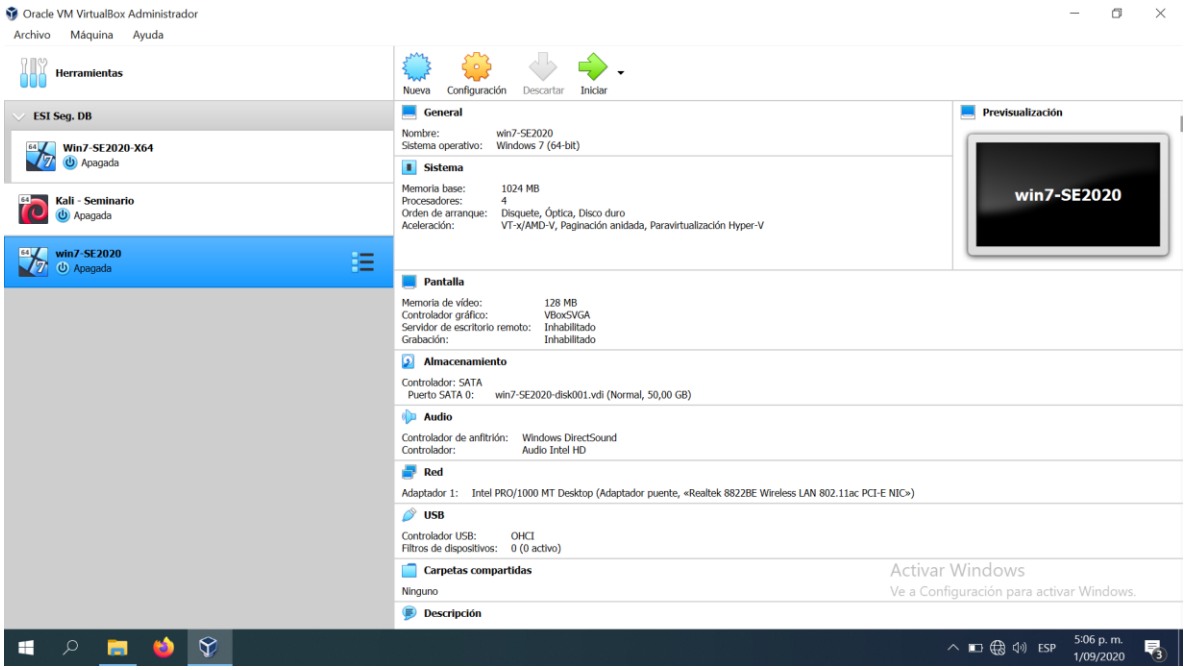
Figure 2. Instalación Sistema Operativo Kali



El Autor.

La siguiente imagen muestra el sistema operativo sistema operativo Windows 7 32bit, memoria base 1024MB instalado en la máquina virtual box

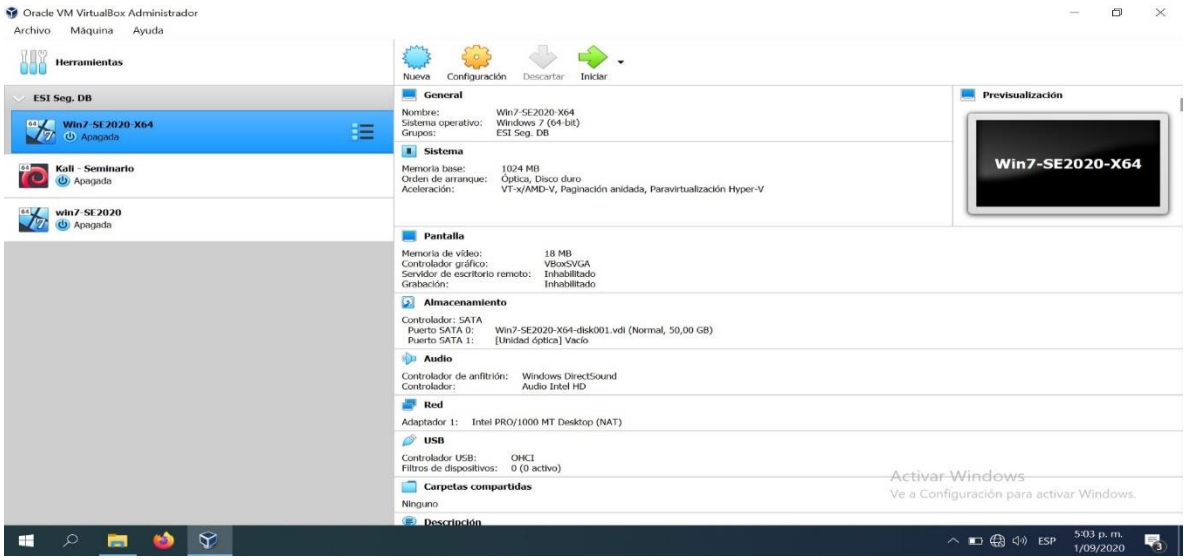
Figure 3. Instalación Windows 7 32bits



El Autor.

La siguiente imagen muestra el sistema operativo Windows 7 64Bit, memoria base 1024MB, GRUPO ESI.SEG.BD, importado e instalado en la máquina virtual box.

Figure 4. instalación sistema operativo Windows 32bit

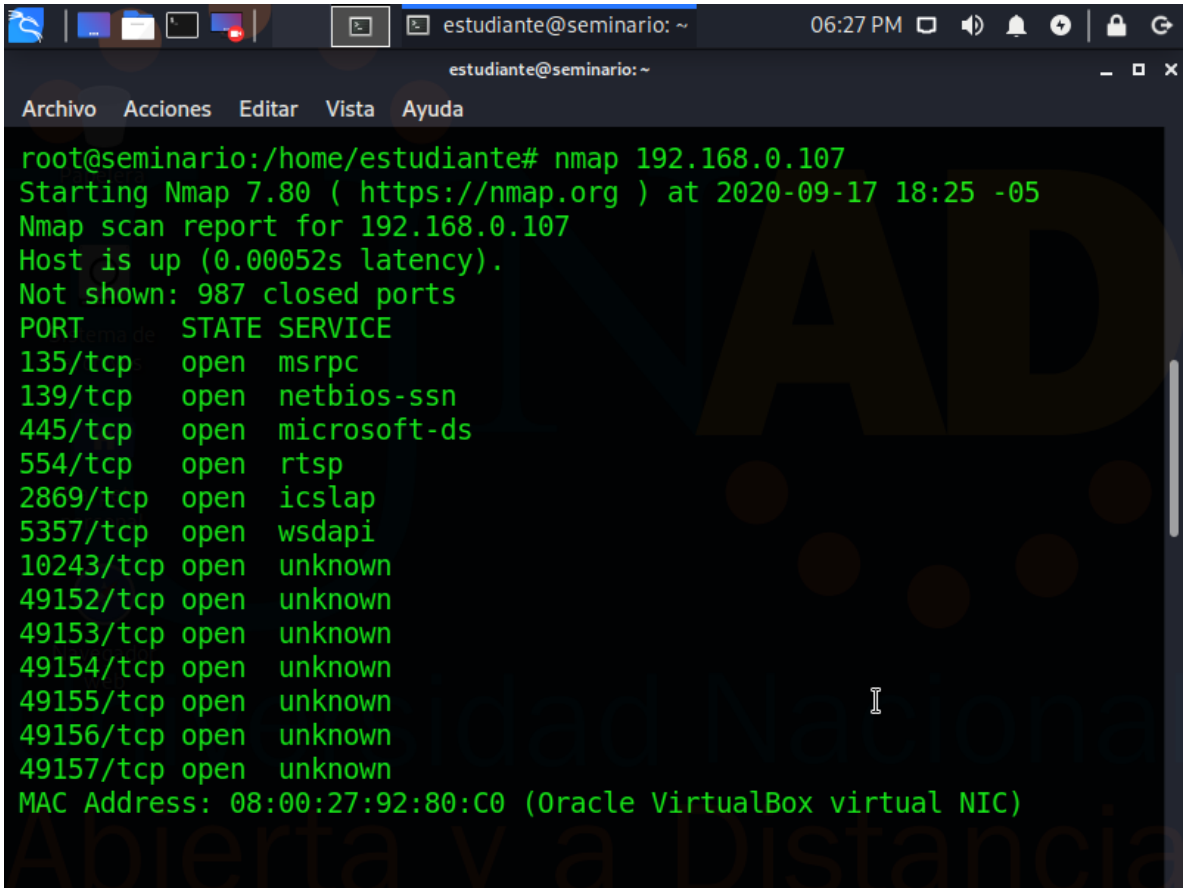


El Autor.

2. PENTESTING MAQUINA WINDOWS 7 64BIST

la herramienta para iniciar nuestro análisis partiendo de la fase de recopilación de información es Nmap, escribimos el comando para identificar los puertos, estado y servicios arrojado el siguiente resultado como lo muestra la siguiente imagen.

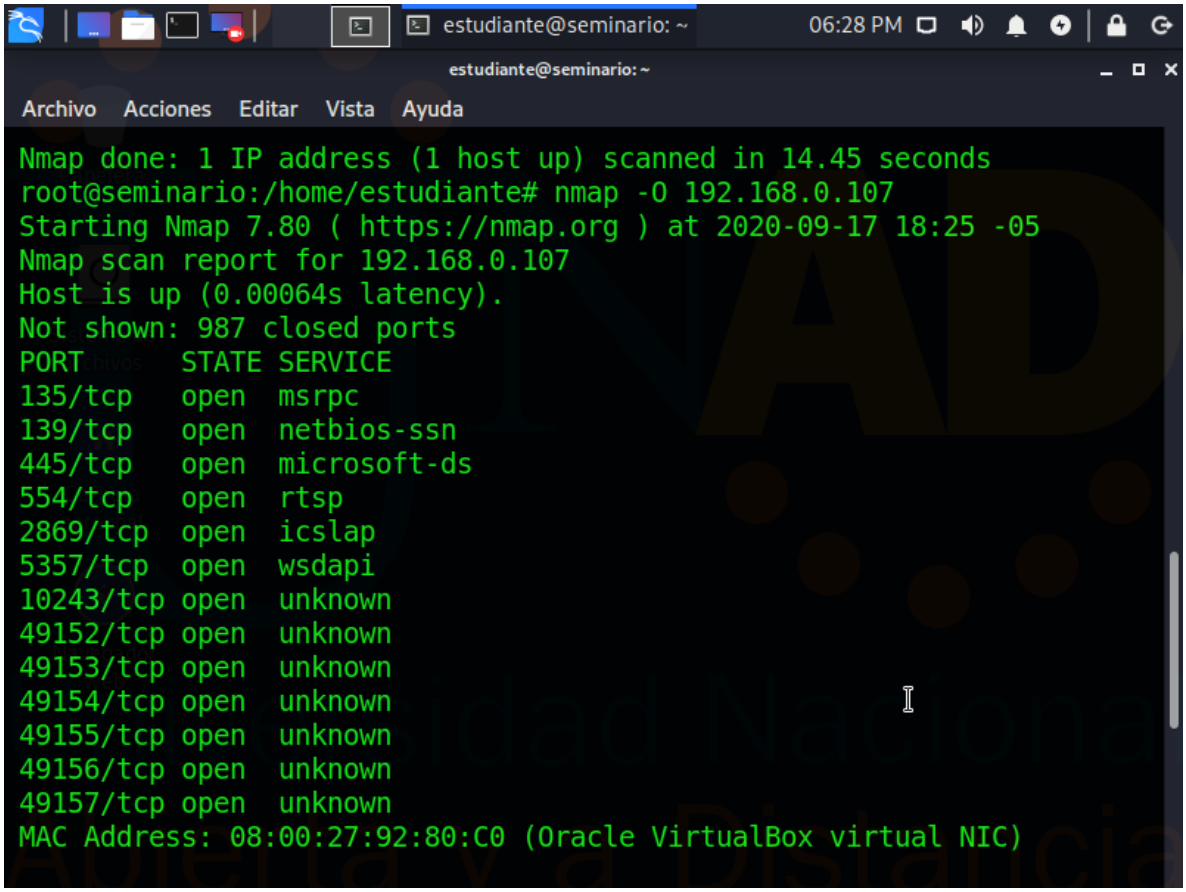
Figure 5. Identificación de Puertos



Fuente. El autor

Continuando con la recopilación de información a nuestra maquina víctima, identificamos el sistema operativo utilizando el siguiente comando **nmap –O 192.168.0.107** como lo enseña la imagen

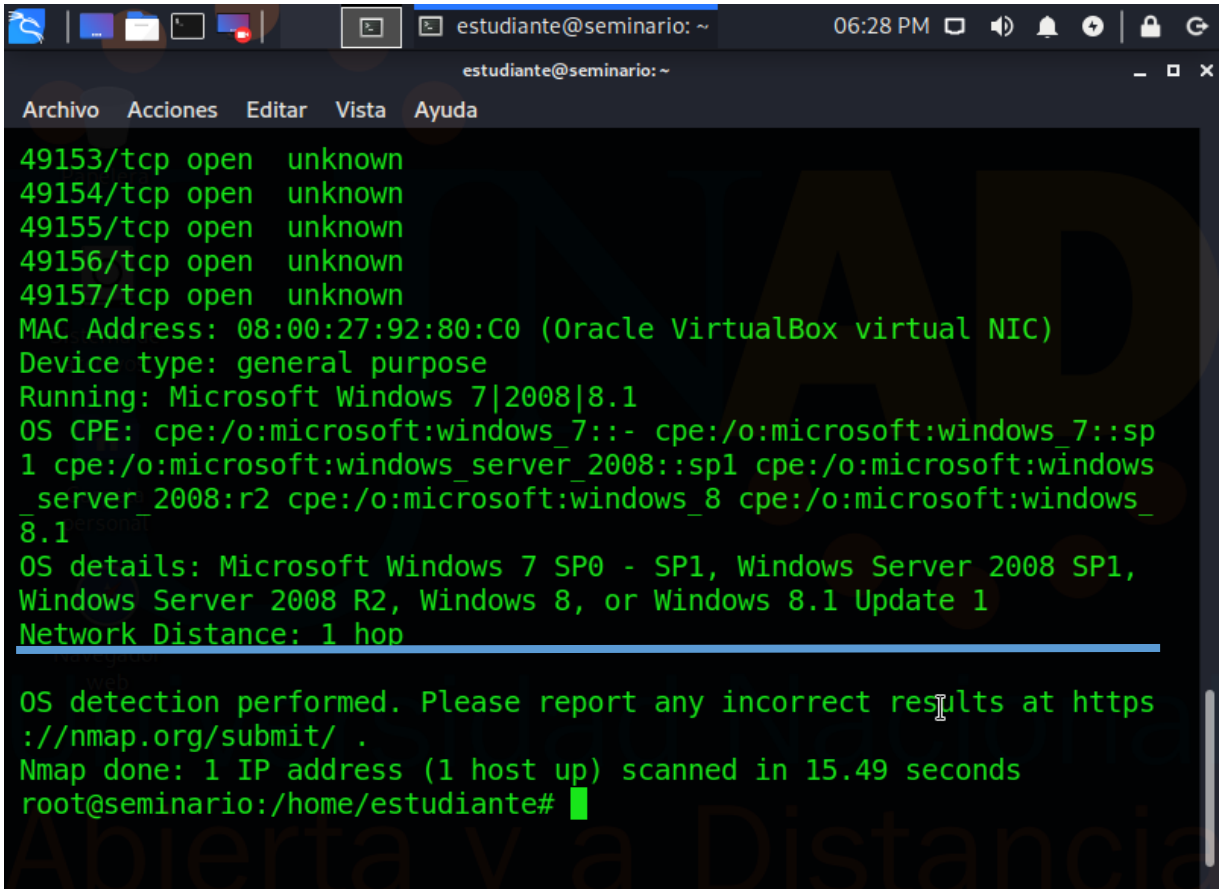
Figure 6. Identificación sistema operativo



Fuente. El autor

La siguiente imagen muestra la descripción del sistema operativo de la maquina victima organización WhiteHouse Security

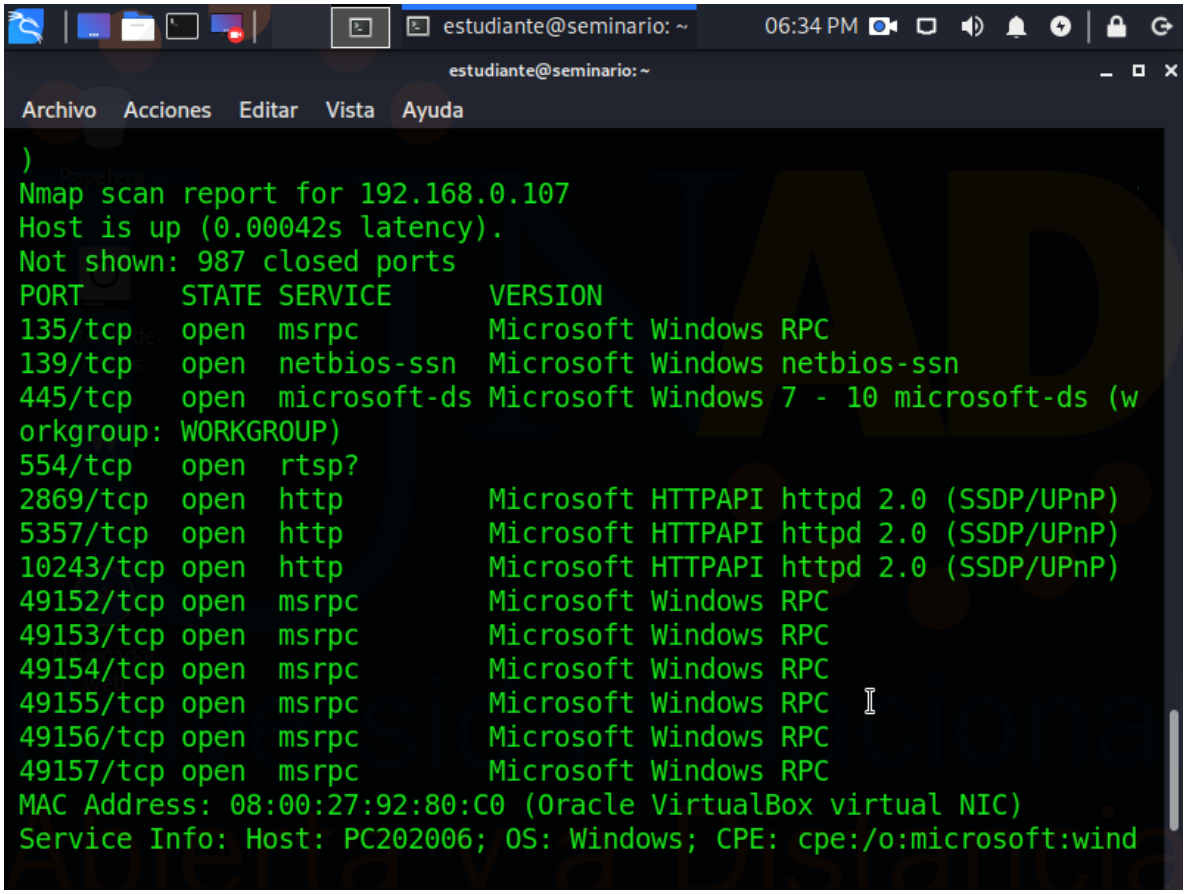
Figure 7. Descripción Sistema Operativo



Fuente. El autor

Por medio de siguiente comando **nmap –sV 192.168.0.107** identifica los puertos, estados, servicio y las versiones de nuestro equipo víctima. Tal como lo enseña la siguiente imagen

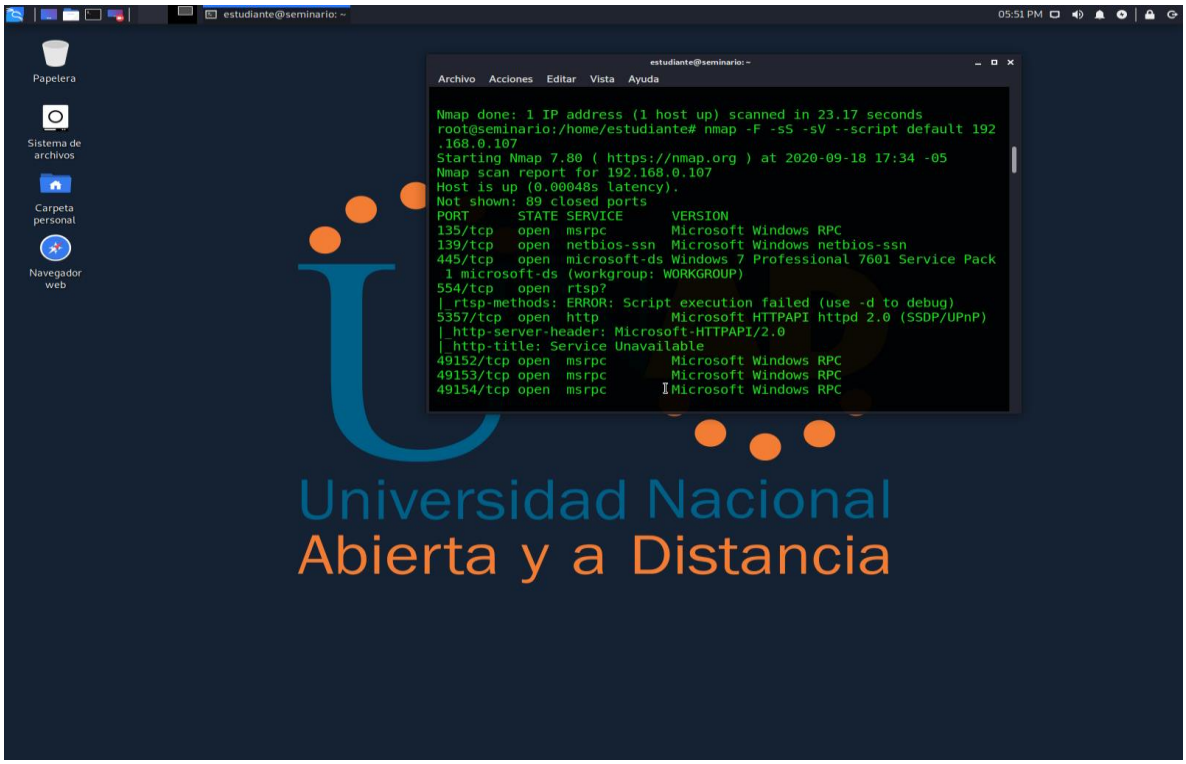
Figure 8. Estado, servicios y versión



Fuente. El autor

Iniciamos **la segunda fase**, consiste en buscar vulnerabilidades en el sistema, lazamos un script para ayudarnos a identificar características principales del sistema como: sistema operativo, servicios, dirección MAC, nombre del equipo, Netbios, modo de seguridad

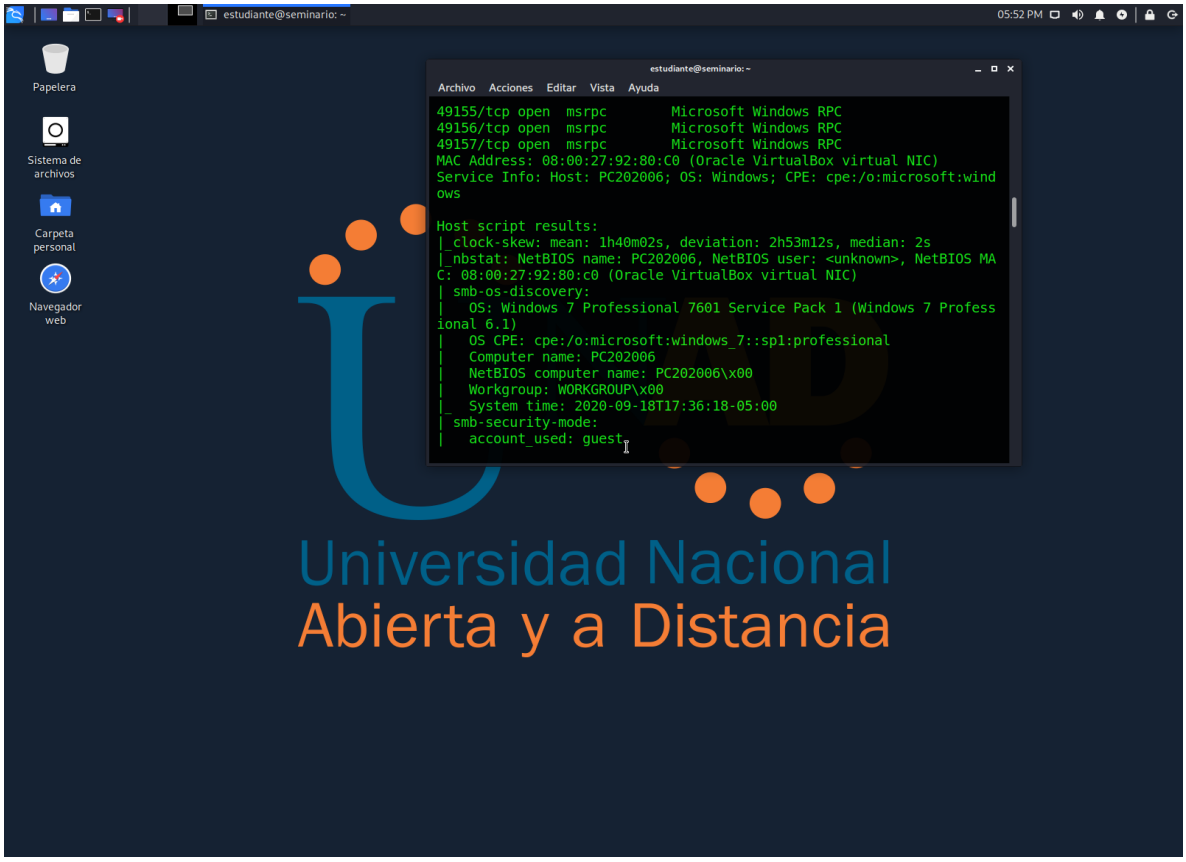
Figure 9. Características Principales



Fuente. El autor

Descripción de las características del sistema operativo Windows 7 64 bits (equipo victima).

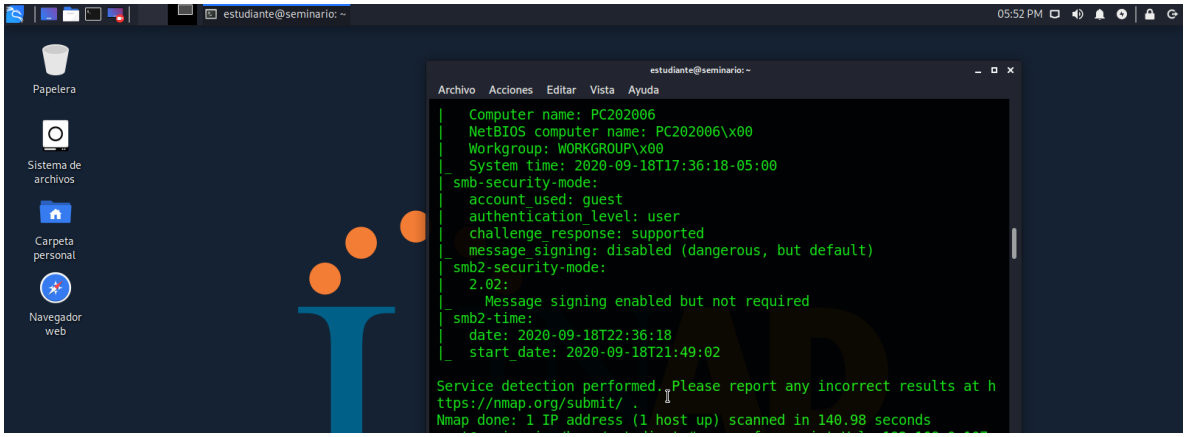
Figure 10. Resultado script Host



Fuente. El autor

Continua la descripción de las características con base al script ejecutado al equipo victima Windows 7 64 bits.

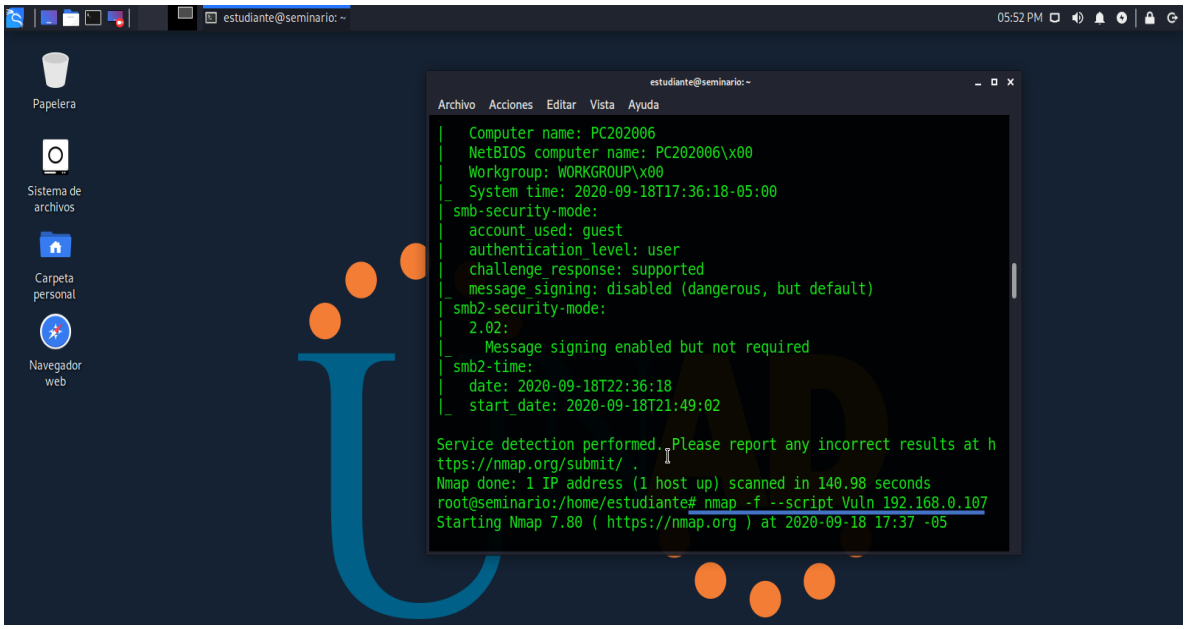
Figure 11. Resultado Script Host



Fuente. El autor

Continuando, lanzamos un scritp para identificar las vulnerabilidades que existen en la maquina víctima, arrojando como resultado vulnerabilidad de ejecución remota de código en Microsoft nivel alto, Con IDs (SIGLA DE VULNERABILIDAD, AÑO DE RESGISTRO Y NUMERO ASIGANDO DE VULNERABILIDAD) CVE-2017-0143.

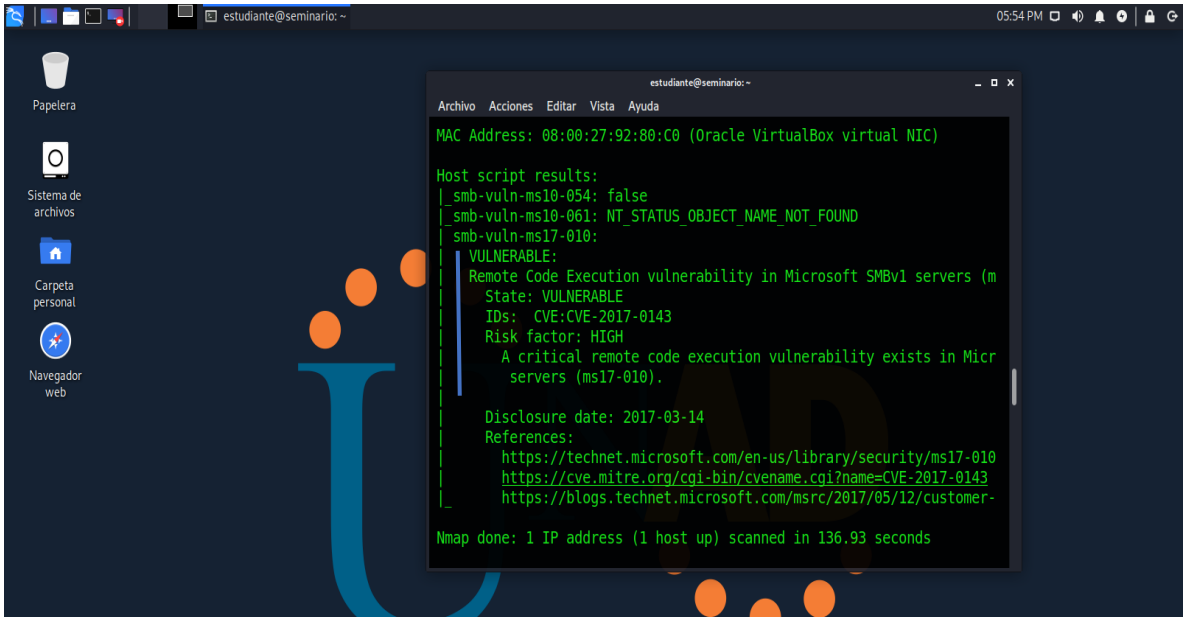
Figure 12. Script Identificación de Vulnerabilidades



Fuente. El autor

la siguiente imagen es el resultado de las vulnerabilidades detectadas en el sistema operativo Windows 7 64bits equipo victima a consecuencia del script **nmap –f --script Vuln 192.168.0.107**

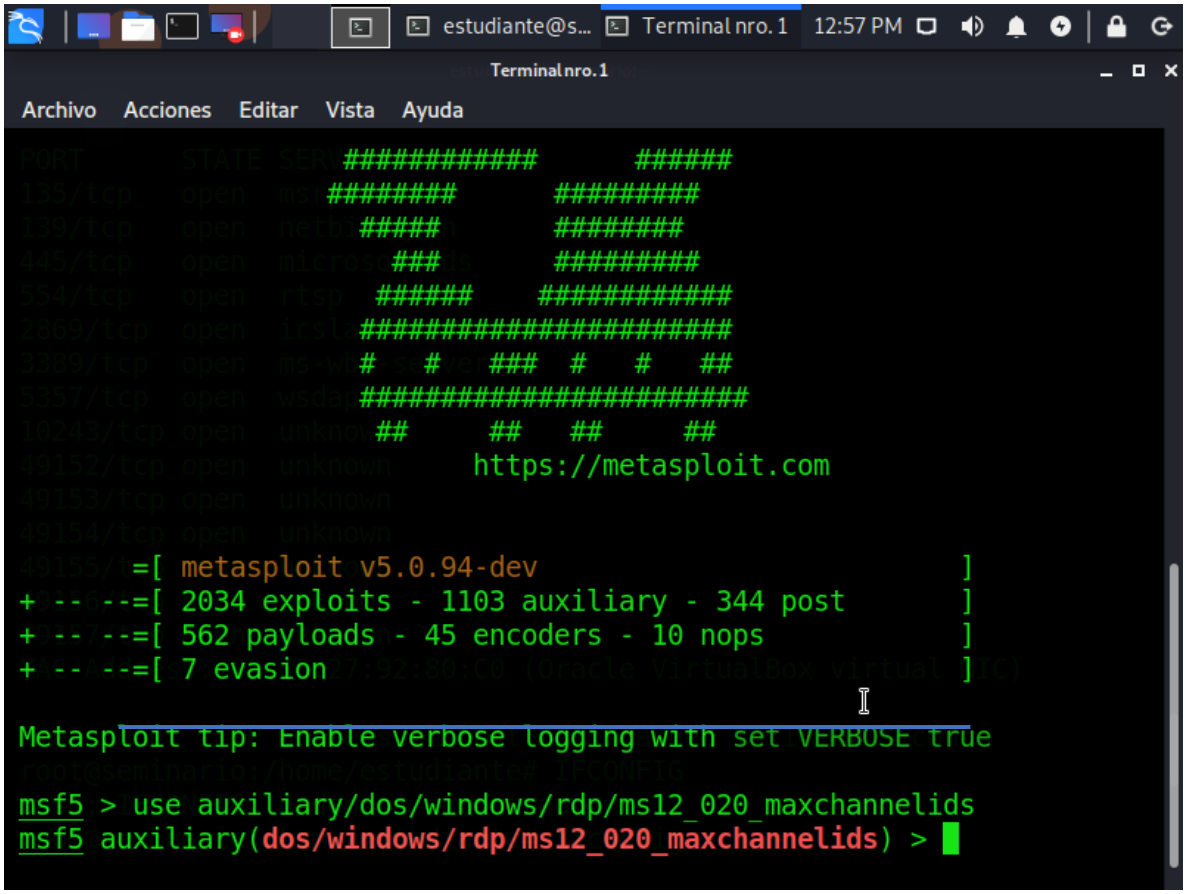
Figure 13. Resultado Vulnerabilidades



Fuente. El autor

Una vez identificadas las vulnerabilidades de acceso remoto nivel alto iniciamos la **fase de explotación** en la maquina víctima. En esta oportunidad vamos a generar un exploit que colocara la pantalla azul y reiniciara nuestro Windows 64bits. Para ello se utiliza la herramienta metasploit, se escribe el script que aparece señalado en la línea azul, este es el exploit que causara un error a la maquina victima generando un una pantalla azul y el reinicio del sistema

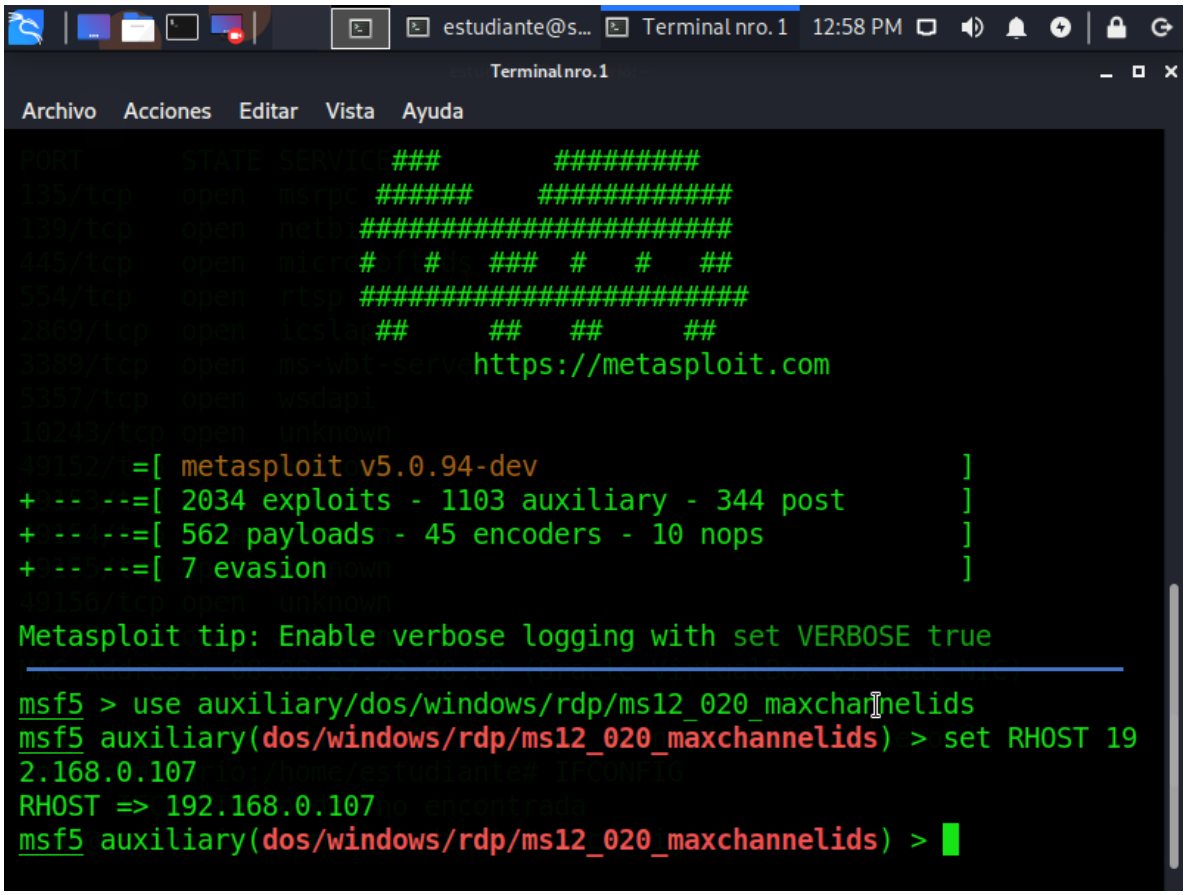
Figure 14. Uso de Exploit



Fuente. El autor

Luego ingresamos la IP de nuestra maquina víctima en este caso es el host Windows 64 bit por medio del siguiente comando

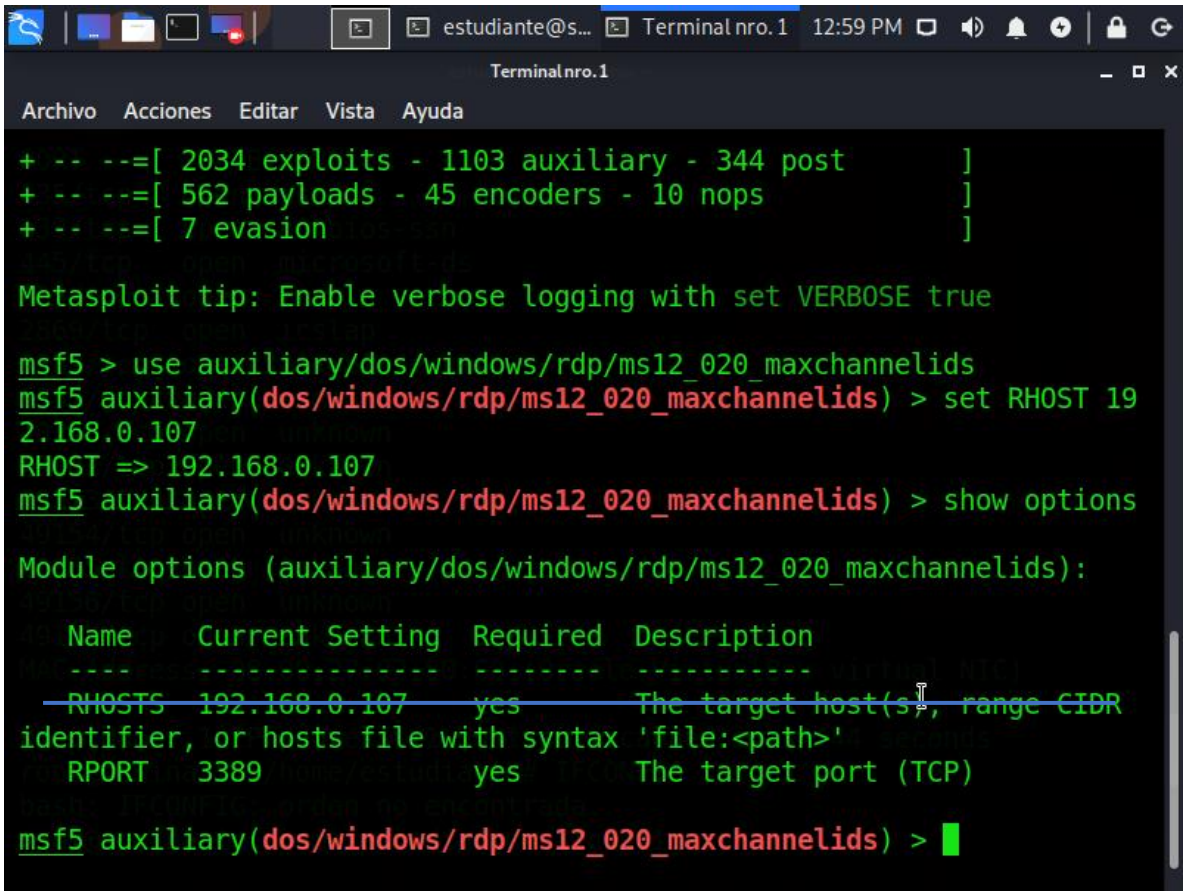
Figure 15. Ingresar IP maquina victima



Fuente. El autor

La siguiente imagen son las opciones en la configuración del exploit muestra la IP de la host víctima y el puerto por defecto 3389, este puerto se habilita cuando activamos la opción permitir acceso remoto desde la opción sistema, configuración acceso remoto del equipo Windows y se puede validar haciendo un escaneo de puertos desde el terminar de kali Linux.

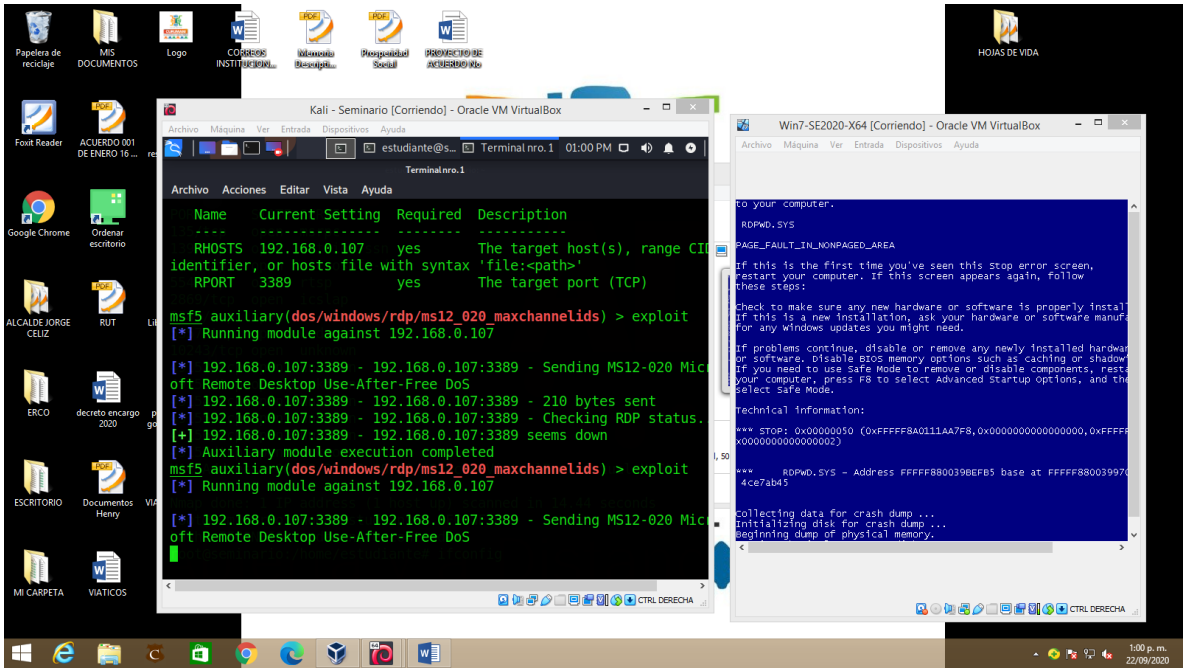
Figure 16. Ingreso a las opciones



Fuente. El autor

Teniendo la configuración establecida, IP víctima y puerto habilitado lanzamos el exploit lo cual causa un error en el Windows 7, generando una pantalla azul y el reinicio del sistema operativo como nos muestra la siguiente imagen.

Figure 17. Exploit Genera pantalla azul

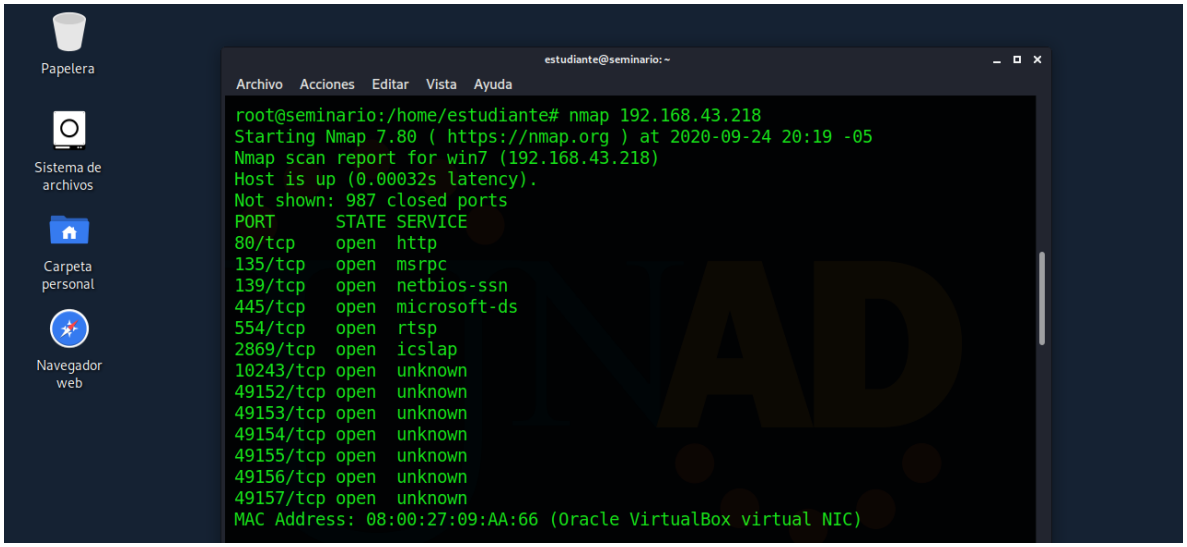


Fuente. El autor

3. PENTESTING MAQUINA WINDOWS 7 32BIST

Se identifica el host analizar en este caso tuve que cambiar de equipo por problemas técnicos y luz en el municipio donde laboro. Una vez identificada la IP 192.168.43.218 del equipo Windows iniciamos la **fase de recopilación de información**, lanzamos el script nmap 192.168.43.218 para identificar puertos estados y servicios.

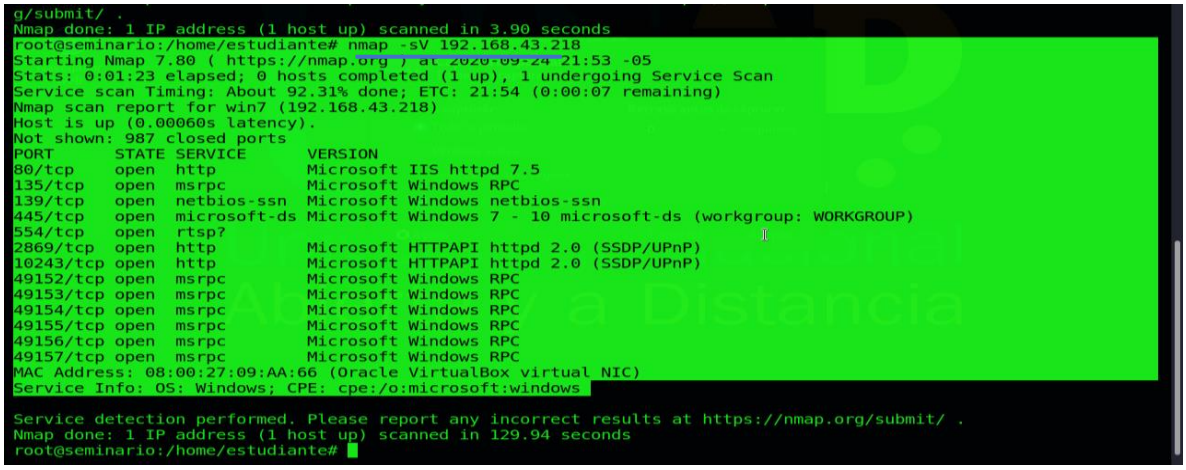
Figure 18. Identificación de puertos



Fuente. El autor

El siguiente script **nmap –sV 192.168.43.218**, permite identificar los servicios disponibles en los puertos en el equipo víctima.

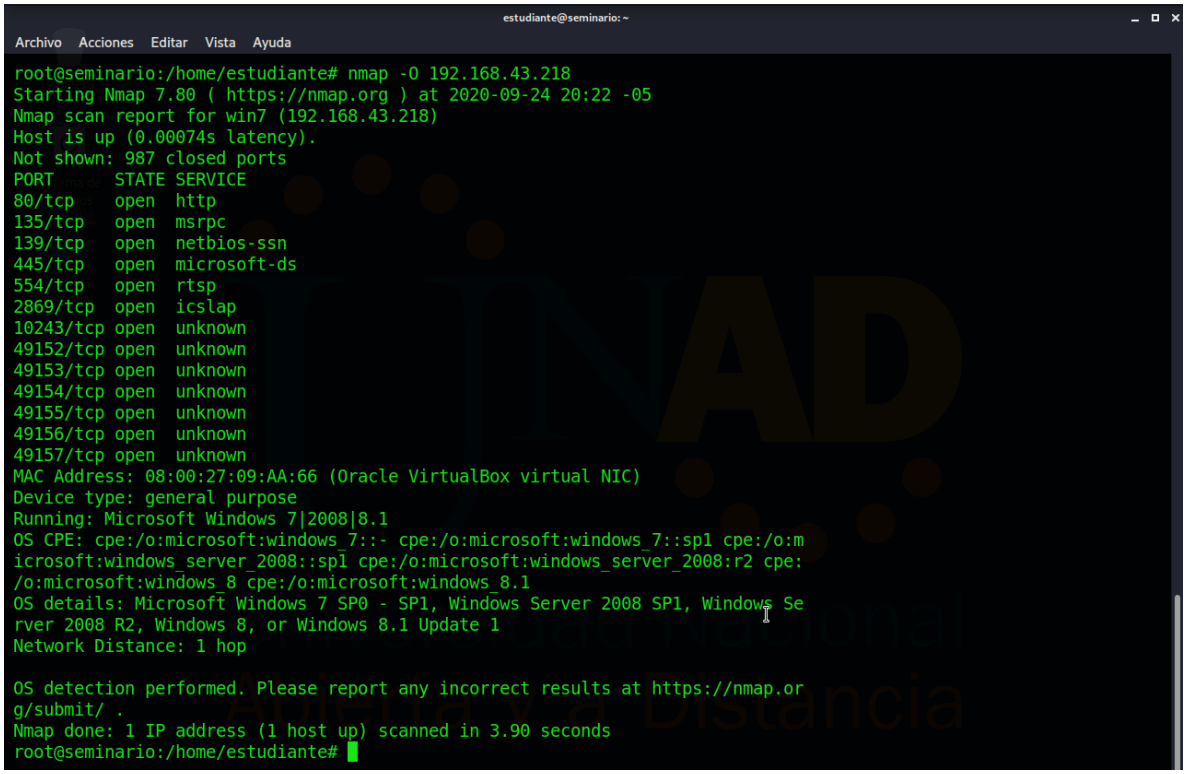
Figure 19. Servicios disponibles



Fuente. El autor

Identificación sistema operativo, dirección MAC del equipo victima por medio del siguiente comando, nmap –O 192.168.43.218

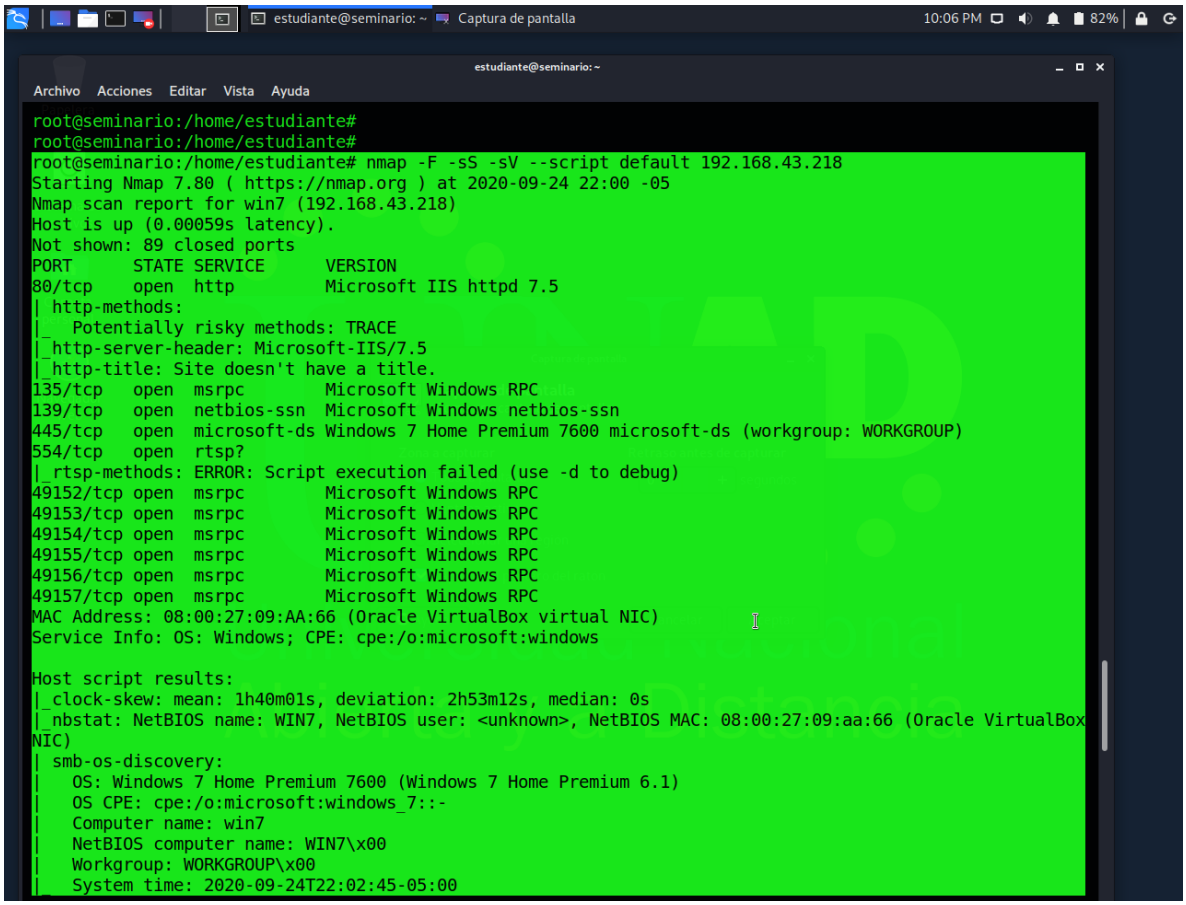
Figure 20. Identificación sistema operativo



Fuente. El autor

Segunda fase identificación de vulnerabilidades enviamos un script al equipo víctima para determinar las características, puertos y su estado, servicios, errores, el estado del protocolo SMB para compartir, archivos, impresoras etc.

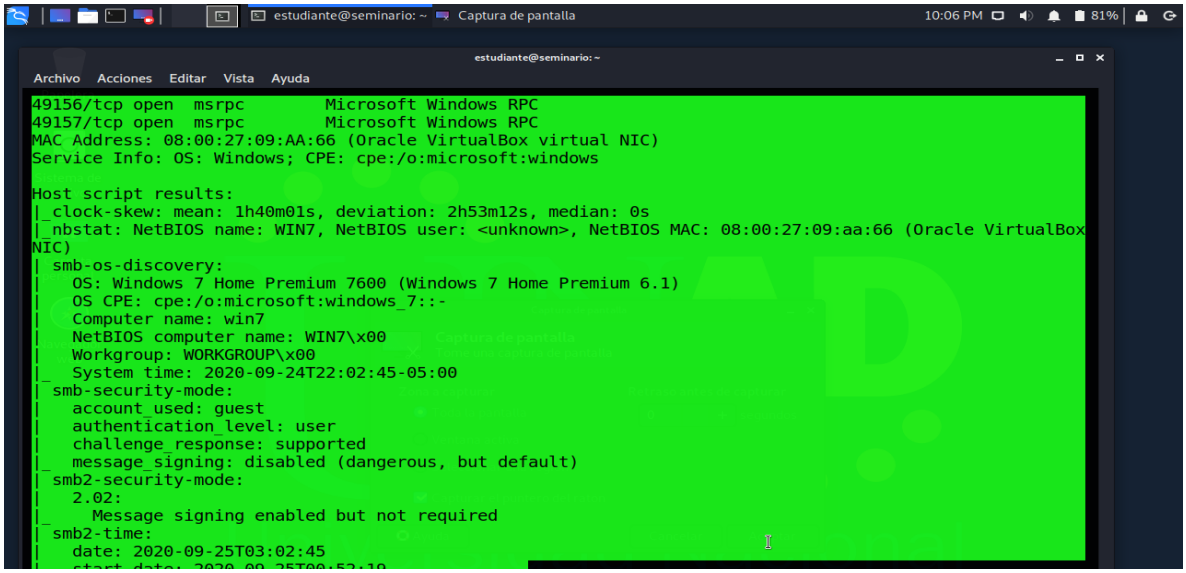
Figure 21. Características principales



Fuente. El autor

Descripción de puertos y su estado, servicios, errores, el estado del protocolo SMB para compartir, archivos, impresoras etc.

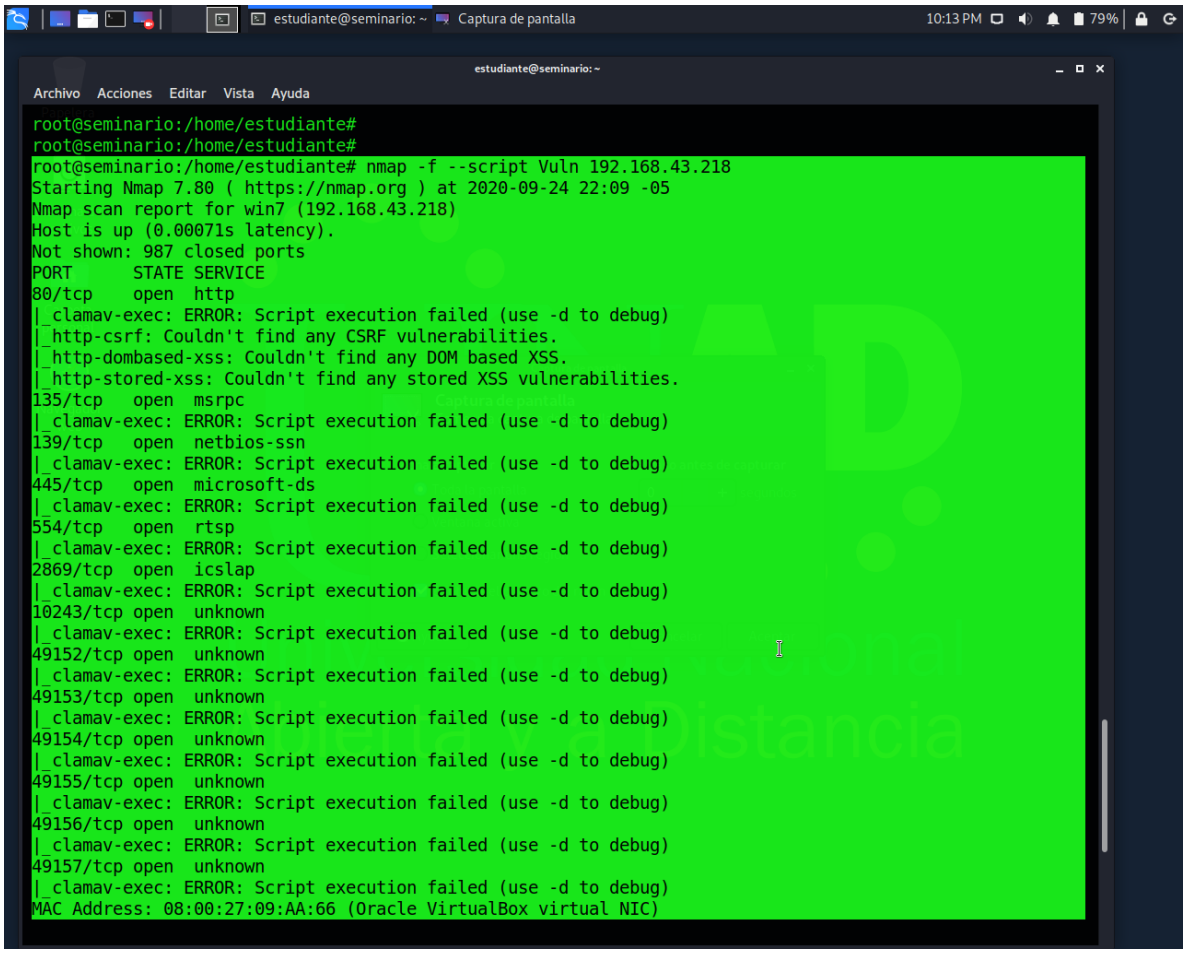
Figure 22. resulta script host



Fuente. El autor

Ahora hacemos un análisis de vulnerabilidades del sistema por medio de la siguiente script con la herramienta nmap en el equipo victima Windows 7 32 bits.

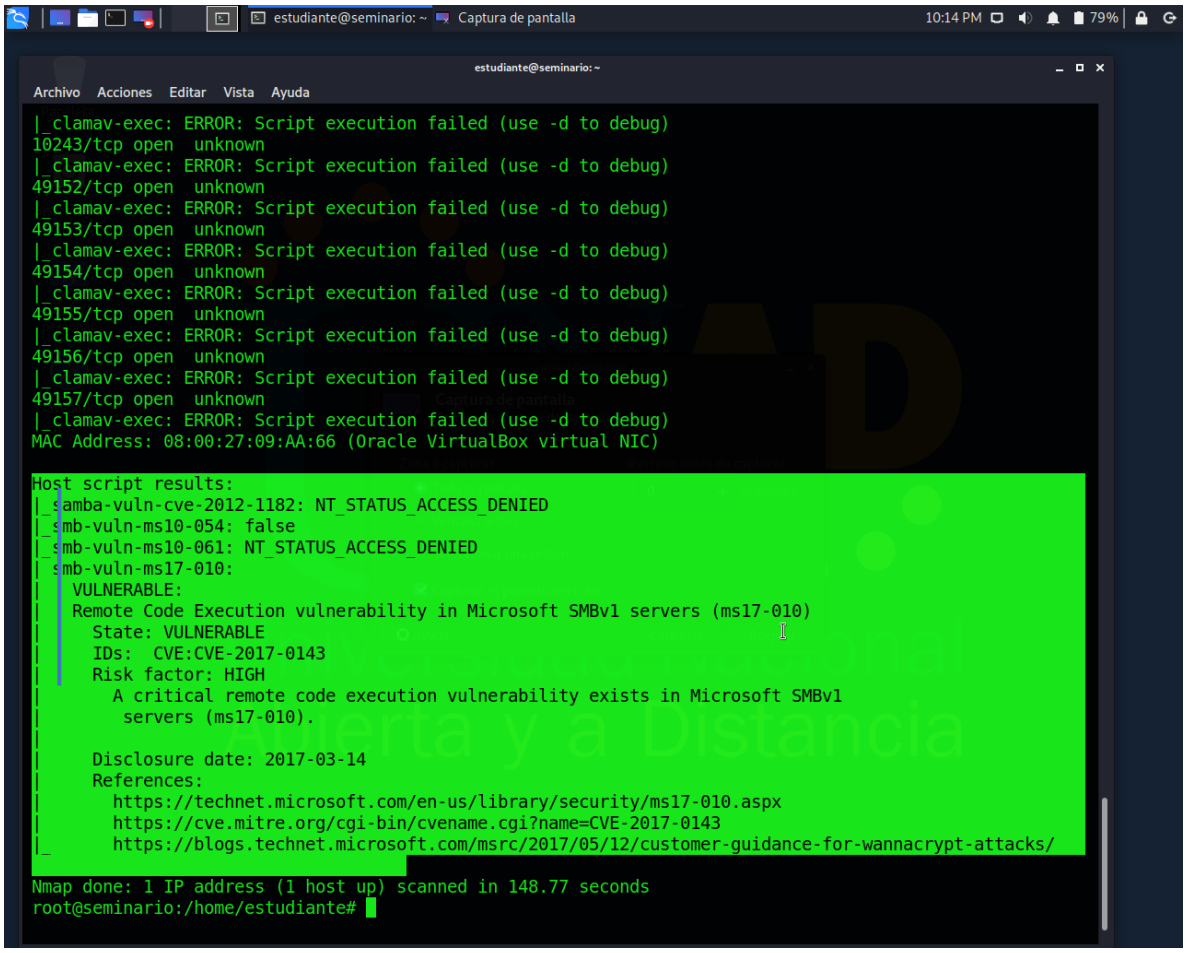
Figure 23. Análisis de vulnerabilidades



Fuente. El autor

Continuando, lanzamos un scritp para identificar las vulnerabilidades que existen en la maquina víctima, arrojando como resultado vulnerabilidad de ejecución remota de código en Microsoft nivel alto, Con IDs (SIGLA DE VULNERABILIDAD, AÑO DE RESGISTRO Y NUMERO ASIGANDO DE VULNERABILIDAD) CVE-2017-0143

Figure 24. Resultado vulnerabilidades



Fuente. El autor

Es importante tener presente: el Windows professional trae por defecto la opción de permitir acceso remoto por tal razón es vulnerable a acciones remotas, en cambio el Windows 7 home Premium no trae por defecto esa opción, sólo a partir del Windows 7 professional, en consecuencia, no habilita el puerto remoto para enviar el exploit que genera error y pantalla azul

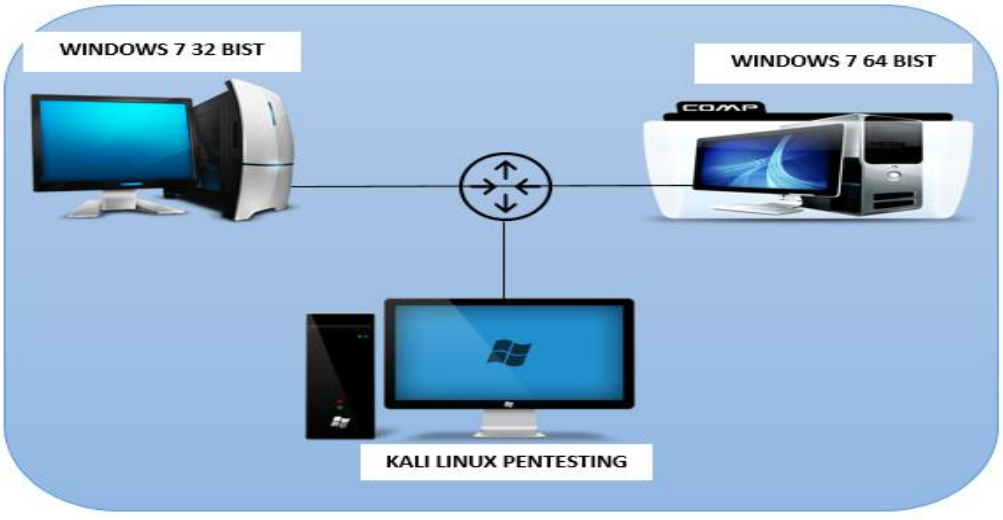
4. TABLA DE FALLOS DE SEGURIDAD

Table 1. Descripción de las vulnerabilidades

Sistema Operativo	Categoría	Descripción general
Windows 7 64bits	Smb-vul sm10-54	Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código
	Smb-vul sm10-61	Vulnerabilidad critica en los trabajos de impresión en equipos con sistema operativo Windows 2008/ 7 / vista/ XP/ 2000
	Smb-vul sm17-010	Vulnerabilidad sobre ejecución sobre el protocolo de red SMB que permite compartir archivos, impresoras y demás
Sistema Operativo	**Categoría**	**Descripción general**
Windows 7 32bits	Smb-vul sm10-54	Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código
	Smb-vul sm10-61	Vulnerabilidad critica en los trabajos de impresión en equipos con sistema operativo Windows 2008/ 7 / vista/ XP/ 2000
	Smb-vul sm17-010	Vulnerabilidad sobre ejecución sobre el protocolo de red SMB que permite compartir archivos, impresoras y demás
IDS(DESCRIPCIÓN DE LA VULNERABILIDAD): CVE: CVE-2017-0143		

Fuente. El autor

Figure 25. Escenario de Análisis Vulnerabilidades



Fuente. El autor

CAPITULO 3. SUGERIR HERRAMIENTAS PARA ESTRATEGIAS DE REDTEAM Y BLUETEAM QUE DETENGAN LOS INCIDENTES EN LA INFRAESTRUCTURA DE RED WHITEHOUSE SECURITY

5. CIS (CENTRO PARA LA SEGURIDAD DE INTERNET)

CIS es una organización sin ánimo de lucro maneja las mejores prácticas a nivel mundial para proteger los sistemas y la tecnología de la información. Lo utilizaría para actualizar, implementar y consolidar los mejores controles en seguridad de la información para proteger la infraestructura de red, prevenir y controlar riesgos, amenazas, vulnerabilidades y ataques de ciberseguridad. Teniendo en cuenta que la organización (CIS CENTRO PARA LA SEGURIDAD DE INTERNET) Contiene módulos avanzados para organizaciones gubernamentales y distintas instituciones, generaría un ambiente de confianza en el ciberespacio.

6. SIEM (SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD)

Es un tipo de software con la capacidad de detectar fallos y amenazas de seguridad en un sistema, usando un procedimiento estandarizado por normas y protocolos en seguridad informática. Es una herramienta de carácter relevante para proteger, robustecer la seguridad de la información en el interior y exterior de las organizaciones.

Características Principales

Arquitectura

El sistema de gestión de información y eventos de seguridad debe estar en las condiciones de distribuir los componentes en varios equipos para aumentar la capacidad de procesamiento, también permitir sectores con procesamientos para paralelos y transmitir datos alta velocidad en caso de ser solicitados, se pueden manejar entornos físicos o virtuales, mejorando el rendimiento para lograr los resultados óptimos.

Despliegue, operaciones y soporte

Contar con la capacidad para que las aplicaciones específicas del negocio cumplan con las diferentes necesidades, implementación de indicadores y de investigación en los procesos de desarrollo del negocio.

Administración de datos y logs

Tener la capacidad de recolectar logs (grabación secuencia de un archivo) y datos de todo emisor y receptor, en los protocolos de red TCP O UDP. Se contextualiza la información con el fin de detectar amenazas y control sobre el rendimiento de la red.

Amenaza y contexto.

Categorizar los activos físicos, lógicos y humanos por nivel de riesgo, teniendo presente las diferentes amenazas externas, la herramienta debe desempeñar un papel importante en la detección, validación y priorización de eventos detectados que ayudan a evaluar y analizar el riesgo y el impacto potencial de un incidente.

Contexto de usuario y monitoreo

Herramienta con la capacidad de ordenar y analizar los datos de autenticación enviando mensajes de alerta en tiempo real, identificando de esta manera: las infracciones de políticas por medio de informes y actividades sospechosas, por ejemplo: ataques de fuerza bruta, bloqueos y desbloqueos de cuentas, cuentas promiscuas, falta de uso en cuentas y cambios en privilegios y roles, etc.

7. HERRAMIENTAS DE CONTENCIÓN

Actualizar de manera periódica el sistema operativo y las aplicaciones instaladas en el sistema, de esta manera permitirá controlar y minimizar la eventualidad de un ataque informático.

“ESET Smart Security, es una suite de seguridad informática, previne el control para ingresar a sitios web (sitios seguros o no seguros), crea listas negras y blancas

para las cuentas de Windows"[4]. Analiza los archivos almacenados en la nube y detecta si existe algún tipo de amenaza. Protege al equipo contra acciones de tipo malware que pueden ocasionar daños en los equipos, tiene la capacidad de monitorear redes, archivos y claves de registro, en caso de anomalías bloquear los intentos de abuso no autorizado en el sistema. También, analiza los canales cifrados Https, POP3S. además explora archivos comprimidos en busca de amenazas. Maneja un filtro de correo no deseados spam, se integra con los correos electrónicos más populares como son Windows Mail, Windows Live Mail y Mozilla Thunderbird. Además, maneja control de acceso a dispositivos extraíble estableciendo reglas para lectura, escritura o para un grupo determinado de usuarios.

"FIREWALL, es un sistema que protege a computadores de intrusión de terceros, se encarga de hacer un filtro de los paquetes de la red externa con la red interna. Las reglas establecidas en el firewall son"[5]:

- Autorizar una conexión
- Bloquear una conexión
- Redirección un pedido de conexión sin avisar al emisor
- Permite solamente conexiones autorizadas

Tipos de firewall

Firewall de Software, son aplicaciones gratuitas o pagas son utilizados en hogares y oficinas. Son muy fáciles de instalar, normalmente viene instalados en sistemas operativos no requiere de ningún hardware para ser instalado en el equipo.

Firewall de hardware, viene normalmente instalado en los Routers donde se accede al internet, indicando que todas las computadoras en el interior de la red están protegidas por el firewall.

[4] ESET, Eset Latinoamérica. Protección Avanzada contra amenazas. Colombia: 2020
[5] TÉCNOLOGÍA INFORMACIÓN, Graciela. Firewall. 2020

8. CONCLUSIONES

- Es importante en las organizaciones contratar personal idóneo, capacitado en seguridad de la información, para realizar auditorías, análisis de riesgo y vulnerabilidades en las infraestructuras de red.

- Para The WhiteHose Security su activo más relevante es la información la compañía. Kali Linux es un sistema operativo que nos permite realizar pentesting, al aplicar cada una de las fases en el sistema de información The WhitheHose con las herramientas configuradas en kali Linux como son **nmpa y metasploit** logramos información completa de cada uno de los sistemas operativos, inclusive análisis y explotación de vulnerabilidades.

- Los resultados del pentesting permiten al equipo BlueTeam tomar decisiones para fortalecer la seguridad de la información, contención frente a un incidente informático cumpliendo el modelo de gestión de incidentes, implementar un sistema de gestión de información y eventos de seguridad con las mejores prácticas estandarizadas a nivel mundial como lo es CIS (el centro para la seguridad de internet).

9. RECOMENDACIONES

MEDIDAS DE HERDENIZACIÓN

- Instalar cortafuegos; el corta fuego controla aquellos servicios de red expuestos, restringiendo el acceso a los puertos.

- Activación y actualización de servicios de actualizaciones automáticas, ayuda a que el equipo tenga los parches de seguridad

- Instalación de programas de antivirus, antispyware, anti spam para fortalecer la seguridad del sistema, mitigando el riesgo.

- Configurar el protocolo de red estableciendo un límite de equipos conectados a la red configurando una lista de control de acceso.

- Configurar el acceso remoto. En caso no ser necesario es importante deshabilitar el acceso remoto. Cuando se requiera el acceso remoto aplicar protocolo de cifrado avanzado SSH, restringiendo en la red un numero límite de usuario estableciendo controles de acceso.

LINK SUSTENTACIÓN DE SEMINARIO

https://youtu.be/SlDfox5pUiQ

10. BIBLIOGRAFIAS

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

- Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

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

- Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

.• Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

- Alvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) Recuperado de: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

- Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

- Gaviria, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira.(pp. 18-61). Recuperado de: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

- Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Recuperado de: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

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

- Mintic. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

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

- SOFECOM, Blog "SIEM: Qué es un sistema SIEM". {En línea}. {2015} disponible en: (https://sofecom.com/que-es-un-siem/#:~:text=SIEM%20(informaci%C3%B3n%20de%20seguridad%20y,la%20tecnolog%C3%ADa%20de%20la%20informaci%C3%B3n).

- CIS, Center for Internet Security "CIS: Mejores Prácticas de Ciberseguridad". {En línea}. {15 Octubre 2020} disponible en: (https://www.cisecurity.org/)

- HACKING, Para Novatos "PENTESTING: Fases de una Auditoria". {En línea}. {14 Octubre 2020} disponible en: (https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/)

- ESET, Eset Latinoamérica "Detención: Protección Avanzada contra amenazas". {En línea}. {14 Octubre 2020} disponible en: (https://www.eset.com/co/)

- TECNOLOGÍA INFORMACIÓN, Graciela "Firewall: Que es un Firewall y como funciona". {En línea}. {14 Octubre 2020} disponible en: (https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/)

.