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

ANDRES ANTONIO AMELINES ACOSTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
2023

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

ANDRÉS ANTONIO AMELINES ACOSTA

JOHN FREDDY QUINTERO TAMAYO
Director de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
PEREIRA
2023

ÍNDICE

INTRODUCCIÓN 11
1. OBJETIVOS 12
1.1. Objetivo General 12
1.2. Objetivos Específicos 12
2. DESARROLLO DEL TRABAJO 13
2.1. Marco Legal En Colombia Sobre Delitos Informáticos Y Protección De Datos Personales. 13
2.1.1. Ley 1273 de 2009. 13
2.1.2. Ley 1581 De 2012. 14
2.1.3. Ley 1928 de 2018. 15
2.1.4. CONPES 3854 15
2.2. Etapas Del Pentesting. 16
2.2.1. Reconocimiento (footprinting). 16
2.2.2. Análisis de Vulnerabilidades. 17
2.2.3. Explotación. 18
2.2.4. Post Explotación 18
2.2.5. Informes o reportes. 18
2.3. Herramientas De Ciberseguridad. 19
2.3.1. Metasploit. 19
2.3.2. Nmap. 19
2.3.3. OpenVAS. 20
2.3.4. ExploitDB. 20
2.3.5. CVE 21
2.4. Banco de Trabajo. 21
2.4.1. Paso A 21
2.5. ¿Logra Evidenciar Algún Proceso Ilegal Y No Ético Que Se Esté Estipulando En Dicho Acuerdo? 22
2.5.1. Anexo 2 – Escenario 2 22
2.5.2. Anexo 3 – Acuerdo 23
2.6. Artículos De La Ley 1273 Que Se Podrían Vulnerar. 25

2.7. Aplicaría Usted Al Trabajo Ofertado En «The Whitehouse». 27

2.8. Punto de Vista «Operación Andrómeda Buggly». 27

2.9. Describir Las Herramientas Que Se Utilizaron Para Resolver El Anexo 4 – Escenario 3 enfocado en Red Team. 29

2.9.1. Terminal De Comandos. 29

2.9.2. PING. 30

2.9.3. NMAP (Network Mapper). 30

2.10. Listar Y Describir Los Datos E Información Del Anexo 4 – Escenario 3 Que Le Fueron De Ayuda. 31

2.11. ¿Cómo identificó las vulnerabilidades de la MV Windows 7? ¿Qué puerto habilita el servicio HFS?. 32

2.12. Gráfico Ataque a Windows 7 X64. 32

2.13. Documente Los Pasos Que Ejecutó Para Explotar La MV WinX64. 33

2.14. ¿Qué Sería Lo Primero Que Indagaría Y Haría Si Llegara A Encontrarse Un Ataque En Tiempo Real? 40

2.15. Medidas De Hardenización Para Evitar Ataques Informáticos. 42

2.15.1. Firewall 42

2.15.2. IDS/IPS (Intrusion Detection System / Intrusion Prevention System ... 43

2.15.3. DMZ (Demilitarized Zone) 43

2.15.4. HoneyPot 43

2.15.5. Proxy Inverso 43

2.15.6. EDR (Endpoint Detection and Response) 44

2.15.7. MPLS (Multiprotocol Label Switching) 44

2.15.8. Actualización De Sistemas Operativos 44

2.15.9. Antivirus 44

2.16. ¿Diferencias Entre Un Equipo Blue Team Y Un Equipo De Respuesta A Incidentes Informáticos? 45

2.17. ¿En Qué Utilizar Un CIS “Center For Internet Security”? 45

2.18. ¿Qué es un SIEM? 46

2.19. Tres Herramientas De Contención De Ataques Informáticos. 46

2.20. Aspectos para el Desarrollo de Estrategias de Red/BlueTeam. 49

2.21. Estrategias para Endurecer la Seguridad en una Organización. 49

2.22. Conclusiones para la Construcción de Conocimiento en Ciberseguridad. 50
3. CONCLUSIONES 51
4. RECOMENDACIONES 52
5. ANEXO 53
BIBLIOGRAFÍA 54

LISTA DE FIGURAS

Figura 1. Logo Nmap 17
Figura 2. Logo Nessus 17
Figura 3. Logo Metasploit 19
Figura 4. Logo OpenVAS 20
Figura 5. Logo ExploitDB 20
Figura 6. Archivo ejecutable de instalación VirtualBox. 21
Figura 7. Ventana de la instalación. 22
Figura 8. VirtualBox 22
Figura 9. Terminal de Comandos 30
Figura 10. Logo Nmap 31
Figura 11. Resultado Nmap 32
Figura 12. Gráfico del ataque informático 33
Figura 13. Dirección IP MV Windows7X64 33
Figura 14. Dirección IP MV Kali Linux 34
Figura 15. Ping desde MV Windows a Kali 34
Figura 16. Ping desde MV Kali a Windows 7 X64. 34
Figura 17. Rejetto v.2.3 35
Figura 18. Nmap a 192.168.80.21 35
Figura 19. Nmap script vuln a 192.168.80.21 36
Figura 20. Metasploit 37
Figura 21. Metasploit – Show Options 37
Figura 22. Exploit 38
Figura 23. Información del sistema de la máquina objetivo 38
Figura 24. Shell 38
Figura 25. Creación usuario 39
Figura 26. Asignación de privilegios 39
Figura 27. Verificación desde Shell 39
Figura 28. CMD – Verificación. 39
Figura 29. CMD - netstat 41

Figura 30. Net users. 41
Figura 31. IBM QRADAR. 47
Figura 32. Herramienta Security Event Manager 48
Figura 33. Sumo Logic 49

GLOSARIO

BLUE TEAM: es un equipo compuesto por personas expertas en temas de seguridad informática que tienen como objetivo proteger la infraestructura de la red empresarial y sus activos[1].

CIBER: relacionado con mundo del ciberespacio[2].

CPP: Abreviatura de Código de Procedimiento Penal de Colombia.

CSIRT: por sus siglas en inglés computer security incident response team.

EXPLOIT: es una secuencia de comandos o algoritmo usado para atacar vulnerabilidades o fallas en software, hardware o IoT, ejecuta tareas preconfiguradas por el administrador o atacante, ya sea para sacar provecho u ocasionar daños[3].

IP: es una dirección dada para identificar un dispositivo en Internet o una red privada. Esto con el fin de permitir la comunicación entre dispositivos en una red.[4].

MÁQUINA VIRTUAL: es la simulación de equipos de cómputo físicos a través de software con el mismo rendimiento y configuración, permite la prueba de aplicaciones en espacio aislados y controlados para evitar problemas en la máquina física[5].

---

[1] UNIVERSITY OF FOREIGN MILITARY AND CULTURAL STUDIES. The Red Team Handbook, the army's guide to making better decisions. p.238

[2] JUNTA INTERAMERICANA DE DEFENSA. Guía de ciberdefensa: orientaciones para el diseño, planteamiento, implantación y desarrollo de una ciberdefensa militar. Canadá, 2020. 113 p.

[3] PANDASECURITY. [Sitio web]. ¿Qué es un Exploit? [Consultado: marzo de 2023]. Disponible en: https://www.pandasecurity.com/es/security-info/exploit/

[4] KASPERSKY. [Sitio web]. Qué es una dirección IP: definición y explicación. [Consulta: noviembre de 2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address

[5] VMWARE. [Sitio web]. Definición de «máquina virtual». [Consultado: marzo de 2023]. Disponible en: https://www.vmware.com/latam/topics/glossary/content/virtual-machine.html

NMAP (Network Mapper): es una herramienta de código o fuente abierta, se utiliza para la identificación de redes, la auditoría de seguridad y pentesting[6].

RED TEAM: Equipo de expertos en ciberseguridad que tienen como fin hallar e identificar vulnerabilidades en redes informáticas, que permitan realizar una explotación y post explotación de sus recursos y activos[7].

ISP: Internet Service Provider, por sus siglas en inglés.

PENTESTING: Es la abreviatura de «penetration» y «testing», es una técnica o método que busca identificar fallas en redes o sistemas informáticos con el fin de informar a los propietarios y prevenir futuros incidentes[8].

PING: Packet Internet Groper por sus siglas en inglés. Es una herramienta de tipo TCP/IP. Por medio de datagramas IP enviados a un host de destino pide una respuesta y mide el tiempo de ida y vuelta. Se usa generalmente para probar comunicación entre dispositivos conectados en red[9].

PUERTO DE CONEXIÓN: Son sitios que permiten entradas y salidas virtuales en un sistema operativo, por allí se comienzan y terminan las conexiones de red. Además, ayudan a clasificar el tráfico de red que reciben[10].

VULNERABILIDAD: es una falla o debilidad en un sistema, para nuestro caso informático, y pueden existir en software, hardware o factor humano[11].

---

[6] NMAP. [Sitio Web]. Nmap: Descubre tu red. [Consultado: febrero de 2023]. Disponible en: https://nmap.org/

[7] KEEPCODING. [Sitio web]. ¿Qué es Red Team en Ciberseguridad?. [Consulta: noviembre de 2022]. Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

[8] CAMPUSCIBERSEGURIDAD. [Sitio web]. ¿Qué es el Pentesting? [Consultado: marzo de 2023]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

[9] PERSONALES.UPV.ES [Sitio web]. Ping. [Consultado: Marzo de 2023]. Disponible en: http://personales.upv.es/rmartin/TcpIp/cap02s05.html#:~:text=Ping%20es%20la%20aplicaci%C3%B3n%20m%C3%A1s,tiempo%20de%20ida%20y%20vuelta

[10] CLOUDFLARE. [Sitio web]. ¿Qué es un puerto de ordenador?. [Consultado: marzo de 2023]. Disponible en: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-computer-port/#:~:text=Los%20puertos%20son%20lugares%20virtuales,tr%C3%A1fico%20de%20red%20que%20reciben.

[11] BANCO SANTANDER. [Sitio web]. ¿Qué es una vulnerabilidad informática? [Consultado: marzo de 2023]. Disponible en: https://www.bancosantander.es/glosario/vulnerabilidad-

RESUMEN

A través del presente documento, se abordará el Marco Legal vigente en el territorio Colombiano respecto a los delitos informáticos y la protección de datos personales, para lo cual se mencionarán leyes como la 1273 de 2009, la 1581 de 2012 y la 1928 de 2018, además de los documentos CONPES 3701 y 3854.

Por otra parte, se mencionarán las etapas que componen un Pentesting, relacionando algunas herramientas de ciberseguridad utilizadas por expertos en informática para llevar a cabo dichas pruebas, para esto, se montará un banco de prueba basado en máquinas virtuales (MV), evitando así daño en equipos físicos.

Teniendo en cuenta el acuerdo presentado por la empresa «Whitehouse Security», se analizará y evidenciará si transgrede o no las leyes vigentes en Colombia y el código de ética de COPNIA.

De igual forma, se dirá qué se puede hacer en caso de encontrarse con un ataque informático en tiempo real, algunas buenas prácticas de endurecimiento o «hardenización» de medidas de seguridad informáticas en dispositivos empresariales.

Se termina con las diferencias entre Blue Team y Red Team y el desarrollo de estrategias para dichos equipos.

informatica#:~:text=Las%20vulnerabilidades%2C%20tanto%20las%20relativas,atacantes%20para%20burlar%20su%20seguridad.

INTRODUCCIÓN

Los delitos informáticos han venido en ascenso, más aún desde la pandemia del COVID 19, esto ha convertido en blanco los ordenadores de escritorio, portátiles, dispositivos IoT y cualquier otro conectado a una red de hogar o empresa, de ahí la importancia de conocer las herramientas jurídicas que nos brinda la legislación vigente en Colombia con relación a este tipo de variable.

De igual forma, se hace necesario conocer las etapas o fases que componen una prueba de penetración o Pentesting y las herramientas usadas por expertos en informática o miembros del Red Team para tal fin. Debido al riesgo que implican estas prácticas, se montará un banco de prueba con máquinas virtuales que permitan realizar el Pentesting en un espacio aislado.

Desde la perspectiva del Blue Team, se presentarán los pasos a realizar (enfocado en la práctica realizada) ante un ataque informático en tiempo real, algunas recomendaciones de endurecimiento de medidas de seguridad informática o «hardenización».

Con base en lo anterior, se logra demostrar la importancia de aplicar o implementar correctamente las políticas de seguridad informática en una empresa y la relevancia de contar con equipos de expertos informáticos que puedan identificar y corregir vulnerabilidades en la red y los dispositivos que la componen, tal como los Blue Team y los Red Team.

1. OBJETIVOS

1.1. Objetivo General

Describir con palabras propias las principales características de las leyes emanadas en Colombia relacionada con los delitos informáticos y protección de datos personales, así como las etapas que componen una prueba de penetración o pentesting y herramientas y servicios en línea para tal fin. De igual manera, se realizará la instalación o montaje del «banco de trabajo» para realizar el Pentesting, y proceder a la explotación de la MV Windows 7 X64.

1.2. Objetivos Específicos

- Describir las principales características de las leyes emanadas en Colombia relacionada con los delitos informáticos y protección de datos personales.
- Describir las etapas de un pentesting y las herramientas o servicios en línea: Metasploit, Nmap, Openvas, ExploitDB y CVE, realizando el montaje del «banco de trabajo».
- Argumentar la respuesta dada respecto al hallazgo o no de procesos ilegales o no éticos plasmado en el Acuerdo de la empresa Whitehouse Security, mencionando los artículos de la ley 1273 de 2009 transgredidos. Como ejemplo se analizará el caso denominado «operación Andrómeda Guggly» y plasmar el punto de vista desde lo legal y ético.
- Describir la herramienta usada para hallar los fallos en la MV Windows 7 X64, explicando cómo afecta a la MV Windows 7 X64 el ataque informático realizado.
- Documentar los pasos realizados para el Pentesting, explicando el procedimiento realizado en caso de presentar un ataque informático en tiempo real, proponiendo medidas de Hardenización para evitar futuros incidentes.
- Describir la diferencia entre Blue Team y un equipo de respuesta a incidentes informáticos.

2. DESARROLLO DEL TRABAJO

2.1. Marco Legal En Colombia Sobre Delitos Informáticos Y Protección De Datos Personales.

2.1.1. Ley 1273 de 2009.

El Congreso de la República de Colombia, emanó el 05 de enero de 2009 la ley 1273 *«por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*»[12], esto con el fin de tipificar las conductas delictivas que tienen como escenario el campo virtual, el espectro, y nuevas tecnologías.

La Ley 1273 de 2009, está compuesta por dos capítulos. El primero denominado «*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*»[13], éste cuenta con ocho artículos:

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

Por su parte, el capítulo 2 «*De las atentados informáticos y otras infracciones*»[14] contiene:

- Artículo 2691. hurto por medios informáticos y semejantes.

[12] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). De la protección de la información y de los datos. En diario oficial. Enero, 2009. 4 p.
[13] Ibid,.
[14] Ibid,.

- Artículo 269J: transferencia no consentida de activos.

Como se puede apreciar, la Ley 1273 de 2009, busca brindar las herramientas jurídicas básicas para que las autoridades judiciales del país puedan combatir las nuevas modalidades de delincuencia; ya que estas tendencias están orientadas al mundo virtual.

2.1.2. Ley 1581 De 2012.

El Congreso de la República de Colombia emanó el 17 de octubre de 2012 la Ley Estatutaria 1581 con la cual «…*se dictan disposiciones generales para la protección de datos Personales*…»[15], como su nombre lo dice busca proteger los datos que las personas han suministrado a diversas entidades para ser almacenadas en archivos o bases de datos; esto, por medio de sus veintinueve artículos y tres capítulos.

Asimismo, contiene una serie de definiciones propias a los datos personales, reserva, procedimientos, medios de almacenamiento y autorizaciones de uso, para determinar y reglamentar el suministro y administración de los mismos.

Se hizo necesario reglamentar parte del contenido de la Ley Estatutaria 1581 de 2012 por medio del decreto 1377 de 2013, el cual a través de seis capítulos y veintiocho artículos, establece lo relacionado con el tratamiento de los datos personales y todo lo mencionado anteriormente.

Siendo más preciso el decreto busca:

> facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada

[15] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley estatutaria 1581 (18, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En diario oficial. Octubre, 2012.

> frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas[16].

2.1.3. Ley 1928 de 2018.

El Congreso de Colombia emanó la Ley 1928 de 2018, por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest[17].

El convenio contra la ciberdelincuencia firmado por varios países en el consejo de Europa, en busca de brindar herramientas para combatir los delitos informáticos, tales como: pornografía infantil, ataques a redes informáticas, derechos de autor, fraude, entre otros.

Así las cosas y con el ánimo de mejorar las capacidades de la Nación, con la adhesión al convenio se busca coordinar y cooperar entre los Estados (65 países suscritos), para prevenir, detectar, investigar y judicializar a todos aquellos que busquen trasgredir la seguridad y leyes en el ámbito del ciberespacio, incluyendo por supuesto toda la Infraestructura Crítica.

2.1.4. CONPES 3854

Existen varios documentos CONPES relacionados con temas de tecnología, el 3854 del 11 de abril de 2016 trata específicamente sobre la «Política Nacional de Seguridad Digital», estableciendo los pasos para gestionar ciberseguridad y ciberdefensa en entidades públicas, infraestructura crítica y empresa privada.

El documento CONPES reza en su objetivo general:

> Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que

[16] COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1377 de 2013 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. En diario oficial. Junio, 2013.

[17] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1928 (24, julio, 2018). Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en budapest. En diario oficial. Octubre, 2012.

a su vez impulsará una mayor prosperidad económica y social en el país[18].

Como se puede apreciar, al buscar tratar y mitigar los riesgos de seguridad digital en el territorio nacional, se cierra la brecha a los ciberdelincuentes, combatiendo por ende los delitos informáticos. Cabe anotar que, los documentos CONPES 3701 «Lineamientos De Política Para Ciberseguridad Y Ciberdefensa» y 3995 «Política Nacional De Confianza Y Seguridad Digital» refuerzan el antes mencionado.

2.2. Etapas Del Pentesting.

Los Red Teams, llevan a cabo las siguientes fases para identificar las vulnerabilidades existentes en una red determinada o cliente y dependiendo del tipo de contrato, explotarlas permitiendo tomar control de equipos, dispositivos o software conectado a la red, extraer documentos como evidencia o crearlo en un equipo específico. Se tomará como referencia el libro Hacker's White book – cómo convertirte en un hacker profesional, de Pablo Gutiérrez[19].

2.2.1. Reconocimiento (footprinting).

Por medio de esta etapa de la prueba de penetración se busca recolectar el mayor número de datos posible que permitan ampliar el rango de posibilidades al momento de la explotación, por ejemplo: dirección IP, puertos y servicios abiertos y filtrados, versión de sistemas operativos, entre otros. No está de más usar herramientas OSINT para recolectar datos privados de los miembros de la junta directiva y colaboradores en general de la empresa que posibiliten usar técnicas de Ingeniería Social.

Para dicha recolección se pueden varias herramientas opensource o de licencia comercial, como por ejemplo:

[18] COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3854 (abril 11 de 2016). Política nacional de seguridad digital. Departamento Nacional de Planeación. Abril, 2016. p. 1-91.

[19] GUTIERREZ, Pablo. Hacker's White book – cómo convertirte en un hacker profesional. Monterrey, Nuevo León: whitesuit hacking, 2019. p.563.

NMAP (Network Mapper): como su nombre lo dice, su principal característica es mapear redes, dependiendo la instrucción o comando introducido se obtendrán resultados generales y específicos. Es de fuente abierta y gratuita[20].

Figura 1. Logo Nmap

Fuente: nmap.org

NESSUS: esta herramienta de licencia comercial tiene dos versiones: Professional y Expert, ambas permiten realizar pruebas de intrusión a redes informáticas, ofreciendo un informe de los hallazgos y posibles soluciones a las vulnerabilidades. Por su parte, la versión Expert, posibilita escanear dominios y servicios en la «nube»[21].

Figura 2. Logo Nessus

Fuente: https://www.tenable.com/

2.2.2. Análisis de Vulnerabilidades.

Ahora, se analizarán los datos recolectados en la fase anterior, cuáles son los servicios abiertos, sistema operativo del objetivo y su versión, sistemas de seguridad lógica o física, en el caso de los firewalls, IDS/IPS, entre otros; esto con el fin de, realizar consultas en bases de datos de acceso público como CVE (Common Vulnerabilities and Exposures) o Exploit-DB y conocer la forma de explotar las

[20] NMAP. [Sitio Web]. Nmap: Descubre tu red. [Consultado: febrero de 2023]. Disponible en: https://nmap.org/

[21] TENABLE. [Sitio web]. Cierre su brecha de exposición cibernética con Nessus. [Consultado: febrero de 2023]. Disponible en: https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial/?utm_campaign=gs-{11596512476}-{116641138521}-{537515898224}_00026643_fy23&utm_promoter=tenable-hv-brand-00026643&utm_source=google&utm_term=nessus&utm_medium=cpc&utm_geo=latam&gclid=EAIaIQobChMIht2m88WD_QIV0vbjBx1ZngX_EAAYASAAEgK_S_D_BwE

vulnerabilidades halladas, claro está, si éstas no han sido corregidas por medio de parches de seguridad.

2.2.3. Explotación.

Los datos recolectados y analizados en las fases anteriores serán puestos a prueba; cabe aclarar que, existen varias formas de iniciar el pentesting, caja blanca (conocimiento completo de la infraestructura a analizar), gris (conocimiento parcial) o negra (sin datos previos), esta última se asemeja más a la realidad de un ataque informático externo.

Hay varias técnicas de ataque informático: Ingeniería Social, Inyección de Sql, Fuerza Bruta, DoS, Infección con Malware, entre otros, el pentester deberá seleccionar las técnicas a ejecutar de acuerdo al análisis realizado.

Al momento de ejecutar las técnicas de ataque informático sobre las vulnerabilidades halladas en la red informática y obtener resultados positivos, se dejará un backdoor o infectados algunos dispositivos, todo depende del requerimiento de pentesting.

2.2.4. Post Explotación

Tras lograr el acceso a la red por medio de la explotación de vulnerabilidades halladas en la misma, se dará cumplimiento a lo requerido en el contrato de pentesting, el analista podrá extraer archivos, infectar equipos o dispositivos IoT con malware, sabotear configuraciones de sistemas operativos, o de seguridad lógica perimetral y de aplicación.

Como ya se mencionó, todo dependerá del acceso obtenido (privilegios, equipos, servidores, entre otros) y de lo requerido en el contrato, por ejemplo: extraer algún archivo específico o crearlo, manipular un equipo clave en la red, hay una variedad de posibilidades en esta fase.

2.2.5. Informes o reportes.

Como su nombre lo dice, el equipo de pentesting elaborará un informe ejecutivo, indicando las pruebas realizadas, las vulnerabilidades

halladas, evidencia de la intrusión a la red y sus equipos/dispositivos y terminando con las posibles soluciones de las vulnerabilidades.

2.3. Herramientas De Ciberseguridad.

2.3.1. Metasploit.

Es un marco usado para pruebas de pentesting y demás interesados, es de código abierto y cuenta con una base de datos para consultar vulnerabilidades halladas en diversos sistemas que permitirán validar la seguridad informática o lógica en éstos[22].

Rapid7, también ha desarrollado una versión comercial de Metasploit denominada Pro, por supuesto, cuenta con algunas herramientas adicionales para los usuarios.

Figura 3. Logo Metasploit

Fuente: metasploit.com

2.3.2. Nmap.

Como se mencionó anteriormente, NMAP es una aplicación opensource utilizada por el público en general, para llevar acabo auditorías de seguridad informática en redes, servidores y demás dispositivos conectados a internet (público o privado)[23].

Cabe anotar que, la versión Nmap para sistemas operativos Windows se llama Zenmap, cuenta con una interfaz gráfica que facilita al usuario realizar escaneos de acuerdo a su necesidad.

[22] CIBERSEGURIDAD.COM. [Sitio web]. ¿Qué es Metasploit framework y cómo funciona?. [Consultado: febrero de 2023]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

[23] NMAP. [Sitio Web]. Nmap: Descubre tu red. [Consultado: febrero de 2023]. Disponible en: https://nmap.org/

2.3.3. OpenVAS.

Es un escáner de vulnerabilidades con licencia GNU – GPL, está disponibles para algunas distribuciones de Linux como Kali, Fedora, Parrot, Ubuntu, éste, es administrado a través de una interfaz web, donde se darán las instrucciones y se mostrarán los resultados[24].

Figura 4. Logo OpenVAS

Fuente: kolibers.com

2.3.4. ExploitDB.

Es un sitio web desarrollado por Offensive Security, mismo creador del sistema operativo Kali Linux, tiene una de las bases de datos más grande y de acceso público en el mercado. Allí se pueden encontrar exploits para explotar vulnerabilidades halladas en redes o equipos de cómputo.

Figura 5. Logo ExploitDB

Fuente: https://www.exploit-db.com/

[24] OPENWEBINARS. [Sitio web]. Qué es OpenVAS. [Consultado: febrero de 2023]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

2.3.5. CVE

Supervisado por MITRE Corporation y financiado por la Agencia de Ciberseguridad y Seguridad de la Infraestructura del Departamento de Seguridad Nacional de Estados Unidos[25].

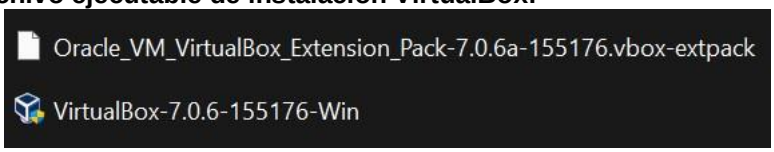
Los CVE tienen un código para individualizarlos en la base de datos, allí se encuentra una definición breve de la vulnerabilidad, como complemento se pueden consultar los sitios web: https://nvd.nist.gov/ y https://www.kb.cert.org/vuls/, para conocer detalles técnicos y riesgos de los CVE.

2.4. Banco de Trabajo.

2.4.1. Paso A

Siguiendo las instrucciones de la guía de la presente etapa del seminario, se procede a descargar la versión más reciente de la aplicación «VirtualBox» desde el sitio web del desarrollador. Cabe anotar que, se descarga con el «Extension Pack».

Figura 6. Archivo ejecutable de instalación VirtualBox.



Fuente: creación propia

Ahora, se ejecutable el archivo descargado y se inicia la instalación de VirtualBox.

[25] REDHAT. [Sitio web]. El concepto de CVE. [Consultado: febrero de 2023]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

Figura 7. Ventana de la instalación.

Fuente: creación propia

Al terminar la instalación, se ejecuta la aplicación en su versión 7.0.6.

Figura 8. VirtualBox

Fuente: creación propia

2.5. ¿Logra Evidenciar Algún Proceso Ilegal Y No Ético Que Se Esté Estipulando En Dicho Acuerdo?

2.5.1. Anexo 2 – Escenario 2

Al revisar el contenido del «Anexo 2», se extraen los siguientes fragmentos por ser considerados ilegales o no éticos:

«*…contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos*…»

El contrato fue elaborado por un profesional que al parecer obró de forma no ética y en contravía a la ley 906 de 2004, artículo 67; ya que

no denunció ante autoridad competente los hechos ilícitos hallados en la empresa WhiteHouse Security durante su permanencia allí.

«..*La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna*…»

El Gobierno Corporativo no está al tanto del contenido de los contratos por prestación de servicios del nuevo personal de profesionales que ingresará a WhiteHouse Security, siendo una conducta poco ética e irresponsable, al ser ellos los representantes legales de la empresa en mención, recayendo en ellos parte de la responsabilidad civil, laboral y penal, de los procesos y productos originados al interior de la empresa.

2.5.2. Anexo 3 – Acuerdo

Respecto al contenido del «Anexo 3», se extraen los siguientes hallazgos:

> Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

Como se manifestó anteriormente, la legislación Colombiana en su Ley 906 de 2004, artículo 67 habla sobre el «Deber De Denunciar: Toda persona debe denunciar a la autoridad los delitos de cuya comisión tenga conocimiento y que deban investigarse de oficio[26]», así las cosas se estaría incurriendo por parte de la empresa WhiteHouse Security en una conducta ilícita, al obligar por medio de contrato de prestación de servicios a no denunciar, lo cual podría tomarse como una violación al artículo 184 (Constreñimiento para delinquir) del Código Penal.

> Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

[26] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 906 (31, agosto, 2004). Por la cual se expide el Código de Procedimiento Penal. En diario oficial. Agosto, 2009

> Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

En la parte del texto subrayada se aprecia claramente, una violación tácita a los artículos 269A (Acceso abusivo a un sistema informático) y 269C (Interceptación de datos informáticos) de la ley 1273 de 2009[27].

> Cuarta. Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:
>
> 3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
>
> 4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
>
> 7. Responder por el mal uso que le den sus representantes a la información confidencial.
>
> 8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

De igual forma, en los anteriores apartes, se pueden observar las palabras «no denunciar», «abstenerse de denunciar», siendo esta una acción tipificada en el artículo 67 de la ley 906 de 2004. Además, al hablar de espionaje, se puede incurrir en acto delictivo; ya que el artículo 15 de la Constitución Política de Colombia[28] protege la intimidad de las personas.

> Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.

Ahora, se evidencia una conducta no ética por parte de la empresa WhiteHouse Security al descargar toda la responsabilidad civil y penal

[27] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En diario oficial. Enero, 2009.

[28] COLOMBIA. Constitución Política de Colombia (20, julio, 1991). En diario oficial. Julio, 1991.

producto de la actividad ilegal que se adelanta en algunos procesos de la misma.

2.6. Artículos De La Ley 1273 Que Se Podrían Vulnerar.

La Ley 1273 de 2009 «*por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*»[29] busca complementar los vacíos jurídicos existente en la ley para la época, cabe resaltar que, no ha sido actualizada a la fecha, siendo algo obsoleta frente a los nuevos desafíos que presenta el cibercrimen.

Ahora bien, enfocado en el «anexo 3» se hacen los siguientes hallazgos:

«… *sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados*…»

Es evidente que la empresa contratante es conocedora de los procesos irregulares o ilegales que se adelantan en algunos de sus procesos, más adelante, en el mismo documento se plasma:

Respecto a la definición de información confidencial. «*…datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos…»*

Así las cosas, se estaría frente a la comisión de una conducta tipificada en la ley 906 de 2004, específicamente en los siguientes artículos:

> Artículo 269A. Acceso Abusivo A Un Sistema Informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, 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.[30]
>
> Artículo 269C. Interceptación De Datos Informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas

[29] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En diario oficial. Enero, 2009

[30] Ibid,.

provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.[31]

Artículo 269F. Violación De Datos Personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases 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.[32]

Artículo 269H. Circunstancias De Agravación Punitiva: Las penas imponible de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para si o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.[33]

En este último artículo, se subrayan los apartes que tienen relevancia jurídica frente al caso de análisis.

[31] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En diario oficial. Enero, 2009.

[32] Ibid,.

[33] Ibid,.

2.7. Aplicaría Usted Al Trabajo Ofertado En «The Whitehouse».

Basado en el contenido de los «Anexos», no estaría interesado en ocupar o aplicar a dicha vacante laboral, por motivos éticos, morales y legales, pese a la buena remuneración económica del cargo, el riesgo de ser inhabilitado profesionalmente y enfrentar cargos penales por adelantar actividades ilícitas en los procesos adelantados por la empresa «WhiteHouse Security» me hace anteponer mi buen nombre, mi familia, mi libertad, tranquilidad y por supuesto mi ética profesional como Ingeniero.

El Código de Ética del Consejo Profesional Nacional De Ingeniería (COPNIA), entre otros artículos pone de presente una serie de lineamientos que se deben seguir como profesional en el área de la Ingeniería, para argumentar mi posición relaciono:

> Artículo 31. Deberes Generales De Los Profesionales.
>
> f. Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.
>
> Artículo 35. Deberes De Los Profesionales Para Con La Dignidad De Sus Profesiones. Son deberes de los profesionales de quienes trata este Código para con la dignidad de sus profesiones.
>
> b. Respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.
>
> Artículo 53. Faltas Gravísimas
>
> e. Incurrir en algún delito que atente contra sus clientes, colegas o autoridades de la República, siempre y cuando la conducta punible comprenda el ejercicio de la ingeniería o de alguna de sus profesiones auxiliares.[34]

2.8. Punto de Vista «Operación Andrómeda Buggly».

Desde mi punto de vista, es una actividad no ética, dada la violación a la intimidad de las personas, la clara violación a los artículos: Artículo 269A. Acceso Abusivo A Un Sistema Informático, Artículo 269C. Interceptación De Datos Informáticos, Artículo 269F. Violación De Datos Personales de

[34] COLOMBIA. CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Ley 842 de 2003 (9, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. En diario oficial. Octubre, 2003.

la ley 1273 de 2009 y el artículo 15 de la Constitución Política de Colombia; sin embargo, al consultar la Ley 1621 de 2013, se aprecia:

> **Artículo 17. *Monitoreo del Espectro Electromagnético e Interceptaciones de Comunicaciones Privadas*.** Las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético debidamente incorporadas dentro de órdenes de operaciones o misiones de trabajo. La información recolectada en el marco del monitoreo del espectro electromagnético en ejercicio de las actividades de inteligencia y contrainteligencia, que no sirva para el cumplimiento de los fines establecidos en la presente Ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. El monitoreo no constituye interceptación de comunicaciones. La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales[35].

En mi opinión, la legislación colombiana permite este tipo de actividades que de una forma u otra viola el artículo 15 de la Constitución Política de Colombia; además, en la misma ley se observa:

> **Artículo 39*. Excepción a los deberes de denuncia y declaración*.** Los servidores públicos de los organismos que desarrollan actividades de inteligencia y contrainteligencia están obligados a guardar la reserva en todo aquello que por razón del ejercicio de sus actividades hayan visto, oído o comprendido. En este sentido, los servidores públicos a los que se refiere este artículo están exonerados del deber de denuncia y no podrán ser obligados a declarar. Lo anterior sin perjuicio de lo establecido en los parágrafos 3° y 4° del artículo 18 y del parágrafo 3° del artículo 33.[36]

Ósea, los funcionarios que adelanten operaciones de inteligencia no están obligados a denunciar, ni declarar en procesos judiciales, por este motivo es que se realizan este tipo de actividades que a la luz pública vulneran una serie de derechos fundamentales y civiles.

Respecto al ámbito ético, considero que tácitamente no se quebranta lo allí plasmado, ya que según la Ley 1621 de 2013, estas actividades

[35]COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1621 (14, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". En diario oficial. Abril, 2013.
[36]Ibid,.

irregulares están amparadas por la misma; ya se entraría a debatir temas de moral y profesionalismo que no son para este espacio.

En pocas palabras, la diferencia entre la empresa Whitehouse Security y la operación Andrómeda, es que esta última es adelantó bajo el amparo de la Ley 1621 de 2013, haciendo de dichas actividades algo licito, de hecho a la fecha no hay una sentencia en firme que condene dichas actividades.

Por otra parte, la empresa privada al parecer lleva a cabo actividades similares pero al margen de la ley vigente en territorio Colombiano, motivo por el cual, es ilegal y no ético.

2.9. Describir Las Herramientas Que Se Utilizaron Para Resolver El Anexo 4 – Escenario 3 enfocado en Red Team.

Con el fin de conocer la situación presentada por la empresa WhiteHouse Security respecto a la fuga de información presentada en una de sus máquinas, se utilizó una MV con sistema operativo Kali Linux y desde allí se ejecutaron las siguientes aplicaciones:

2.9.1. Terminal De Comandos.

La Terminal de comandos, conocida también como «Prompt», «Shell», entre otros, es utilizada para leer y ejecutar sentencias por medio de línea de comandos[37], para el caso específico se usó desde el Sistema Operativo Kali Linux.

[37] SOFTZONE.ES [Sitio web]. Domina la Terminal de Linux como un profesional. [Consultado: Marzo de 2023]. Disponible en: https://www.softzone.es/linux/tutoriales/terminal-linux/

Figura 9. Terminal de Comandos

Fuente: *https://ethicalhackneox.wordpress.com/2015/11/03/introduccion-linux-kali-comandos-basicos-terminal-directorios/*

2.9.2. PING.

Para comprobar la existencia o no de comunicación entre las MV Kali Linux y Windows 7 X64, se utilizó «Ping» desde la terminal de comandos, para tener más claro el concepto, se trae la definición para en el sitio web «PERSONALES.UPV.ES».

> Ping es la aplicación más simple de todas las de TCP/IP. Envía uno o más datagramas IP a un host de destino especificado pidiendo una respuesta y midiendo el tiempo de ida y vuelta. La palabra ping, que se usa como nombre y como verbo, se tomó de la operación de sondeo de profundidad para localizar un objeto bajo el agua. También es una abreviatura de Packet InterNet Groper[38].

2.9.3. NMAP (Network Mapper).

Quizá la herramienta más importante en la etapa de reconocimiento y recopilación de datos en una prueba de Pentesting, es Nmap; ya que nos ofrece principalmente los puertos y servicios abiertos en el objetivo, también informa la versión y estado de los mismos. Un dato adicional que se puede encontrar en un escaneo es el filtrado de puertos.

[38] PERSONALES.UPV.ES [Sitio web]. Ping. [Consultado: Marzo de 2023]. Disponible en: http://personales.upv.es/rmartin/TcpIp/cap02s05.html#:~:text=Ping%20es%20la%20aplicaci%C3%B3n%20m%C3%A1s,tiempo%20de%20ida%20y%20vuelta

Nmap, es una herramienta de código abierto que explora redes recopilando una serie de datos útiles para auditorías de seguridad[39].

Figura 10. Logo Nmap

Fuente: https://nmap.org/images/

2.10. Listar Y Describir Los Datos E Información Del Anexo 4 – Escenario 3 Que Le Fueron De Ayuda.

Tras analizar el archivo «Anexo 4 - Escenario 3.pdf» se toman los siguientes datos como base para efectuar el Pentesting:

- Windows 7 x64: El sistema operativo, versión y arquitectura es importante a la hora de realizar un Pentesting.

- Rejetto v2.3: Al investigar sobre esta aplicación, se conoció que permite enviar y recibir archivos; ya que se trata de servicios HFS (http file server), éste, facilita la conexión entre equipos de manera directa y remota, y permite ser administrada por medio del navegador web (local host).[40]

- Shell Reversa: Este es un dato que complementa al Rejetto y Meterpreter; ya que, el shell permite establecer conexiones de forma remota por medio de terminal de línea de comandos.

- Meterpreter: Cuando se habla de Meterpreter, se hace referencia a un «payload», ósea, se puede decir que es un canal que permite ejecutar tareas (por lo general maliciosas) de forma remota en otra máquina[41].

[39] NMAP.ORG. [Sitio web]. Guía de referencia de Nmap (Página de manual). [Consultado: marzo de 2023]. Disponible en: https://nmap.org/man/es/index.html.

[40] WIKI. [Sitio web]. HFS: Introducción. [Consultado: marzo de 2023]. Disponible en: https://www.rejetto.com/wiki/index.php?title=HFS:_Introducci%C3%B3n

[41] KEEPCODING. [Sitio web]. ¿Qué es Meterpreter? [Consulta: marzo de 2023]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/#:~:text=Meterpreter%20es%20un%20payload%20que,es%20bastante%20dif%C3%ADcil%20de%20detectar

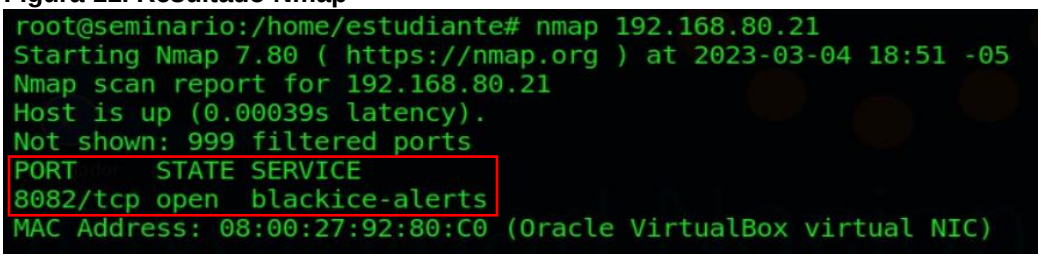
- Creación De Usuario Y Escalamiento De Privilegios: Este es otro dato de importancia, especialmente a la hora de explotar una vulnerabilidad hallada que se relacione con esta acción. Solo es atar cabos y llevar a cabo la creación del usuario y asignación de privilegios a través de línea de comandos en una Shell Reversa.

2.11. ¿Cómo identificó las vulnerabilidades de la MV Windows 7? ¿Qué puerto habilita el servicio HFS?.

Como se manifestó anteriormente, para la exploración y recopilación de datos, se usó la herramienta Nmap instalada en el sistema operativo de la MV Kali Linux.

Inicialmente se realiza un escaneo estándar a la MV Windows 7 X64, la cual tiene asignada la dirección IP 192.168.80.21, hallando:

Figura 11. Resultado Nmap



Fuente: creación propia.

Como se puede observar, el reporte indica que la MV Windows 7 X64 tiene 999 puertos filtrados y uno abierto. El puerto abierto hace referencia al 8082 asignado al HFS Rejetto v2.3.

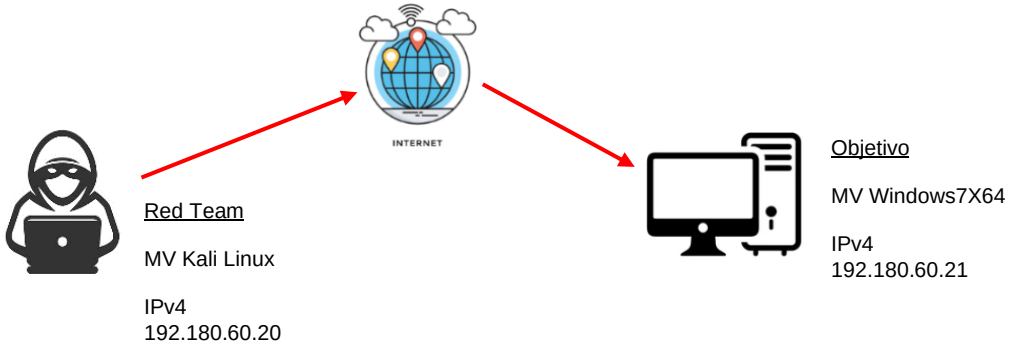
2.12. Gráfico Ataque a Windows 7 X64.

Con la explotación de la vulnerabilidad CVE 2014-6287 (*The findMacroMarker function in parserLib.pas in Rejetto HTTP File Server (aks HFS or HttpFileServer) 2.3x before 2.3c allows remote attackers to execute arbitrary programs via a %00 sequence in a search action*[42]), se logra afectar toda la máquina; ya que, de manera remota se pueden crear usuarios y elevar privilegios, lo que daría acceso ilimitado a terceros al

[42] CVE [Sitio web]. CVE-2014-6287. [Consultado: marzo de 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

sistema, una vez adentro se pueden extraer, suprimir, crear archivos o cambiar configuraciones.

Figura 12. Gráfico del ataque informático



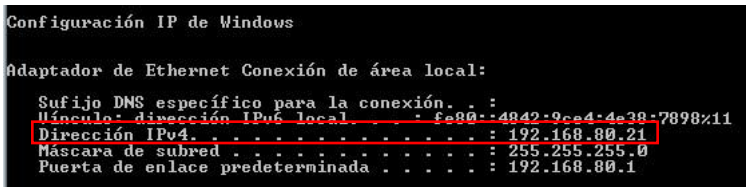
Fuente: creación propia.

2.13. Documente Los Pasos Que Ejecutó Para Explotar La MV WinX64.

A continuación, se documentará el paso a paso del Pentesting realizado a la MV Windows 7 X64 desde la MV Kali Linux.

Inicialmente, se busca conocer con las direcciones IP de las MV que interactúan en el proceso; así las cosas, conoce:

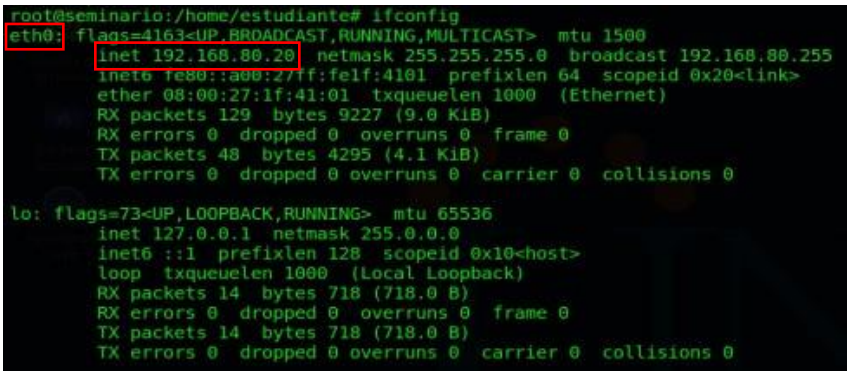
Figura 13. Dirección IP MV Windows7X64



Fuente: creación propia.

Como se puede apreciar, la dirección IPv4 de la MV de Windows 7 X64 es 192.168.80.21.

Figura 14. Dirección IP MV Kali Linux

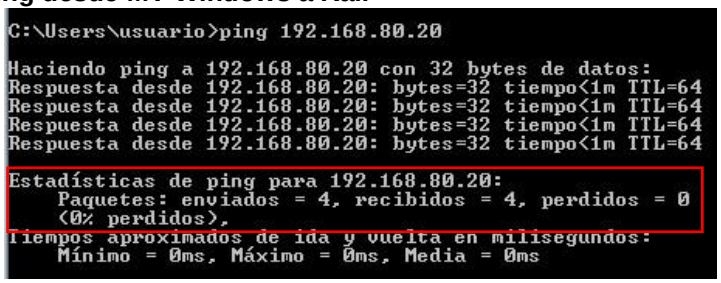


Fuente: creación propia

En la Figura 14 se puede observar la dirección IPv4 de la MV Kali Linux 192.168.80.20.

Ahora, tras conocer las direcciones IP de las máquinas se debe verificar la correcta comunicación entre las mismas, por medio de la sentencia PING.

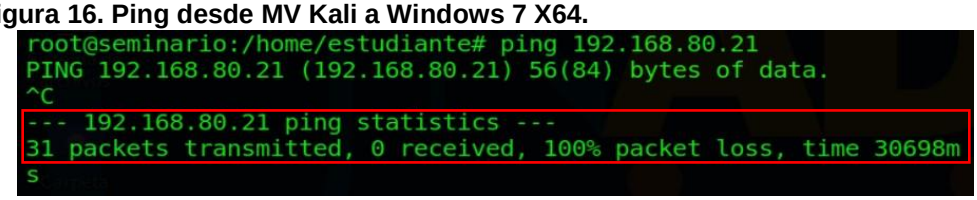
Figura 15. Ping desde MV Windows a Kali



Fuente: creación propia.

Como se ve en la Figura 15, se logra obtener comunicación con la MV Kali Linux (192.168.80.20) desde el CMD de la MV Windows 7 X64.

Figura 16. Ping desde MV Kali a Windows 7 X64.

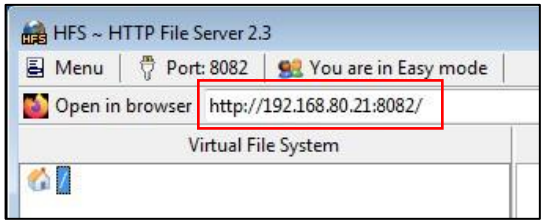


Fuente: creación propia

Se logra evidenciar en la Figura 16, que no se obtiene respuesta al Ping enviado a la MV Windows 7 X64 (192.168.80.21) desde MV Kali Linux, puede ser por bloqueos de Firewall.

Se procede a instalar la aplicación Rejetto v.2.3 en la MV Windows 7 X64, asignando el puerto 8082 para el servicio HFS con otros equipos.

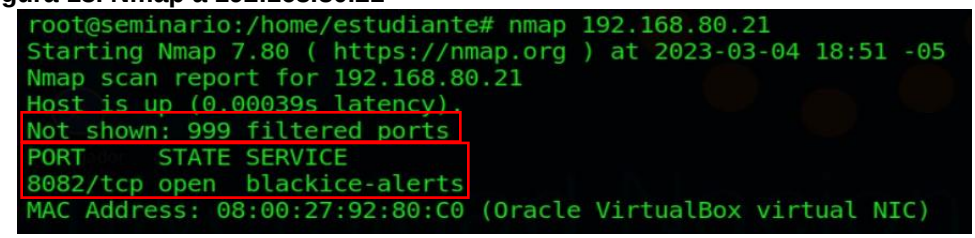
Figura 17. Rejetto v.2.3



Fuente: creación propia

En la MV Kali Linux se abre el Terminal de línea de comandos, allí y con privilegios de Root, se ejecuta Nmap para escanear la dirección IPv4 192.168.80.21 (Windows 7 X64).

Figura 18. Nmap a 192.168.80.21

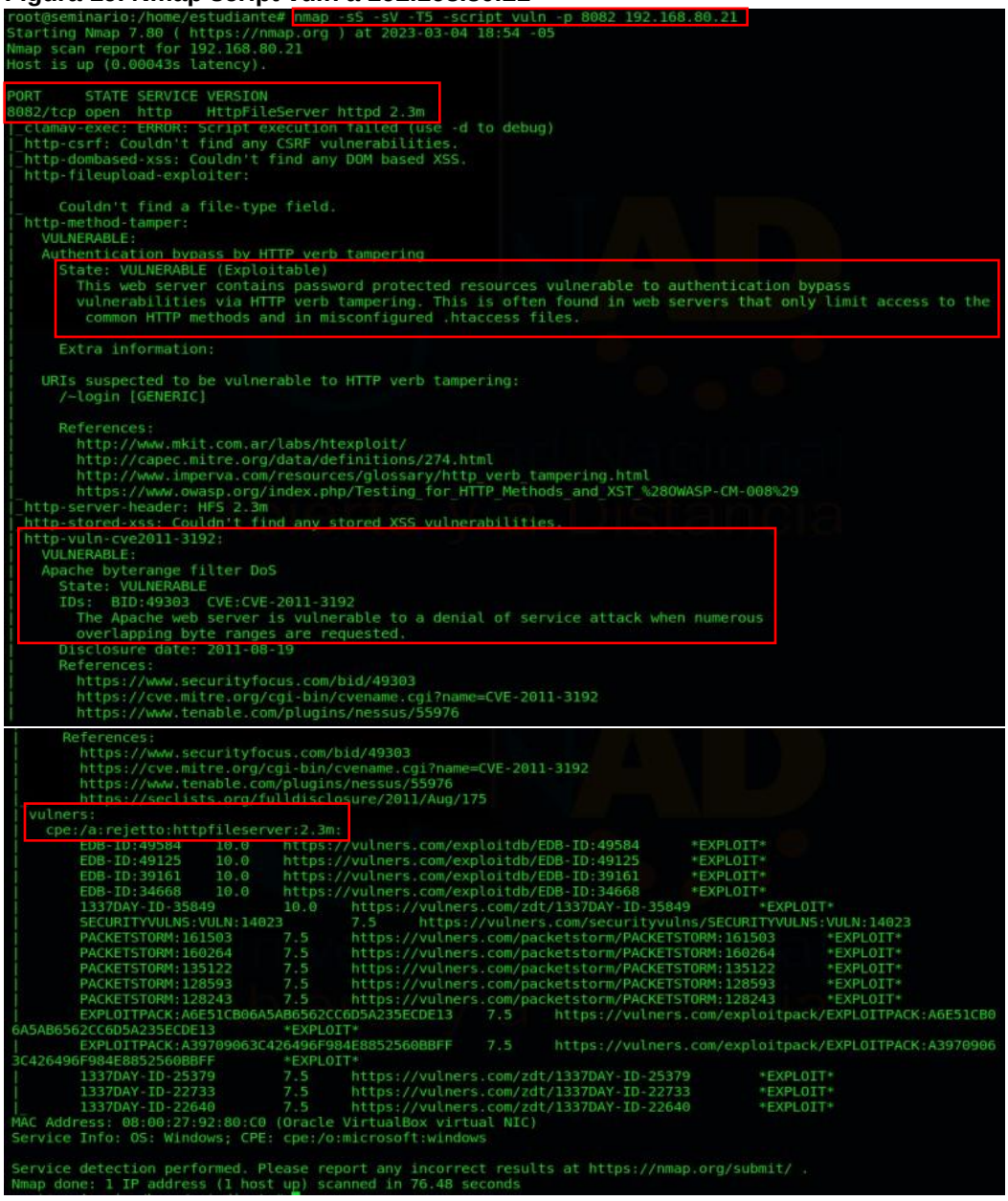


Fuente: creación propia

Con los resultados mostrados en la Figura 18, se conoce que la MV Windows7 X64 tiene un Firewall activo que bloquea o filtra el escaneo a los puertos y que tiene el puerto 8082 abierto.

Así las cosas, se hace un escaneo más específico al puerto abierto 8082 Para lo cual se dan las siguientes instrucciones: -sS (escaneo estándar o default) –sV (versión de los servicios que corre el puerto) –T5 (intensidad del escaneo, T5 es el más alto) –script vuln (usar el script de vulnerabilidades) –p 8082 (dirigir el escaneo al puerto 8082) 192.168.80.21 (dirección IP objetivo).

Figura 19. Nmap script vuln a 192.168.80.21



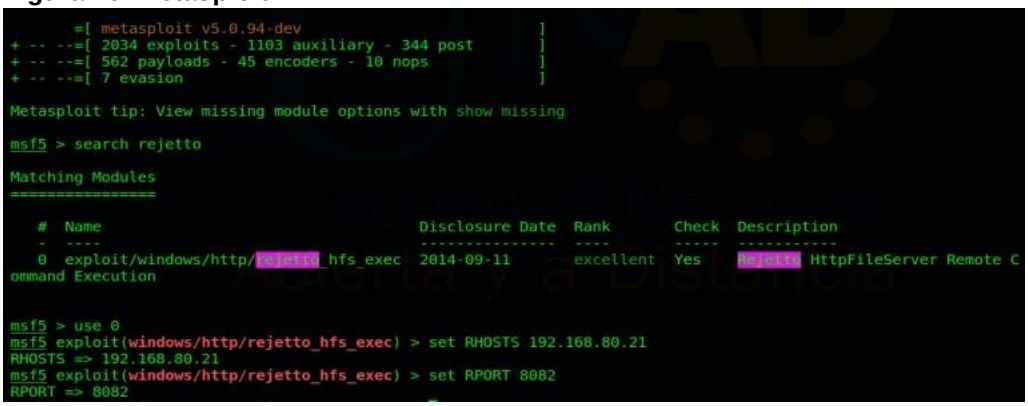
Fuente: creación propia.

Se analizan los resultados obtenidos con el segundo escaneo realizado con Nmap a las vulnerabilidades que puedan existir en el puerto y servicio abierto, estableciendo que hay varias vulnerabilidades con el servicio «rejetto http file server».

Conociendo que el puerto abierto (8082) tiene vulnerabilidades en su servicio HFS, se ejecuta con privilegios de Root en la terminal de Kali

Linux la aplicación Metasploit. Allí, se busca en la base de datos, vulnerabilidades que tengan que ver con la aplicación Rejetto.

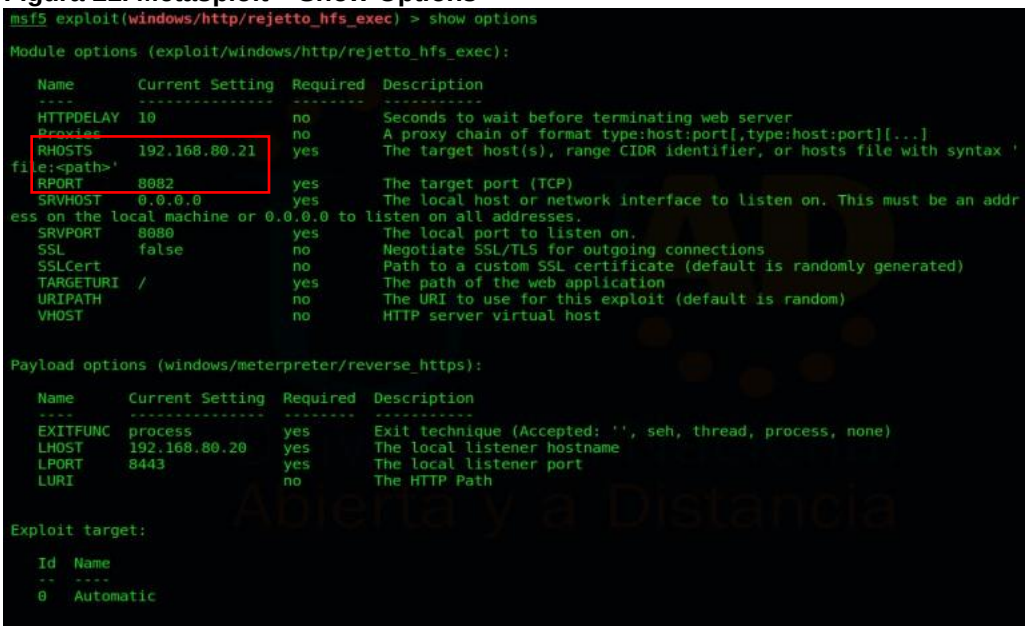
Figura 20. Metasploit



Fuente: creación propia.

Metasploit indica que halló un xploit para la aplicación Rejetto servicio HFS, motivo por el cual se ordena usar el ítem 0 y se procede a especificar la dirección IP y puerto del equipo remoto a atacar o conectar.

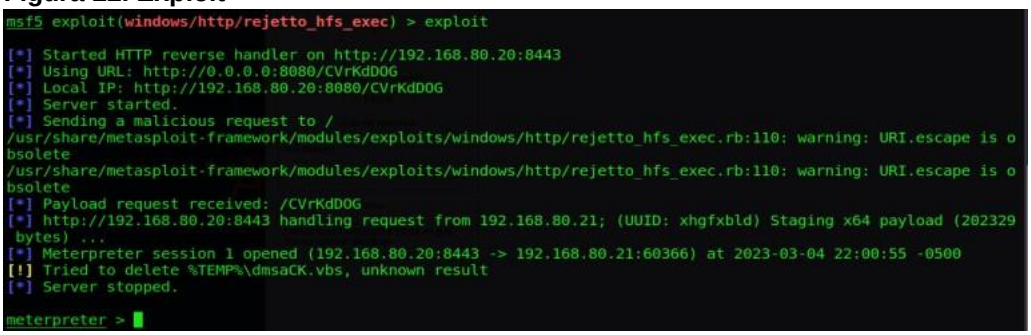
Figura 21. Metasploit – Show Options



Fuente: creación propia.

Al verificar que efectivamente se asignó la dirección IP y el puerto del equipo objetivo se ejecuta el exploit.

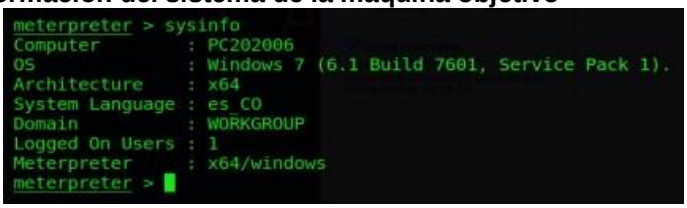
Figura 22. Exploit



Fuente: creación propia

En la Figura 22 se aprecia los pasos realizados por el xploit ejecutado, logrando establecer conexión entre las máquinas abriendo una sesión en el objetivo a través del puerto 60366.

Figura 23. Información del sistema de la máquina objetivo



Fuente: creación propia

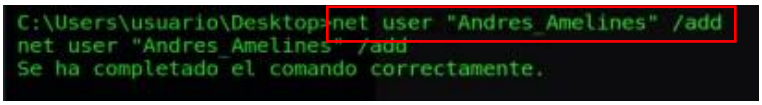
A través de la consola de Meterpreter se ingresa la instrucción «sysinfo», conociendo que la máquina objetivo tiene un sistema operativo Windows 7 SP1 con arquitectura X64, también se informa que hay un usuario logueado.

Figura 24. Shell

Fuente: creación propia

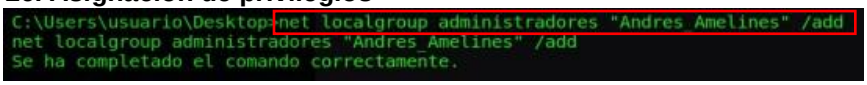
Se procede a ejecutar el Shell para dar inicio a la creación de usuario y asignación de privilegios en la máquina Windows 7 X64 (objetivo). Desde allí, se crea el nuevo usuario con el nombre y apellido del suscrito, y se le asignan privilegios de administrador como se observa en las Figuras 25 y 26.

Figura 25. Creación usuario



Fuente: creación propia

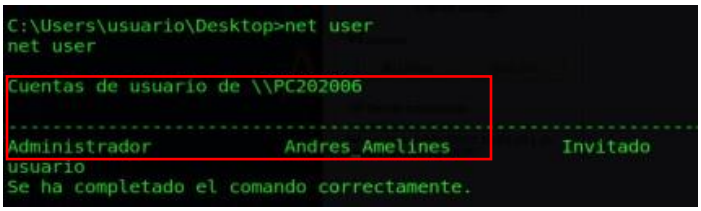
Figura 26. Asignación de privilegios



Fuente: creación propia

Para verificar la creación del usuario desde el Shell se da la instrucción «net user».

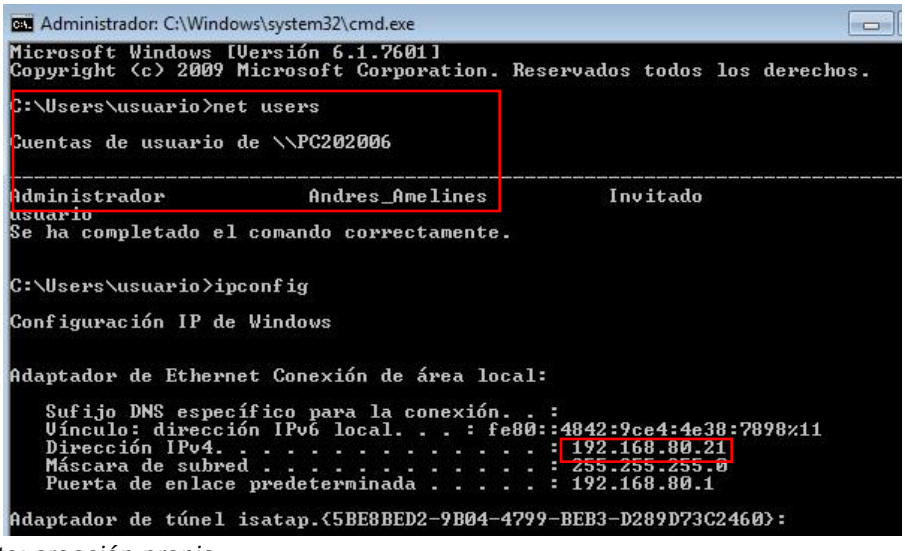
Figura 27. Verificación desde Shell



Fuente: creación propia

Desde la MV Windows 7 X64 se abre el CMD y se verifica la creación del usuario y se pide la dirección IP para corroborar que se trata de la misma máquina relacionada anteriormente.

Figura 28. CMD – Verificación.



Fuente: creación propia

Con base en lo anterior, se termina la documentación de la exploración, recopilación de datos y explotación de la vulnerabilidad aportada por la aplicación Rejetto v2.3.

2.14. ¿Qué Sería Lo Primero Que Indagaría Y Haría Si Llegara A Encontrarse Un Ataque En Tiempo Real?

Al ser detectado el incidente o ataque informático, se deben tomar las medidas establecidas en las políticas de seguridad informática de la empresa, se iniciaría generalmente con el análisis y evaluación del incidente.

Para analizar el incidente se debe contar con un conocimiento profundo del funcionamiento de la red en general, para detectar conductas anormales en la transmisión de datos, usuarios logueados, privilegios de dispositivos y usuarios, entre otros; además, revisar los LOGs de los sistemas de detección de intrusos en caso de contar con ellos (IDS/IPS).

En cuanto a la evaluación del incidente, la guía para gestionar y clasificar incidentes informáticos elaborada por el MINTIC, indica o clasifica en tres tipos de severidad o impacto:

- Alto Impacto: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Instituto. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.
- Medio Impacto: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.
- Bajo Impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto[43].

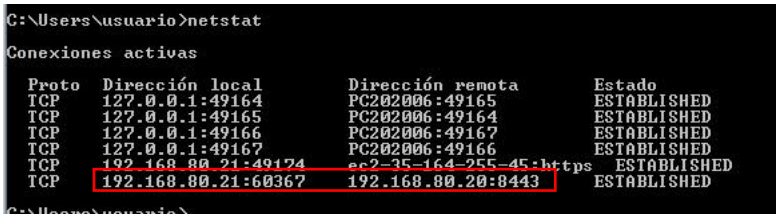
Ahora bien, basado en el ejercicio realizado en la etapa 4 del presente seminario, tras analizar y evaluar el incidente informático, se procede a clasificarlo determinando que se trata de un «Multicomponente»; ya que

[43] MINISTERIOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. MINTIC. p 29

se observa un «acceso no autorizado» y una «Modificación de recursos no autorizado»[44].

Desde la MV Windows 7 X64 se abre el CMD y con el comando «netstat» se verifican las conexiones activas en la máquina, observando que existe conexión remota establecida con la máquina 192.168.80.20, al parecer por el puerto 8443. Así de comprueba el acceso no autorizado.

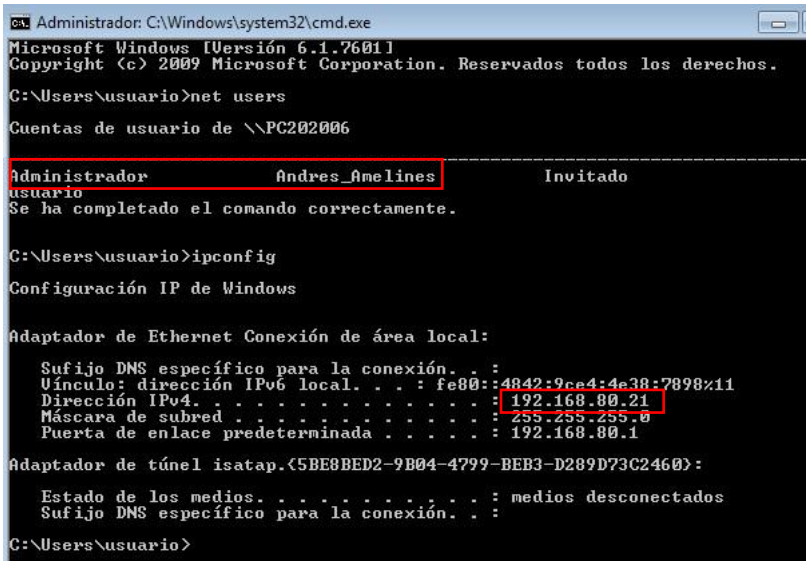
Figura 29. CMD - netstat



Fuente: creación propia

Al verificar la lista de usuarios en la MV Windows 7 X64, se aprecia que se ha creado uno nuevo «Andres_Amelines» con privilegios de «Administrador», lo cual podría conllevar a la modificación de recursos no autorizados; ya que éste, tiene las credenciales necesarias para modificar configuración del sistema.

Figura 30. Net users.



Fuente: creación propia

[44] MINISTERIOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. MINTIC. p 29.

Se verifica el LOG de eventos o «Registro de Windows» del sistema operativo Windows 7 X64, hallando los eventos correspondientes a la intrusión remota, la creación del nuevo usuario y la asignación de privilegios de administrador.

Se procede a verificar los puertos activos y abiertos en la MV afectada, hallando el puerto 8082 abierto, motivo por el cual se bloquea el puerto específico a través de las políticas del Firewall de Windows y se desconecta de la red la MV para eliminar el usuario creado, desinstalar la aplicación HFS y restablecer los servicios.

Para culminar las actividades se realiza una imagen de la MV para posterior análisis forense, se formatea el equipo para instalar nuevamente los servicios y montar el Backup; esto teniendo en cuenta que, la máquina afectada no presta un servicio primordial para la empresa.

Por último, se realizan todas las actividades Post Incidente enmarcadas en las políticas de seguridad informática de la empresa.

2.15. Medidas De Hardenización Para Evitar Ataques Informáticos.

Desde la perspectiva de Blue Team, se proponen las siguientes medidas de endurecimiento del hardware y el software, para fortalecer la seguridad informática de la empresa afectada por la fuga de información.

2.15.1. **Firewall**: son elementos indispensables al momento de hablar de seguridad en redes, ya sean perimetrales o de aplicación, se propone la instalación de éstos como primera línea de defensa, el Firewall perimetral filtrará las solicitudes que provienen del internet público hacía la red privada.

De igual forma, se propone la implementación de Firewall de Aplicación para proteger las aplicaciones ubicadas en el servidor Web y el servidor de Base de Datos, por ejemplo:

WAF (Web Application Firewall): con la implementación del WAF en la infraestructura informática de la empresa, se busca fortalecer la seguridad lógica en la capa 7[45].

[45] F5. [Sitio web]. ¿Qué es un WAF (Web Application Firewall)? [Consulta: noviembre de 2022]. Disponible en: https://www.f5.com/es_es/services/resources/glossary/web-application-firewall

DBF (Data Base Firewall): En caso de manejar bases de datos en la MV Windows 7 X64, se puede instalar un DBF en el SMDB (Sistema Manejador de Bases de Datos), esto; con el fin de filtrar las peticiones que se hagan desde la aplicación web, evitando así ataques informáticos de inyección SQL que intenten extraer datos de la base de datos o bloquear el servicio[46].

2.15.2. IDS/IPS (Intrusion Detection System / Intrusion Prevention System): Con el fin de endurecer la seguridad en la red empresarial, se pueden instalar sensores IDS/IPS para monitorear las actividades, generar alertas y tomar medidas frente a usuarios y/o solicitudes que busquen ingresar a la red privada, motivo por el cual, estarán actuando en los Firewall perimetrales[47].

2.15.3. DMZ (Demilitarized Zone): Por lo general las red empresariales proporcionan servicios a usuarios internos y externos que requieren ser consultados constantemente desde el internet público y la red privada, siendo necesario segmentarla. Con un DMZ los servidores de Correo Electrónico, el servidor ERP (Enterprise Resource Planning) y el servidor Web estarán aislados, protegiendo así, los servidores con servicios más críticos para los servicios suministrados[48].

2.15.4. HoneyPot: Dentro de la zona desmilitarizada, para ser más precavidos se ubicará una trampa o «Honeypoy»; esto con el fin de proteger la red privada de la empresa y conocer la estadística y otros datos relacionados con los ataques informáticos que buscan afectar el servicio e infraestructura de la misma[49].

2.15.5. Proxy Inverso: Aportará a la seguridad informática un eslabón más, que permitirá filtrar el tráfico o solicitudes de los usuarios (internos y externos) para luego hacer el canal de comunicación con los servidores de correo electrónico y sitio web, esto en aras de preservar en secreto las direcciones IP de estos servicios y ayudar a

[46] UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. [Sitio web]. Firewall de bases de datos. [consulta: noviembre de 2022]. Disponible en: https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

[47] INCIBE. [Sitio web]. Qué son y para qué sirven los SIEM, IDS e IPS?. [Consulta: noviembre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

[48] INCIBE. [Sitio web]. Qué es una DMZ y cómo te puede ayudar a proteger tu empresa. [Consulta: Noviembre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

[49] KASPERSKY. [Sitio web]. ¿Qué es un honeypot?. [Consulta: noviembre de 2022]. Disponible en: https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

evitar un incidente informático con el filtro de parámetros configurados[50].

2.15.6. EDR (Endpoint Detection and Response): proporcionará un filtro de seguridad extra a la infraestructura de ABC S.A.; ya que sus características técnicas (detección, contención, investigación y eliminación), permitirán monitorear el tráfico en la red y el endpoint. Gracias a su heurística, puede analizar archivos y compararlos con los parámetros establecidos por el administrador a fin de identificar diversos ataques informáticos[51].

2.15.7. MPLS (Multiprotocol Label Switching): No se debe restar importancia a las comunicaciones entre sedes y el nivel central, por ello cada una de las sedes ubicadas a nivel nacional, contarán con un canal exclusivo de comunicación privada para realizar sus labores diarias[52].

2.15.8. Actualización De Sistemas Operativos: como se pudo evidenciar en la práctica o ejercicio de la etapa 4 del presente seminario especializado, la MV afectada tiene instalado un sistema operativo Windows 7 X64 SP1, éste, no tiene soporte actualmente por el desarrollador, haciéndolo vulnerable para la seguridad informática de la empresa, motivo por el cual, se recomienda actualizar el sistema operativo a una versión 10 o superior.

2.15.9. Antivirus: las aplicaciones de Antivirus son indispensables para la seguridad informática de toda empresa; ya que permite bloquear acciones de aplicaciones maliciosas o virus que pretendan infectar un equipo o dispositivo conectado a la red.

---

[50] F5. [Sitio web]. Proxy Inverso. [Consulta: noviembre de 2022]. Disponible en: https://www.f5.com/es_es/services/resources/glossary/reverse-proxy

[51] TECNOZERO. [Sitio web]. ¿Qué es un EDR? ¿Por qué es diferente de un antivirus?. [consulta: noviembre de 2022]. Disponible en: https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/#:~:text=t%C3%A9cnicas%20de%20detecci%C3%B3n.-,%C2%BFQu%C3%A9%20es%20EDR%20en%20inform%C3%A1tica%3F,(APT)%20con%20mayor%20facilidad

[52] CITELIA.ES. [Sitio web]. ¿Qué es una red MPLS y cómo funciona?. [Consulta: noviembre de 2022]. Disponible en: https://citelia.es/blog/que-es-una-red-mpls-y-como-funciona/

2.16. ¿Diferencias Entre Un Equipo Blue Team Y Un Equipo De Respuesta A Incidentes Informáticos?

En el medio de la seguridad informática se escucha hablar mucho sobre los equipos de respuesta a incidentes, entre ellos tenemos los Blue Team y los CSIRT (Computer Security Incident Response Team) o CERT (Computer Emergency Response Team), a primera vista parecen lo mismo, pero no lo son, entre ellos existen entre muchas, las siguientes diferencias:

a) Los CSIRT son equipos conformados por expertos en informática, con el fin de analizar y plantear soluciones ante la ocurrencia de incidentes informáticos, por lo general ante la solicitud de otro CSIRT, entidad gubernamental o empresa aliada. Por otra parte, los Blue Teams funcionan al interior de las empresas con el fin de realizar actividades más preventivas frente a los ataques informáticos; ósea, tienen una cobertura local.

b) Los Blue Team, llevan a cabo actividades correctivas en la configuración de los dispositivos conectados en la red, siguiendo los protocolos establecidos en las políticas de seguridad informática de la empresa y basado en los hallazgos de los informes presentados por el Red Team, a fin de proteger los activos de la empresa de incidentes informáticos; además, suministran recomendaciones a los altos directivos para la creación de políticas referentes a seguridad informática de la empresa.

2.17. ¿En Qué Utilizar Un CIS “Center For Internet Security”?

En el caso específico de la práctica realizada en la etapa 4 del presente seminario especializado y haciendo parte del Blue Team, podría utilizar el CIS en la MV Windows 7 X64 para evaluar su seguridad informática y tomar medidas preventivas, como por ejemplo haber filtrado en el Firewall perimetral y del Sistema Operativo el puerto 8082 y todos aquellos que no se están usando, esto teniendo en cuenta que, al parecer es un sistema heredado con vulnerabilidades[53].

De igual manera, puede ser un buen complemento para las políticas empresariales de seguridad informática; ya que brinda, las recomendaciones del desarrollador del servicio y otros expertos en el

[53] AMAZON WEB SERVICES. [Sitio web]. ¿En qué consisten los puntos de referencia del CIS?. [Consultado: Marzo de 2023]. Disponible en: https://aws.amazon.com/es/what-is/cis-benchmarks/

tema en diferentes frentes y para diversos dispositivos, como: dispositivos móviles, sistemas operativos (parches de seguridad, control de acceso), puertos de equipos, servicios en la nube, entre otros.

2.18. ¿Qué es un SIEM?

Por sus siglas en inglés Security Information and Event Management, son herramientas que permiten centralizar los datos referentes a incidentes y amenazas detectadas en los dispositivos conectados en la red, permitiendo tomar medidas en tiempo real; además, crea informes sobre alertas para ser analizados por los administradores del sistema, Microsoft en su sitio web, brinda la siguiente definición:

> La Administración de eventos e información de seguridad, SIEM, para abreviar, es una solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones del negocio.
>
> SIEM (pronunciado "sim") combina la administración de información de seguridad (SIM) y la administración de eventos de seguridad (SEM) en un solo sistema de administración de seguridad. La tecnología SIEM recopila datos de registro de eventos de varias fuentes, identifica la actividad que se desvía de la norma con análisis en tiempo real y toma las medidas adecuadas.
>
> En resumen, SIEM proporciona a las organizaciones visibilidad sobre la actividad de su red para que puedan responder rápidamente a posibles ataques cibernéticos y cumplir los requisitos de cumplimiento.
>
> En la última década, la tecnología SIEM ha evolucionado y utiliza la inteligencia artificial para hacer que la detección de amenazas y la respuesta a incidentes sean más inteligentes y rápidas[54].

Actualmente, se está incorporando Inteligencia Artificial a las herramientas SIEM para automatizar medidas preventivas y respuesta a incidentes en tiempo real.

2.19. Tres Herramientas De Contención De Ataques Informáticos.

Partiendo del concepto contención, dado por el Instituto Nacional de Ciberseguridad de España (INCIBE):

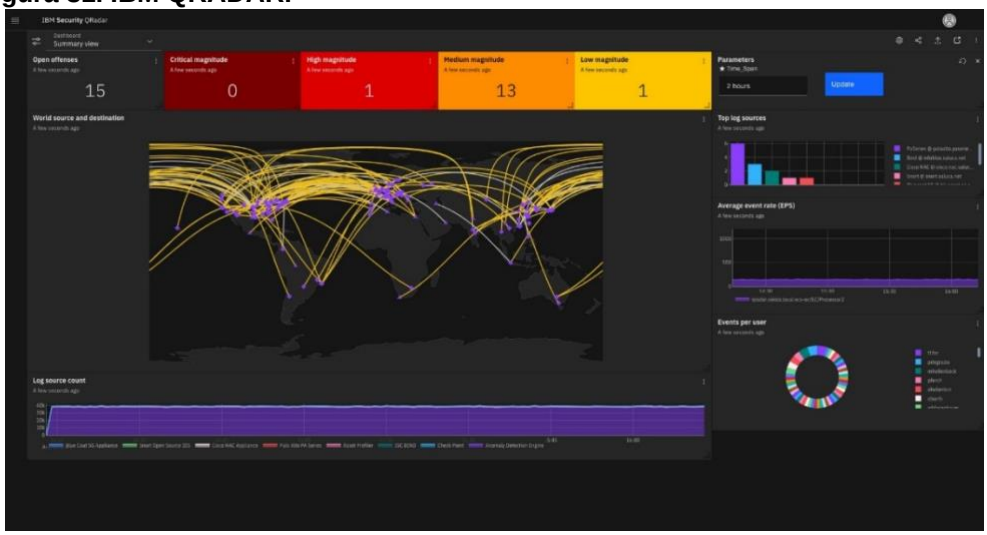
[54] MICROSOFT. [Sitio web]. SIEM definida. [Consultado: marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

impidiendo que el incidente se extienda a otros recursos. Como consecuencia, se minimizará su impacto (separando equipos de la red afectada, deshabilitando cuentas comprometidas, cambiando contraseñas, etc.)[55].

Se relacionarán tres herramientas de contención de incidentes informáticos:

IBM QRADAR XDR: gracias a la integración de herramientas EDR (Endpoint Detection and Response), NDR (Network Detection and Response) y SIEM (Security Information and Event Management), IBM QRADAR XDR se convierte en una herramienta de contención importante para todo administrador o encargado de seguridad en red informática; ya que dispondrá de informes de amenazas y vulnerabilidades que ponen en riesgo los activos de la empresa, logrando contener en tiempo real el incidente informático[56].

Figura 31. IBM QRADAR.



Fuente: ibm.com

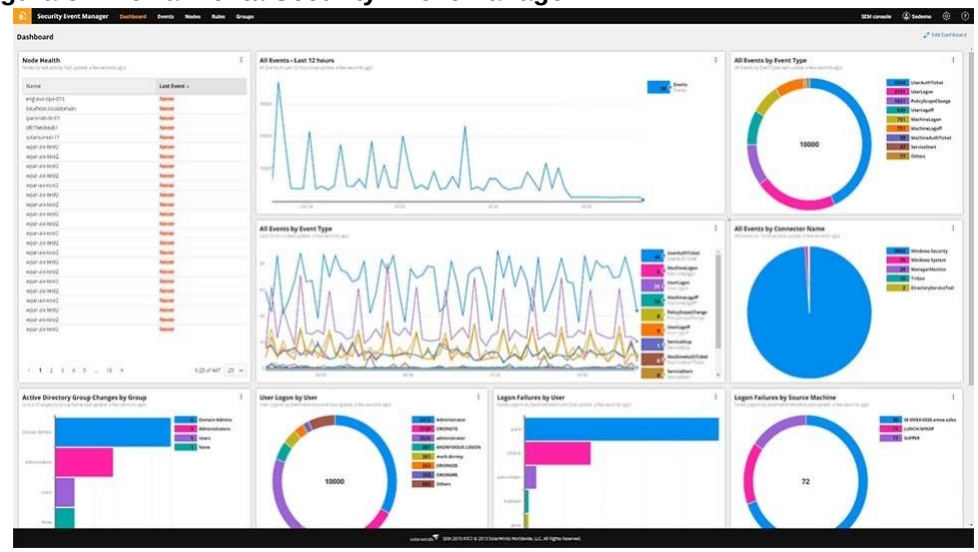
SECURITY EVENT MANAGER: la empresa SolarWinds pone a disposición esta herramienta, tiene características como: informes de cumplimiento, inteligencia de ciberamenazas, respuesta a incidentes automatizada, análisis forense y monitoreo de integridad de archivos;

[55] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). [Sitio web]. Respuesta a incidentes, ¿estais preparados?. [Consultado: marzo de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/respuesta-incidentes-estais-preparados

[56] IBM. [Sitio web]. IBM Security Qradar. [Consultado: marzo de 2023]. Disponible en: https://www.ibm.com/mx-es/qradar

además, cuenta con SEM y SIEM[57]. Facilita el control de eventos e incidentes informáticos en una red empresarial al administrador y/o sus colaboradores.

Figura 32. Herramienta Security Event Manager



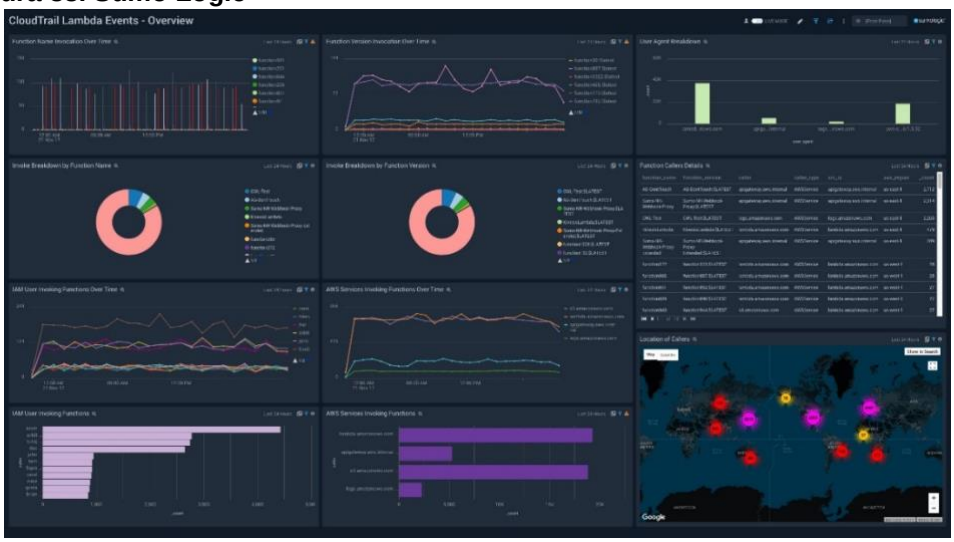
Fuente: solarwinds.com

SUMO LOGIC: Al igual que las herramientas anteriores, Sumo Logic ha procurado desarrollar una interfaz gráfica completa, que permita al administrador o encargado de la seguridad informática de la empresa visualizar el tráfico en red, alertas, y demás procesos configurados; además, si se desea puede tomar medidas de contención y eliminación de amenazas de forma automática[58].

[57] SOLARWINDS. [Sitio web]. Security Event Manager. [Consultado: marzo de 2023]. Disponible en: https://www.solarwinds.com/security-event-manager

[58] SUMO LOGIC. [Sitio web]. Making the world's apps reliable and secure. [Consultado: marzo de 2023]. Disponible en: https://www.sumologic.com/

Figura 33. Sumo Logic



Fuente: sumologic.com

2.20. Aspectos para el Desarrollo de Estrategias de Red/BlueTeam.

Al hablar de estrategias, se abre un abanico de posibilidades para cada uno de los equipos, referente a los Red Teams uno de los aspectos que ayudarían a desarrollar y/o mejorar sus métodos, es asistir a los diversos eventos de ciberseguridad a nivel mundial, allí se presentan muchos exponentes con nuevas técnicas y herramientas, también se puede realizar cursos específicos en pentesting y certificaciones con validez internacional.

En cuanto a los Blue Team, las certificaciones internacionales también aplican como por ejemplo en ISO 27001, CHFI, CISSP, entre otros, que permitan ampliar sus conocimientos y herramientas a la hora de enfrentar un incidente informático y a la hora de corregir fallas o vulnerabilidades en la red.

2.21. Estrategias para Endurecer la Seguridad en una Organización.

Debido al aumento desmesurado de los ataques informáticos a nivel mundial, el constante avance tecnológico y el amplio acceso a información por medio de internet, las redes privadas y empresariales se han convertido en un blanco para los ciberdelincuentes, siendo necesario

tomar medidas por parte de los directivos de dichas corporaciones para proteger sus activos.

En vista de lo anterior, se hacen las siguientes recomendaciones:

- Selección de personal capacitado en las diversas áreas que comprenden el Gobierno TI.

- Capacitación de todo el personal que compone la planta empresarial en temas relacionados con las políticas de seguridad informática.

- Auditorías internas y externas en relación con el cumplimiento de las políticas de seguridad informática.

- Por medio del Gobierno TI y los Red Team y Blue Team, hacer auditorías de seguridad informática periódicas, así como, implementar la «hardenización» en la red privada, siguiendo las recomendaciones dadas en el ítem 2.15 del presente documento.

2.22. Conclusiones para la Construcción de Conocimiento en Ciberseguridad.

La construcción del conocimiento en temas de ciberseguridad debe partir desde lo académico y la experiencia, como se sabe, la tecnología crece o avanza a pasos agigantados y los profesionales en esta área del conocimiento no deben ser ajenos a ello, razón por la cual deben estar actualizados sobre nuevas amenazas y sistemas de protección.

De igual manera, se sugiere hacer parte de grupos de expertos por medios virtuales o remotos donde se compartan experiencias profesionales, dudas e inquietudes, algo similar a los CSIRT.

3. CONCLUSIONES

Por medio del presente trabajo se logró describir con palabras propias las principales características de las leyes emanadas en Colombia relacionada con los delitos informáticos y protección de datos personales, tales como la ley 1273 de 2009, ley 1581 de 2012 y la ley 1928 de 2018.

Asimismo, se relacionaron las etapas que componen la prueba de penetración o «pentesting», así como, las herramientas y servicios online usados por los expertos para tal fin. De igual manera, se realizó la instalación o montaje del «banco de trabajo» requerido para llevar a cabo el «pentesting» a la MV Windows 7 X64 SP1.

Desde la perspectiva del suscrito, se dio concepto ético y legal respecto a la propuesta o «acuerdo de confidencialidad» requerido por la empresa «Whitehouse Security» a sus futuros colaboradores.

Por otra parte, se logró describir el procedimiento realizado desde el enfoque del Blue Team ante un incidente informático en tiempo real, se dieron algunas recomendaciones de endurecimiento de medidas de seguridad informáticas, basado en el ejercicio de la etapa 3.

Finalizando en documento, se plasmaron las principales diferencias entre un grupo de expertos en informática que conforma un Blue Team y los que conforman un Equipo de Respuesta a Incidentes de Seguridad Informáticos – CSIRT.

4. RECOMENDACIONES

A toda la población interesada en el tema de la seguridad informática; ya sea desde el campo de acción de Red Team o Blue Team, se les exhorta a seguir investigando y ahondar en esta área, con el fin de desarrollar nuevas técnicas y métodos más avanzados que permitan efectuar análisis más completos, claros y sólidos respecto a la identificación de vulnerabilidades y la protección de la infraestructura de la red privada y los activos empresariales.

Como se manifestó anteriormente, el conocimiento se construye desde la base de lo académico y la experiencia, siendo importante invitar a las universidades y centros de educación, para ampliar y enriquecer la oferta en áreas del conocimiento referentes a la ciberseguridad, proporcionando los medios necesarios e idóneos a los estudiantes, quienes serán los futuros profesionales que llegarán a fortalecer esta rama del saber con buenos principios y ética.

Al sector público y privado, se les recomienda no escatimar en costos al momento de proteger su infraestructura y activos de los ciberdelincuentes, tampoco al momento de contratar el personal que integrará su planta de colaboradores; que ya estos factores serán decisivos para el correcto funcionamiento de la Entidad o Empresa, al contar con los elementos idóneos (hardware y software) y el personal calificado será posible hacer frente a los nuevos desafíos propuestos por el mundo virtual.

5. ANEXO

Enlace video sustentación.

https://unadvirtualedu-my.sharepoint.com/:v:/g/personal/aamelinesa_unadvirtual_edu_co/EXBlZ7CZfbJAiAfTqb9_tfIBdUYTLyCf3S4_FaEC6X0kFA?e=zUT4F3

BIBLIOGRAFÍA

AMAZON WEB SERVICES. [Sitio web]. ¿En qué consisten los puntos de referencia del CIS?. [Consultado: Marzo de 2023]. Disponible en: https://aws.amazon.com/es/what-is/cis-benchmarks/

BANCO SANTANDER. [Sitio web]. ¿Qué es una vulnerabilidad informática? [Consultado: marzo de 2023]. Disponible en: https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=Las%20vulnerabilidades%2C%20tanto%20las%20relativas,atacantes%20para%20burlar%20su%20seguridad.

BARWISE, Ian. The Red Team Guide, A practical guide for Red Teams and Offensive Security. Peerlyst. p.241.

CAMPUSCIBERSEGURIDAD. [Sitio web]. ¿Qué es el Pentesting? [Consultado: marzo de 2023]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

CIBERSEGURIDAD.COM. [Sitio web]. ¿Qué es Metasploit framework y cómo funciona?. [Consultado: febrero de 2023]. Disponible en: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

CITELIA.ES. [Sitio web]. ¿Qué es una red MPLS y cómo funciona?. [Consulta: noviembre de 2022]. Disponible en: https://citelia.es/blog/que-es-una-red-mpls-y-como-funciona/

CLOUDFLARE. [Sitio web]. ¿Qué es un puerto de ordenador?. [Consultado: marzo de 2023]. Disponible en: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-computer-port/#:~:text=Los%20puertos%20son%20lugares%20virtuales,tr%C3%A1fico%20de%20red%20que%20reciben.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 906 (31, agosto, 2004). Por la cual se expide el Código de Procedimiento Penal. En diario oficial. Agosto, 2009.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En diario oficial. Enero, 2009.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley estatutaria 1581 (18, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. En diario oficial. Octubre, 2012.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1621 (14, abril, 2013). Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". En diario oficial. Abril, 2013.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1928 (24, julio, 2018). Por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en budapest. En diario oficial. Octubre, 2012

COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. CONPES 3854 (abril 11 de 2016). Política nacional de seguridad digital. Departamento Nacional de Planeación. Abril, 2016. p. 1-91.

COLOMBIA. CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA. Ley 842 de 2003 (9, octubre, 2003). Por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones. En diario oficial. Octubre, 2003.

CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA (COPNIA). [Sitio web]. Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. [Consulta: febrero de 2023]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

COLOMBIA. Constitución Política de Colombia (20, julio, 1991). En diario oficial. Julio, 1991.

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1377 de 2013 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. En diario oficial. Junio, 2013.

CONSEJO DE EUROPA. Convenio número 185 – Ciberdelincuencia. Budapest, 2001.

CVE [Sitio web]. CVE-2014-6287. [Consultado: marzo de 2023]. Disponible en: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

ELTIEMPO. [Sitio web]. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [Consultado: febrero de 2023]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

GUTIERREZ, Pablo. Hacker's White book – cómo convertirte en un hacker profesional. Monterrey, Nuevo León: whitesuit hacking, 2019. p.563

F5. [Sitio web]. Proxy Inverso. [Consulta: noviembre de 2022]. Disponible en: https://www.f5.com/es_es/services/resources/glossary/reverse-proxy

F5. [Sitio web]. ¿Qué es un WAF (Web Application Firewall)? [Consulta: noviembre de 2022]. Disponible en: https://www.f5.com/es_es/services/resources/glossary/web-application-firewall

IBM. [Sitio web]. IBM Security Qradar. [Consultado: marzo de 2023]. Disponible en: https://www.ibm.com/mx-es/qradar

INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). [Sitio web]. Qué son y para qué sirven los SIEM, IDS e IPS?. [Consulta: noviembre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). [Sitio web]. Qué es una DMZ y cómo te puede ayudar a proteger tu empresa. [Consulta: Noviembre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). [Sitio web]. Respuesta a incidentes, ¿estais preparados?. [Consultado: marzo de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/respuesta-incidentes-estais-preparados

JUNTA INTERAMERICANA DE DEFENSA. Guía de ciberdefensa: orientaciones para el diseño, planteamiento, implantación y desarrollo de una ciberdefensa militar. Canadá, 2020. 113 p

KASPERSKY. [Sitio web]. Qué es una dirección IP: definición y explicación. [Consulta: noviembre de 2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address

KASPERSKY. [Sitio web]. ¿Qué es un honeypot?. [Consulta: noviembre de 2022]. Disponible en: https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

KEEPCODING. [Sitio web]. ¿Qué es Meterpreter?. [Consulta: marzo de 2023]. Disponible en: https://keepcoding.io/blog/que-es-meterpreter/#:~:text=Meterpreter%20es%20un%20payload%20que,es%20bastante%20dif%C3%ADcil%20de%20detectar

KEEPCODING. [Sitio web]. ¿Qué es Red Team en Ciberseguridad?. [Consulta: noviembre de 2022]. Disponible en: https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

MICROSOFT. [Sitio web]. SIEM definida. [Consultado: marzo de 2023]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

MINISTERIOR DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. MINTIC. p 29.

NMAP.ORG. [Sitio web]. Guía de referencia de Nmap (Página de manual). [Consultado: marzo de 2023]. Disponible en: https://nmap.org/man/es/index.html

NMAP. [Sitio Web]. Nmap: Descubre tu red. [Consultado: febrero de 2023]. Disponible en: https://nmap.org/

OPENWEBINARS. [Sitio web]. Qué es OpenVAS. [Consultado: febrero de 2023]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

PANDASECURITY. [Sitio web]. ¿Qué es un Exploit? [Consultado: marzo de 2023]. Disponible en: https://www.pandasecurity.com/es/security-info/exploit/

PERSONALES.UPV.ES [Sitio web]. Ping. [Consultado: Marzo de 2023]. Disponible en: http://personales.upv.es/rmartin/TcpIp/cap02s05.html#:~:text=Ping%20es%20la%20aplicaci%C3%B3n%20m%C3%A1s,tiempo%20de%20ida%20y%20vuelta

REDHAT. [Sitio web]. El concepto de CVE. [Consultado: febrero de 2023]. Disponible en: https://www.redhat.com/es/topics/security/what-is-cve

SEMANA [Sitio web]. El informe que sacudió el caso de la fachada Andrómeda. [Consultado: febrero de 2023]. Disponible en: https://www.semana.com/nacion/articulo/el-informe-que-sacudio-el-caso-de-la-fachada-andromeda/415642-3/

SOFTZONE.ES [Sitio web]. Domina la Terminal de Linux como un profesional. [Consultado: Marzo de 2023]. Disponible en: https://www.softzone.es/linux/tutoriales/terminal-linux/

SOLARWINDS. [Sitio web]. Security Event Manager. [Consultado: marzo de 2023]. Disponible en: https://www.solarwinds.com/security-event-manager

SUMO LOGIC. [Sitio web]. Making the world's apps reliable and secure. [Consultado: marzo de 2023]. Disponible en: https://www.sumologic.com/

TENABLE. [Sitio web]. Cierre su brecha de exposición cibernética con Nessus. [Consultado: febrero de 2023]. Disponible en: https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial/?utm_campaign=gs-{11596512476}-{116641138521}-{537515898224}_00026643_fy23&utm_promoter=tenable-hv-brand-00026643&utm_source=google&utm_term=nessus&utm_medium=cpc&utm_geo=latam&gclid=EAIaIQobChMIht2m88WD_QIV0vbjBx1ZngX_EAAYASAAEgK_S_D_BwE

TECNOZERO. [Sitio web]. ¿Qué es un EDR? ¿Por qué es diferente de un antivirus?. [Consulta: noviembre de 2022]. Disponible en: https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/#:~:text=t%C3%A9cnicas%20de%20detecci%C3%B3n.-,%C2%BFQu%C3%A9%20es%20EDR%20en%20inform%C3%A1tica%3F,(APT)%20con%20mayor%20facilidad

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. [Sitio web]. Firewall de bases de datos. [Consulta: noviembre de 2022]. Disponible en: https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

UNIVERSITY OF FOREIGN MILITARY AND CULTURAL STUDIES. The Red Team Handbook, the army's guide to making better decisions. p.238.

VMWARE. [Sitio web]. Definición de «máquina virtual». [Consultado: marzo de 2023]. Disponible en: https://www.vmware.com/latam/topics/glossary/content/virtual-machine.html

WIKI. [Sitio web]. HFS: Introducción. [Consultado: marzo de 2023]. Disponible en: https://www.rejetto.com/wiki/index.php?title=HFS:_Introducci%C3%B3n