INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

UNIDAD CULHUACAN

"ESTUDIO DE METODOLOGÍAS PARA PRUEBAS DE PENETRACIÓN A SISTEMAS INFORMÁTICOS"

T E S I S

QUE PARA OBTENER EL GRADO DE

MAESTRO EN INGENIERÍA EN SEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

PRESENTA

Ing. AGUSTÍN LÓPEZ LÓPEZ

ASESORES:

M. en C. MARCOS ARTURO ROSALES GARCÍA

Dr. GUALBERTO AGUILAR TORRES

MEXICO D.F. DICIEMBRE 2011

SIP-14-BIS

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D. F. siendo las 12:00 horas del día 1° del mes de diciembre del 2011 se reunieron los miembros de la Comisión Revisora de la Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI ESIME CULHUACAN para examinar la tesis titulada:

"Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos"

Presentada por el alumno:

López	**López**	**Agustín**
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

B	0	9	1	8	0	6

aspirante de:

MAESTRÍA EN INGENIERÍA EN SEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Directores de tesis

M. en C. Marcos Arturo Rosales García

Dr. Gualberto Aguilar Torres

Dr. Gabriel Sánchez Pérez

Dra. Linda Karina Toscano Medina

Dr. Moisés Salinas Rosales

INSTITUTO POLITECNICO NACIONAL ESTADOS UNIDOS MEXICANOS
S.E.P.
SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION ESIME CULHUACAN

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Gonzalo Isaac Duchen Sánchez

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México, D.F. el día 1 del mes de Diciembre del año 2011, el (la) que suscribe Agustín López López alumno (a) del Programa de Maestría en Ingeniería en Seguridad y Tecnologías de la Información con número de registro B091806, adscrito a la Sección de Estudios de Posgrados e Investigación de la ESIME Unidad Culhuaca, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección de M. en C. Marcos Arturo Rosales García y del Dr. Gualberto Aguilar Torres y cede los derechos del trabajo intitulado **"Estudio de Metodologías para Pruebas de Penetración a Sistemas Informáticos"**, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección agus_lopez85@hotmail.com, marosales@ipn.mx y gaguilar@ipn.mx. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Agustín López López

Nombre y firma

RESUMEN

En este trabajo se realiza el análisis de tres metodologías de pruebas de penetración (NIST SP800-115, EC-Council LPT y OSSTMM), que consiste en describir sus procedimientos, las técnicas, el enfoque y la forma en que cada una de ellas concibe la seguridad en un sistema informático. Cada una de las metodologías es descrita con diagramas de flujos y con tablas para su mejor entendimiento.

Posteriormente de entender cada una de las metodologías, se realiza la comparación entre ellas, teniendo como referencia las etapas que conforman un Hacking Ético. De esta forma es visualizada las semejanzas y diferencias entre cada una de ellas, teniendo como resultado criterios para la aplicación de cada una de las metodologías.

ABSTRACT

This paper is the analysis of three penetration testing methodologies (NIST SP800-115, EC-Council LPT and OSSTMM), which is to describe its procedure, techniques, approach and the way each conceives the security in a computer system. Each methodology is described with flow charts and tables for better understanding.

Then to understand each of the methodologies, the comparison is made between them, taking as reference the stages comprising an Ethical Hacking. In this way displayed the similarities and differences between each, resulting in the application of criteria for each of the methodologies.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad se está prestando mayor atención el nivel de seguridad en los sistemas informáticos, con la elaboración de mejores prácticas, estándares y leyes. Entre estas actividades para determinar el nivel de seguridad de una organización se encuentran las metodologías de pruebas de penetración, análisis de riesgos y auditorías de seguridad.

En el capítulo 1 se dan tres definiciones de las pruebas de penetración desde el punto de vista de las metodologías contempladas en este trabajo, sus objetivos, así como los tipos de pruebas que hay. También se realiza una clasificación de las pruebas de penetración y es proporcionada una explicación general cada una de ellas.

En el capítulo 2 se realiza el estudio de cada una de las metodologías, se expone en qué consiste las actividades y las herramientas.

En el capítulo 3 se realiza el estudio comparativo de las tres metodologías, NIST SP800-115, EC-Council LPT y OSSTMM; tomando como referencia las etapas de un Hacking Ético; de esta forma es visualizada las diferencias y semejanzas entre cada una de ellas.

En el capítulo 4 son presentadas las conclusiones del estudio comparativo de las del NIST SP800-115, EC-Council LPT y OSSTMM.

PLANTEAMIENTO DEL PROBLEMA

En los últimos años se ha dado un crecimiento exponencial del uso de Internet. De acuerdo con cifras de COFETEL, en el 2010 son contemplados un poco más de 34 millones de usuarios de Internet en México (COFETEL, 2010). El Internet ya es considerado como una necesidad en los sectores empresariales y educativos. Por otro lado, el crimen cibernético está aprovechando la mala administración y/o la falta de los controles de seguridad de los sistemas informáticos, trayendo como consecuencia fraudes electrónicos, el robo de información, la denegación de servicios, spam, phishing, malware, botnets, etc.

En la siguiente tabla se muestra el número de incidentes informáticos de acuerdo con el CERT de la UNAM (CERT UNAM, 2011).

Tabla 1 Reporte anual por tipo de Incidente en Red UNAM 2010

Mes	Bot	Escaner	Gusano	Malware	Denegación de Servicio	Otros	Phishing	Spam	Total
Ene	8515	2	0	0	4	2250	0	332	11103
Feb	4505	0	0	0	3	8	2	1153	5671
Mar	347	5	0	0	97	19	2	1200	1670
Abr	343	2	0	2	57	57	1	1842	2304
May	656	2	0	0	56	9	0	1333	2056
Jun	760	0	0	0	214	0	3	1264	2241
Jul	595	2	0	0	2	1	0	586	1186
Ago	1079	5	0	0	71	1	0	1375	2531

Sep	1059	1	0	0	1	5	0	1149	2215
Oct	527	1	1	0	15	3	0	1076	1623
Nov	611	4	0	0	51	4	0	883	1553
Dic	321	0	0	0	1	0	0	433	755
Total	19318	24	1	2	572	2357	8	12626	34908

La aparición y crecimiento exponencial de incidentes o delitos informáticos ha generado la necesidad de mejorar la seguridad de los sistemas informáticos para no ser víctimas de ataques informáticos.

Muchos administradores de sistemas informáticos desconocen si su infraestructura tiene un nivel aceptable de seguridad o en qué puntos necesita mejorar. Dentro de las alternativas para cubrir esta necesidad, está la aplicación de pruebas de penetración a los sistemas informáticos, aunque una prueba de este tipo generalmente implica un fuerte gasto para las organizaciones, por lo tanto, no todas tiene la posibilidad de aplicarlas.

OBJETIVO

Estudio comparativo de tres Metodologías de Pruebas de Penetración mediante el uso de las etapas de un Hacking Ético, para identificar sus semejanzas y diferencias, con la finalidad de determinar en qué escenarios es más adecuada la aplicación de cada una de ellas.

OBJETIVOS PARTICULARES

- Estudio de las siguientes metodologías de Pruebas de Penetración:
    - National Institute of Standards and Technology Special Publication 800-115 (NIST SP800-115).
    - EC-Council Licensed Penetration Tester (EC-Council LPT).
    - The Open Source Security Testing Methodology Manual (OSSTMM).
- Estudio comparativo entre cada una de las metodologías.
- Determinar qué metodología aplicar dependiendo de las necesidades de la organización.

JUSTIFICACIÓN

Dado que en los últimos años se han incrementando los ataques a los distintos tipos de empresas y organizaciones, de igual forma han evolucionando las técnicas de los atacantes para cometer delitos informáticos; surge la necesidad de evolucionar las formas de proteger los sistemas informáticos.

Uno de los caminos es a través de las pruebas de penetración, que hacen uso de las técnicas utilizadas por los mismos atacantes para cometer sus delitos. Una prueba de penetración nos ayuda a valorar los controles de protección de la organización, así como mostrarnos los puntos débiles de una infraestructura que a simple vista no son tan evidentes de observar (McAfee, 2011).

En este trabajo, se analizan y comparan de tres metodologías. El criterio de selección fue tomar una metodología del gobierno de los Estados Unidos (NIST SP800-115), una metodología propietaria (EC-Council LPT) y una metodología de código abierto (OSSTMM). Con esta selección de metodologías, se pretende abarcar distintos enfoques y objetivos en la realización de pruebas de penetración.

Para el estudio comparativo, se toma como referencia las etapas que conforman un Hacking Ético, mediante estas etapas son determinas las semejanzas y diferencias de las tres metodologías anteriormente mencionadas. Las metodologías para pruebas de penetración son derivadas de las etapas de un Hacking Ético, por tal motivo es la métrica que utilizamos para realizar nuestro estudio.

Capítulo 1

Generalidades de Pruebas de Penetración

En este capítulo se muestra un panorama general de las pruebas de penetración, como son las distintas formas de realizarlas y una clasificación de las mismas. También se describen otras metodologías de pruebas de penetración.

1.1 Definición de una Prueba de Penetración

A continuación son presentadas distintas definiciones de pruebas de penetración, de acuerdo a las tres metodologías que se analizan en este trabajo:

- Son las pruebas de seguridad en el que las personas que los realizan imitan los ataques del mundo real en un intento por identificar los métodos para eludir las medidas de seguridad de una aplicación, sistema o red. Las pruebas de intrusión a menudo implica la realización de ataques a sistemas y datos, usando las mismas herramientas y técnicas utilizadas por los atacantes (Scarfone, 2008).
- Son pruebas de seguridad en la que especialistas explotan las vulnerabilidades de un sistema informático de forma controlada para evaluar los controles de seguridad de dicho sistema. (EC-Council, 2010).
- Es el resultado final de un proceso o solución que define qué o quién se pone a prueba, así como cuándo y dónde es realizada dicha prueba. (Herzog, 2010).

A partir de estas definiciones, podemos notar el enfoque que tienen cada una de las metodologías en la aplicación de las pruebas de penetración, en donde la definición más rebuscada es la definición dada por OSSTMM.

1.2 Objetivos de una Prueba de Penetración

Los objetivos de cualquier prueba de penetración son los siguientes:

- Probar y validar la eficacia de los controles de seguridad de una organización.
- Identificar las vulnerabilidades de la organización, tanto interna como externamente.

- A través de la recopilación de información de las pruebas de seguridad, proporcionar evidencia real, amplia y detallada del nivel de seguridad de una organización.
- Ayuda en la priorización de la aplicación de los parches adecuados para las vulnerabilidades reportadas.
- Descubrir sí la infraestructura de la red y/o los sistemas de una organización requieren de un cambio o mejora en su diseño.
- Ayuda a alcanzar y mantener el cumplimiento con regulaciones, normas o estándares de seguridad.

Los objetivos de las pruebas de penetración son los mismos para todas, pero la forma a estos varía conforme a su metodología.

1.3 Como realizar una Prueba de Penetración

Las diferentes formas de realizar una prueba penetración son clasificadas de acuerdo con la cantidad de información que el penetration tester (pentester) sabe acerca de la organización, que tanto conoce la organización acerca del pentester o qué espera de la prueba de seguridad, y la legitimidad de la prueba (Pete, 2010). Esta clasificación es una propuesta por parte de OSSTMM.

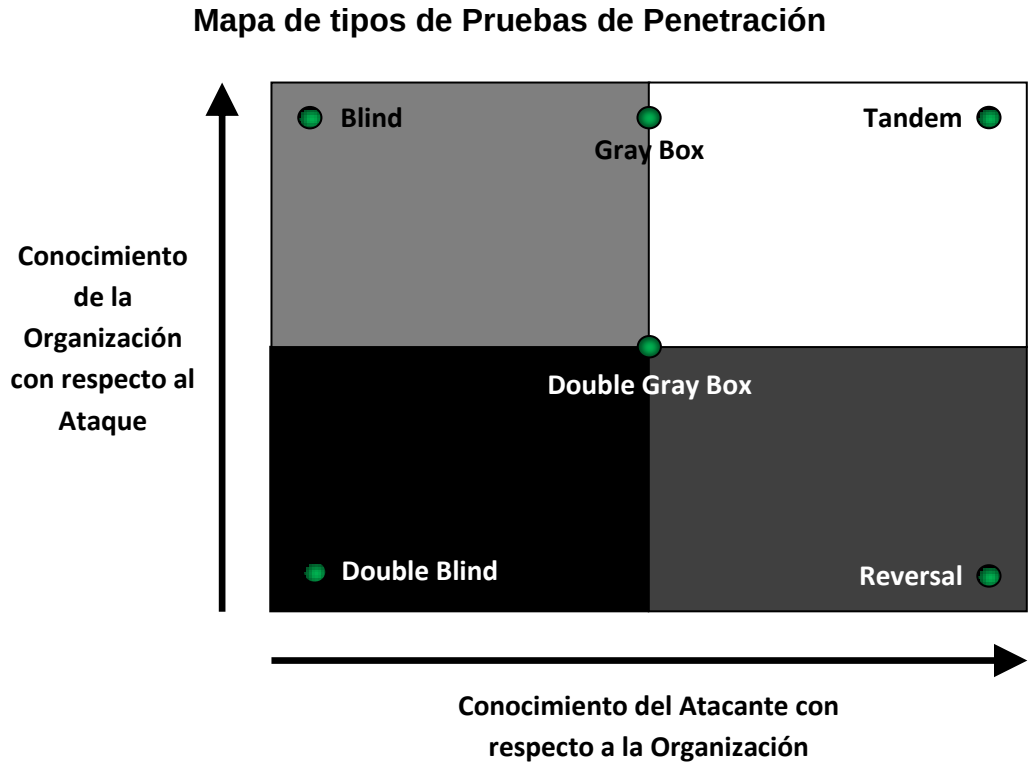

Figura 1 Mapa de las distintas de formas de realizar una prueba de penetración.(obtenido del manual de OSSTMM 3.1)

1. Blind: El pentester no tiene ninguna información previa de las defensas e infraestructura de la organización y la organización tiene conocimiento de qué tipo de pruebas se realizarán y cuándo. Principalmente pone a prueba la habilidad del pentester. También es conocido como Ethical Hacking.
2. Double Blind: El pentester en relación con la organización no tiene ningún conocimiento previo de sus defensas e infraestructura de la organización. La organización no es notificada con antelación del alcance de las pruebas de seguridad y que elementos serán probados y cuándo. Una auditoría de Double Blind prueba la habilidad del

pentester y la preparación de la organización ante ataques informáticos. También es conocida como una Prueba de Caja Negra.

3. Gray Box: El pentester en relación con la organización tiene un conocimiento limitado de sus defensas y los activos. La organización está consciente de qué tipo de pruebas se realizarán y cuándo. La amplitud y profundidad depende de la calidad de la información proporcionada al pentester antes de la prueba, así como el conocimiento aplicable del pentester. Este tipo de prueba se refiere a menudo como una prueba de vulnerabilidad y con mayor frecuencia iniciada por la organización como una auto-evaluación.
4. Double Gray Box: El analista en relación con el objetivo tiene un conocimiento limitado de sus defensas y los activos de la organización. La organización conoce las técnicas que ha de utilizar el pentester pero no conoce cómo ni cuándo serán utilizadas. El tipo Double Gray Box pone a prueba la habilidad del pentester y la preparación del objetivo a variables desconocidas de ataques. La amplitud y profundidad depende de la calidad de la información proporcionada al pentester y a la organización antes de la prueba, así como el conocimiento aplicable del pentester. También se conoce como una prueba de White Box.
5. Tandem: El pentester y la organización son preparados para las pruebas de seguridad, sabiendo de antemano todos los detalles de las pruebas. El tipo Tandem prueba la protección y los controles de la organización. Sin embargo, no se puede probar la preparación de la organización a variables desconocidas de ataques. La verdadera naturaleza de la prueba es la minuciosidad como el pentester realiza todas las pruebas. La amplitud y la profundidad depende de la calidad de la información proporcionada al pentester antes de la prueba, así como el conocimiento aplicable del analista. Esto tipo de prueba

también es conocida como una prueba de Cristal Box y el pentester es generalmente parte del personal de seguridad.

6. Reversal: El pentester en relación con la organización tiene pleno conocimiento de sus procesos y su infraestructura de seguridad, pero la organización no sabe nada de qué, cómo, cuándo el pentester realizará la prueba. La verdadera naturaleza de esta prueba es determinar la preparación de la organización ante ataques que se dan si tenga conocimiento de la forma que se desarrollarán. La amplitud y profundidad depende de la calidad de la información proporcionada al pentester y los conocimientos prácticos y la creatividad del pentester. También a menudo se llama un ejercicio Red Team.

Esta clasificación de pruebas de penetración cubre de mejor forma las distintas posibilidades de realizarlas, ya que la clasificación tradicional de caja negra, caja gris y caja blanca no abarcan todas las posibilidades.

1.4 Metodologías de Pruebas de Penetración

1.4.1 Metodologías Propietarias

Hay muchas organizaciones que aplican pruebas de penetración y además proporcionan cursos dirigidos a los especialistas en seguridad para dar a conocer su metodología. De igual forma ofrecen certificaciones para garantizar la adecuada aplicación de su metodología. Su propósito tiene fines lucrativos. Algunas metodologías de este tipo son:

- EC-Council Licensed Penetration Tester. El EC-Council (The International Council of Electronic Commerce Consultants) fue fundado en 2002 (EC-Council, 2010), actualmente es muy reconocido por preparar y certificar a personal de Tecnologías de la Información (TI), sus certificaciones más representativas son:

- Certified Ethical Hacker (CEH)
- Computer Hacking Forensics Investigator (CHFI)
- EC-Council Certified Security Analyst (ECSA)/License Penetration Tester (LPT)

En este trabajo es analizado el Lincense Penetration Testing.

- IBM-Internet Security Systems. IBM-ISS dentro de sus servicios profesionales de Seguridad, proporciona el servicio de pruebas de penetración que además de tener una metodología y herramientas propietarias, tiene el soporte de su equipo de seguridad inteligente llamado ISS X-Force, dedicado a la investigación acerca de vulnerabilidades y amenazas informáticas (IBM, 2011).
- Foundstone Professional Services. Foundstone divide en dos fases fundamentales su metodología de pruebas de penetración. La primera consiste una comprensión global y detallada de la red de la organización. La segunda fase pretende proporcionar soluciones para proteger los activos más importantes de la organización. Entre sus pruebas ofrece están: ingeniería social, pruebas de denegación de servicio, ejercicios de validación del sistema de detección de intrusos y los ejercicios de respuestas a incidentes, entre otras pruebas (McAfee, 2011).

1.4.2 Metodologías de Código Abierto (Open Source)

Estás metodologías están disponibles al público en general y no tiene fines lucrativos. Algunos ejemplos de este tipo de metodologías son:

- OSSTMM (The Open Source Security Testing Methodology Manual). Es una metodología para evaluar la seguridad operacional de ubicaciones físicas, las interacciones humanas, todas las formas de comunicaciones tales como la inalámbrica, por cable, analógico y

digital. Esta metodología es una medida exacta de la seguridad a nivel operativo, diseñada para ser consistente y repetible (Herzog, 2010).

Pretende ser una metodología científica para la caracterización precisa de la seguridad operativa (OPSEC – Operational Security) a través de pruebas y la correlación de los resultados de una manera confiable.

El proyecto es mantenido por el Institute for Security and Open Methodologies (ISECOM), creado por Pete Herzog, 18 de diciembre de 2000.

- CHECK (Computer IT Health Check Service). Está metodología tiene por objetivo identificar las vulnerabilidades en los sistemas informáticos y en las redes que pueden comprometer la confidencialidad, integridad o disponibilidad de la información en ese sistema informático. Fue definida por el CESG (Communications-Electronics Security Group), qué es una autoridad gubernamental Británica, y es muy utilizada en el Reino Unido (Check, 2011).
- OWASP (Open Web Application Security Project). El Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP), es una comunidad abierta dedicada a permitir a las organizaciones realizar el desarrollo, adquisición y mantenimiento de aplicaciones Web fiables. Todas las herramientas, documentos, foros y delegaciones del OWASP son libres y abiertas a cualquiera interesado en mejorar la seguridad de las aplicaciones Web (OWASP, 2008).
- ISSAF (Information System Security Assessment Framework). El Marco de Evaluación de Seguridad de Sistemas de Información es una metodología estructurada de análisis de seguridad en varios dominios y detalles específicos de pruebas para cada uno de estos. Su objetivo es proporcionar procedimientos muy detallados para la realización de pruebas de seguridad de sistemas de información que

reflejan situaciones reales. Esta metodología es soportada por OSSIG (Open Information Systems Security Group) (OISSG, 2010).

- NIST SP800-115 (National Institute of Standards and Technology). NIST es responsable de normas y guías para las agencias federales de los Estados Unidos para proporcionarles una adecuada seguridad de la información para sus operaciones y activos. El documento que provee la guía para las organizaciones en la planificación, la realización y análisis de las pruebas de seguridad, así como el desarrollo de estrategias de mitigación, es el NIST SP800-115, que sustituye al NIST SP800-42 (Scarfone, 2008).

1.5 Conclusiones del capítulo 1

Tradicionalmente los tipos de pruebas de penetración son clasificados en caja negra, caja blanca y caja gris. En este trabajo se presenta la clasificación de tipos de pruebas de OSSTMM, debido a que es más completa y cubre de mejor manera las necesidades y requerimientos de las organizaciones.

Las metodologías de código abierto generalmente no tienen ninguna inclinación o preferencia por el uso de determinadas herramientas debido a que no tienen compromisos comerciales. En este trabajo serán mencionados ambos tipos de herramientas.

En el siguiente capítulo es analizado las metodologías del NIST SP800-115, EC-Council LPT y OSSTMM, de igual forma son mencionadas las herramientas que recomiendan utilizar para llevar a cabo a cada una de sus etapas, abarcan tanto herramientas de código abierto así como propietarias.

Capítulo 2

Estudio de las metodologías de Pruebas de Penetración (NIST SP800-115, EC-Council LPT y OSSTMM)

En este capítulo es realizado el estudio granular de cada una de las metodologías de Pruebas de Penetración (NIST SP800-115, EC-Council LPT y OSSTMM), a través de diagramas de flujos y tablas, también son especificados los elementos necesarios para llevarlas a cabo y la forma sistemática en que deben desarrollarse.

2.1 NIST SP800-115 Technical Guide to Information Security Testing and Assessment

La metodología propuesta por el NIST, tiene como finalidad proporciona recomendaciones a las agencias federales de Estados Unidos de cómo realizar de forma adecuada una prueba de penetración.

2.1.1 Fases de la Prueba de Penetración

El NIST, en su Special Publication 800-115, divide una prueba de penetración en 4 fases: planificación, descubrimiento, ataque y reporte.

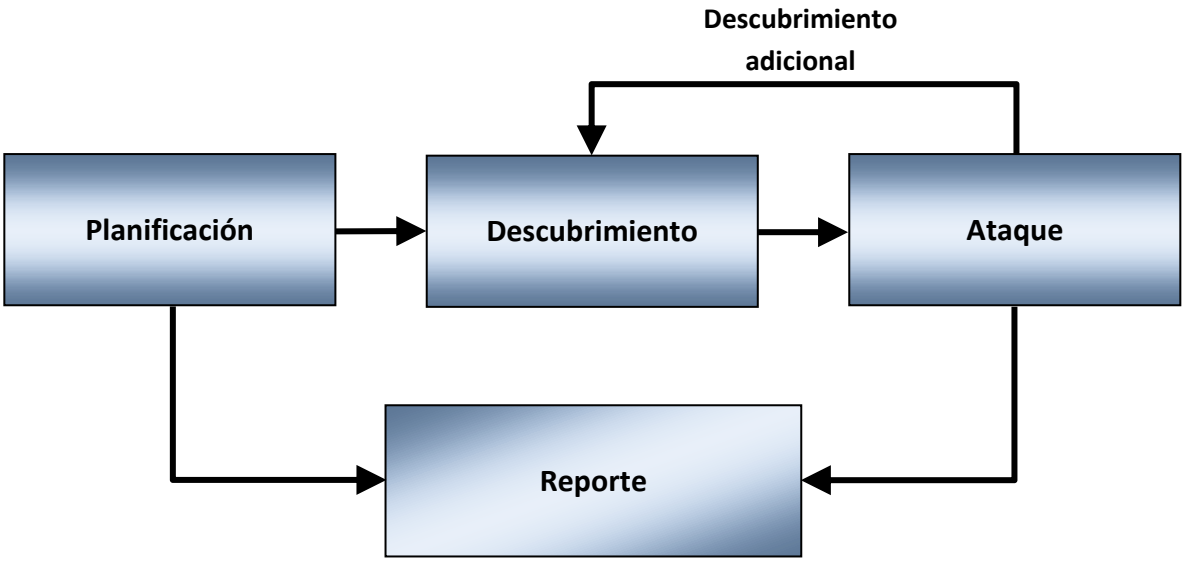

Figura 2 Las 4 fases de la Metodología de la Prueba de Penetración del NIST SP 800-115.(obtenido del NIST SP800-115)

2.1.2 Fase de Planificación

En la fase de planificación consiste en establecer los objetivos y las reglas de la prueba de penetración, para encaminar todo el proceso hacia un resultado satisfactorio para la empresa en cuestión.

Las actividades que son necesarias para elaborar un plan para la administración del proyecto se muestran a continuación.

- Determinar las necesidades y requerimientos que deben cumplir la evaluación de la seguridad de la organización.
- Definir el alcance de las pruebas. Establecer los límites de la prueba en términos de acciones y de los resultados esperados.
- Se debe identificar los riesgos inherentes en la realización de la prueba de penetración, así como las técnicas y medidas de mitigación que serán utilizados por el pentester.
- Definir el personal que conformará al equipo de la prueba de penetración, así como el personal clave de la organización responsable de los activos que serán probados. También se debe incluir los distintos medios para contactarlos, en dado caso que sea necesario.
- Establecer la programación de las pruebas, la cual debe de incluir las pruebas críticas y sus etapas. También se deben abordar los horarios en que se llevarán a cabo.
- Determinar los lugares autorizados para realizar la prueba de penetración. Si las pruebas se realizarán dentro de la organización, es necesario determinar el procedimiento para el acceso físico del pentester, así como de los equipos para realizar las pruebas, respetando las políticas de acceso a las instalaciones de la empresa.
- Determinar el nivel de acceso (usuario o administrador) a los sistemas y/o red.
- En caso de que aplique, indicar la dirección IP desde donde la cual ser harán las pruebas de forma remota.
- Especificar el hardware y software, que el equipo de pentesters utilizará para realizar las pruebas.

- Determinar la frecuencia y los métodos de comunicación con respecto a los avances e incidentes ocurridos durante el proceso de la prueba de penetración.
- Definir los criterios y procedimientos a realizar en caso de que una de las pruebas tenga un impacto negativo en la red o que un ataque se presente durante la prueba en marcha.
- Determinar los sistemas y/o redes que se probará durante todo el proceso de pruebas. También es importante establecer una lista de exclusión.
- Detallar las actividades permitidas y no permitidas, además debe incluir una descripción de la metodología de la prueba de penetración que se va a utilizar.
- En dado caso que se pretenda realizar algún tipo de entrevista (ingeniería social), se debe proporcionar las preguntas y deben de ser aprobadas por la alta gerencia antes de ser aplicadas.
- Establecer la forma en que será la recolección, almacenamiento, transmisión y destrucción de los datos generados como resultado de las pruebas.
- Establecer los requisitos de la presentación y el informe de los resultados que se esperan durante y finalización de las pruebas. Especificar la información mínima que debe contener cada reporte (por ejemplo, las vulnerabilidades y las técnicas recomendadas de mitigación).

Los detalles importantes deben ser especificados para asegurarse que todas las partes son conscientes de lo que está autorizado y que se espera como resultado de la prueba de penetración.

Todo lo antes mencionado, es necesarios plasmarlo en un documento de carácter legal, en el cual se están respaldando la empresa en cuestión y el equipo de pentesters.

2.1.3 Fase de descubrimiento

La fase de descubrimiento en esta metodología consta de dos partes. La primera parte consiste en la recopilación de información y la realización de escaneos; la segunda parte consiste en realizar un análisis de vulnerabilidades.

2.1.3.1 Primera parte: Recopilación de información

Es recomendable obtener información relacionada con el Hostname y la dirección IP puede ser obtenida a través de varios métodos, incluidos preguntas al DNS, realizar queries en InterNIC (WHOIS) y realizando sniffing a la red.

Los nombres de los empleados e información para contactarlos se puede obtener mediante la búsqueda en la página web de la organización o servidores de directorio.

En algunos casos, se puede utilizar técnicas como dumpster diving (búsqueda de información en la basura desechada por parte de la organización) y/o con un recorrido por el área de trabajo de los usuarios en búsqueda de información, en el cual podría encontrar contraseñas escritas en un papel.

Dentro de las actividades para la recolección de información están las siguientes:

- Descubrimiento en la red. Se realiza con el propósito de descubrir los equipos activos en la red. Existen dos tipos de escaneos: el pasivo y el activo. **El escaneo pasivo** consiste en utilizar un sniffer de red, para realizar el monitoreo de los equipos que están en la red. Este escaneo requiere de más tiempo para obtener la información de los equipos. Este tipo de técnica se aplica de forma interna en donde es posible

monitorear la red. **El escaneo activo** consiste en enviar al objetivo diferentes tipos de paquetes y dependiendo del comportamiento del equipo a tráficos ya sea normal, anormal y/o ilegal, es posible determina qué tipo de sistema operativo se trata. El escaneo activo requiere de menos tiempo para obtener la información pero es más propensa que sea detectado.

- Identificación de puertos y servicios de red. Para identificar los servicios y los puertos de red se utilizan un port scan. A través de los puertos abiertos de un equipo es posible identificar el tipo de sistema operativo, proceso llamado *OS fingerprint.* Para identificar la versión de la aplicación, se utiliza el llamado *banner grabbing*, el cual consiste en capturar la información transmitida por el banner cuando es iniciada una conexión.

Al final de este proceso se pretende tener una relación de los equipos activos en la red, así como los puertos que tiene abiertos.

2.1.3.2 Segunda parte: Análisis de Vulnerabilidades

El análisis las vulnerabilidades consiste en comparar los servicios, aplicaciones y sistemas operativos de los hosts escaneados contra una base de datos de vulnerabilidades.

El escaneo de vulnerabilidades ayuda a identificar versiones obsoletas de software, parches no instalados, malas configuraciones y validar el cumplimiento de las políticas de la organización.

Al disponer con el conocimiento de las vulnerabilidades de los sistemas de la organización, es posible definir la estrategia para realizar la prueba de penetración a los equipos de la red.

2.1.4 Fase de Ataque

En la fase de ataque, a partir de las vulnerabilidades identificadas previamente, el pentester trata de aprender más acerca de la red específica y aprovechar las vulnerabilidades identificadas. Algunos exploits permiten al pentester elevar privilegios en el sistema o en la red para acceder recursos adicionales. Es recomendable navegar por el sistema en búsqueda de más información, lo cual realizamos un descubrimiento adicional en busca de más vulnerabilidades.

Si el pentester es capaz de explotar una vulnerabilidad, puede instalar más herramientas en el sistema para obtener información y/o acceso adicionales, para determinar el nivel de acceso que un atacante podría adquirir. Después de adquirir el acceso es necesario cubrir las huellas con el uso de rootkits y la eliminación de logs que registren nuestra actividad.

Las vulnerabilidades que podrían ser explotadas pueden caer en cualquiera de las siguientes categorías:

- Errores de configuración.
- Errores del kernel.
- Código propenso a ataques de Buffer Overflows.
- Insuficiente validación posibles entradas que puede recibir una aplicación.
- Enlaces simbólicos.
- Ataques de descriptor de archivos.
- Race conditions. Puede ocurrir durante el tiempo que un programa o proceso ha entrado en modo privilegio. Un usuario puede aprovechar los privilegios elevados mientras el programa o proceso está todavía en modo progreso.
- Incorrecta asignación de permisos a archivos y directorios.

Al finalizar la fase de ataque, es necesario eliminar los archivos creados y la desinstalar las herramientas utilizadas durante las pruebas, las vulnerabilidades encontradas serán corregidas por parte del personal de la organización a partir del reporte generado por parte del equipo de pentesters.

2.1.5 Fase de Reporte

En la fase de reporte, se describe las vulnerabilidades identificadas, se indica el proceso utilizado para la explotación de las mismas y finalmente se proporciona una guía de cómo mitigar las debilidades encontradas.

2.1.6 Síntesis de la Metodología del NIST SP800-115

La metodología del NIST consiste en 4 fases:

Planificación. Se establecen los objetivos y reglas para realizar las pruebas de penetración.

Descubrimiento. Se divide en dos partes:

- Recopilación de información. Obtener información relacionada con el dominio y la IP de la organización, realizar sniffing a la red, utilizar la técnica de dumpster diving, escaneos pasivos y activos, aplicar técnicas de OS fingerprint y Banner grabbing.
- Análisis de vulnerabilidades.

Ataque. Consiste en explotar las vulnerabilidades encontradas, conseguir el acceso a la red y a los sistemas, la elevación de privilegios y cubrir las huellas de lo previamente realizado. Sí la situación lo amerita regresamos a la fase de descubrimiento. Al final de esta fase es restablecida la red y los sistemas a su estado original, a como se encontraba hasta antes de las pruebas.

Reporte. Es la entrega del informe de los resultados obtenidos de las pruebas de penetración.

El NIST recomienda utilizar como herramienta BackTrack durante las pruebas, además hace mención como buena alternativa la metodología de OSSTMM.

2.2 EC-Council Licensed Penetration Tester (LPT)

Para aplicar la metodología de EC-Council es necesario primero cumplir con una serie prerrequisitos, en los cuales son establecidas las reglas de cómo se va a realizar la prueba de penetración.

La metodología, en la parte de pruebas, consta de veintiséis módulos, en los cuales indican las actividades a realizar de forma secuencial y precisa de cómo realizar las pruebas y qué herramientas utilizar.

2.2.1 Pre-requisitos para iniciar una Prueba de Penetración de acuerdo al EC-Council LPT

Estas son las actividades necesarias a realizar antes iniciar cualquier prueba de penetración en forma, desde el punto de vista de EC-Council:

1. Recopilar información sobre la organización, incluyendo su historia.
    - Objetivos de la organización.
    - Productos y/o servicios proporcionados por la organización.
    - Activos de la organización.
    - Información acerca de los empleados.

- Tipos de clientes y partners de negocios.

2. Visitar las instalaciones de la organización en cuestión para familiarizarse con el entorno e instalaciones.

  - Verificar el acceso a las instalaciones de la organización, así como al site de servidores

3. Lista de requisitos y necesidades de la organización que la prueba de penetración debe cumplir.

4. Obtener el permiso para realizar la prueba de penetración de la Alta Gerencia de la organización.

5. De acuerdo a las necesidades de la organización, determinar los tipos de pruebas a realizar y los servicios que serán revisados.

6. Identificar el espacio asignado de oficina para que el equipo de pentesters trabaje durante la duración del proyecto. Debe tener acceso restringido a los empleados o clientes de la organización.

7. Obtener Tarjetas de Identificación temporal para el acceso a la organización del equipo de pentesters, así como del equipo necesario para el desarrollo de las pruebas, de acuerdo con las políticas de acceso físico por parte de la organización.

8. Especificar las reglas de la forma a realizar la prueba de penetración así como indicar las limitaciones y líneas de tiempo. Es necesario indicar los tipos de ataques a realizar, a que servidores y los horarios y tiempos de duración para ejecutarlos.

9. Preparar el documento legal de la prueba de penetración, en la cual se indique las reglas, las condiciones y aspectos legales de las pruebas que se pretenden realizar, el cual debe ser examinado por el

abogado contratado. También es necesario especificar hasta donde llegan las obligaciones y limitaciones del pentester, es decir, definir puntualmente los alcances del proyecto.

10. Preparar el contrato de Confidencialidad.

11. Si es posible, obtener un seguro de responsabilidad de una empresa de seguros. Para protegerse en caso de provocar un daño no intencionado a cualquiera de los activos informáticos de la organización durante la prueba de penetración.

12. Preparar el equipo humano para realizar la prueba de penetración.

- Jefe del equipo de las Pruebas de Penetración.
- Experto en Base de Datos y aplicaciones Web.
- Experto en Redes.
- Hacker Ético.
- Analista de Datos.
- Encargado de documentar las pruebas realizadas.

13. Lista de las herramientas de seguridad que se van a utilizar para el proyecto de la prueba de penetración.

14. Identificar los requisitos de cumplimiento de seguridad del cliente.

15. Enumerar los servidores, computadoras de escritorio y dispositivos de red que necesitan ser probados.

16. Identificar el tipo de pruebas que se llevarán a cabo. Ya sea que se trate de pruebas de Caja Negra, de Caja Blanca ó Caja Gris, además de pruebas anunciadas ó sin previo aviso.

17. Realizar una relación de los administradores de los principales activos de la organización, con sus respectivos datos, para contactarlos en caso de ser necesario:

18. Si es posible, identificar al encargado de seguridad física de la organización en caso de presentarse una emergencia, tales como un incendio, fallas eléctricas, etc.

19. Lista de las pruebas que no se realizarán en la red de la organización.

20. En caso que se requiera realizar una prueba desde Internet que sea considerada como prohibida o como un delito informático, solicitar un permiso especial para el cumplimiento de la ley.

21. Especificar la línea de tiempo para el proyecto de la prueba de penetración.

- Etapas del proyecto con los tiempos de duración.
- Fecha de la terminación del proyecto.
- Entrega y presentación de resultados.

2.2.2 Roadmap de las Prueba de Penetración de EC-Council LPT

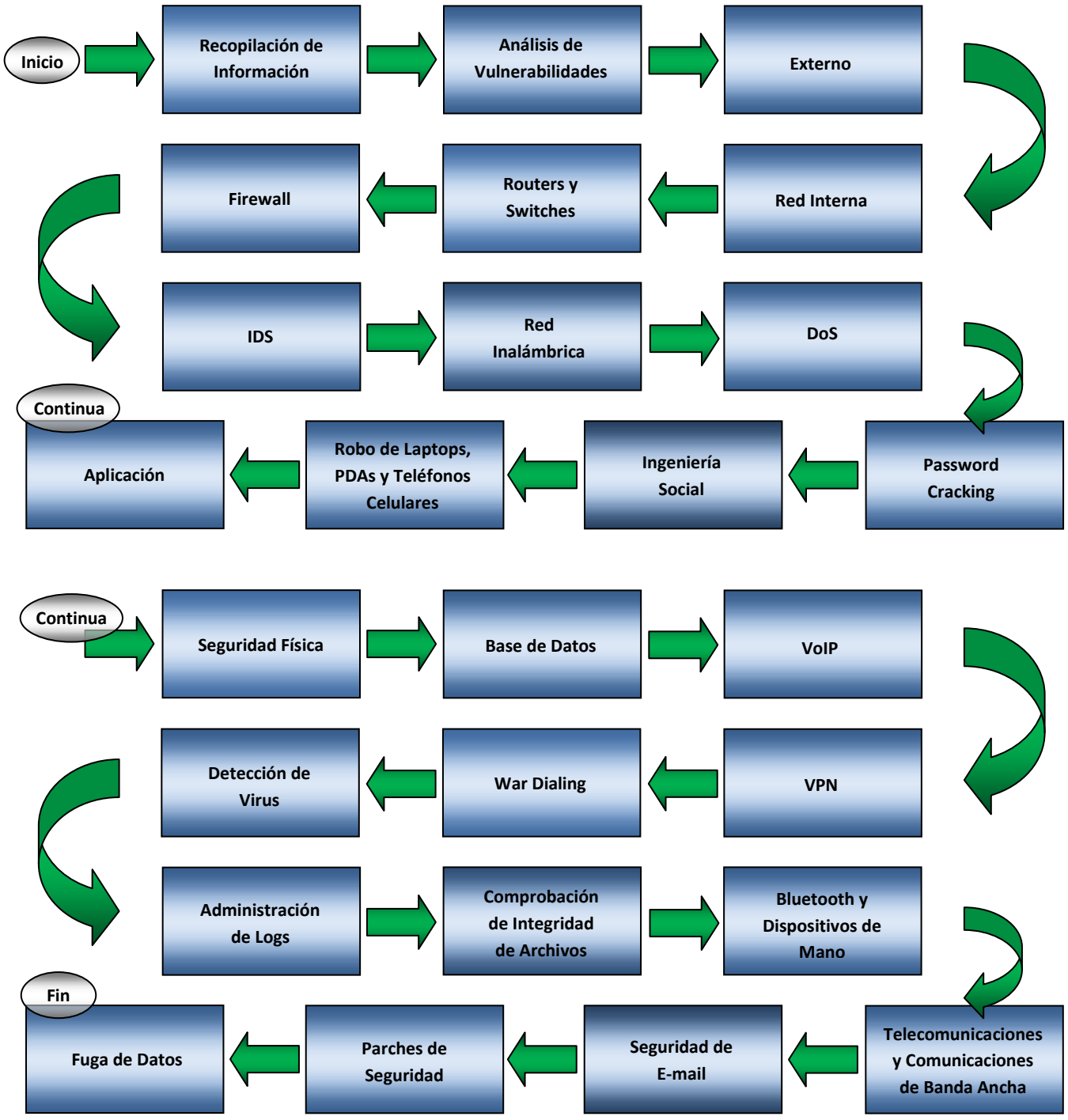

Figura 3 Trayectoria de la metodología para pruebas de penetración de EC-Council LPT. (Obtenido del manual EC-Council LPT)

2.2.3 Recopilación de Información

1. Buscar el sitio Web y replicarlo en un equipo de pruebas.
   Herramientas: HTTrack, Webcrawl, cURL and Libcurl, W3mir, Web Copier, Folder Synchronization tolos, FileDog, BlackWindow.
2. Buscar el sitio FTP y replicarlo las páginas en un equipo de pruebas.
   Herramientas: Ftpcopy, Ftp Mirror Manager, Get Right, Ftp Mirror Tracker, Auto FTP Manager.
3. Buscar información referente al registro del dominio en Internet, el propietario y los contactos de administración.
   Herramientas: WHOIS, Sam Spade, Whois.net, WhereisIP, Lockbox, ActiveWhois.
4. Listar los productos que vende la organización.
   - Visitar el sitio Web de la organización.
   - Solicitar un catálogo del producto.
   - Solicitar un producto por email.
   - Solicitar un descuento, si es aplicable.
   - Solicitar una lista de sus distribuidores y de sus canales de venta al por menor.
   - Solicitar el contacto internacional para sus productos.
5. Listar la información del contacto, direcciones de email y sus números telefónicos. Realizar llamadas telefónicas a la organización y preguntarle a la recepcionista por personas en las siguientes áreas: ventas, marketing, servicio al cliente, gerencia, soporte técnico y producción.
6. Enlistar los distribuidores de la organización.
7. Enlistar los socios de la organización.
8. Buscar en Internet, grupos de noticias, anuncios y sitios web información negativa sobre la organización.
9. Búsqueda de directorios de asociaciones comerciales.

10. Comparar el precio del producto o servicio del competidor de la organización.
11. Encontrar la localización geográfica de la organización.
    - maps.google.com.mx/
    - www.WindowLiveLocal.com
    - www.Wikimapia.com
    - www.Palacepedia.com
12. Buscar listados de nombres de dominio similares al de la organización.
    - www.mydomainfriend.com
13. Buscar en sitios de trabajo anuncios de parte de la organización. Revisar si están solicitando administradores de sistema, operadores de base de datos y /o administradores de seguridad.
14. Revisar la información acerca de la organización en redes sociales.
15. Listado de los empleados clave de la organización.
    - Listar a todos los empleados de la organización.
    - Anunciarse como cliente y solicitar una presentación.
    - Después, contactar a diferentes personas a través de ingeniería social.
    - Buscar información de los contactos y las extensiones telefónicas.
16. Investigar al personal clave, buscar en google información acerca de sus vidas, es muy útil para utilizar ingeniería social.
17. Realizar una relación de los empleados de la organización con su dirección de email personal.
18. Visitar a la organización como investigador y extraer información privilegiada. Determinar que tan fácil es el acceso a las instalaciones de la empresa, los horarios de trabajo.
19. Visitar la localidad de la organización. Para obtener información de otras fuentes como:
    - Personal auxiliar.

- Agentes que le proveen un servicio al personal de la empresa.
- Vecinos comerciantes, proveedores y vendedores ambulantes.

20. Buscar en eBay la presencia de la organización.
    www.ebay.com/
21. Utilizar una herramienta de investigación de dominio para obtener información referente de la organización. www.domainresearchtool.com
22. Obtener el registro DNS de la organización de sus servidores disponibles.
    www.DNSstuff.com
23. Utilizar GHDB (Google Hacking Database) y buscar el nombre de la organización. El GHDB es una base de datos de consultas utilizadas por los hackers para identificar datos sensibles en un sitio web, tales como páginas de inicio de sesión del portal, los registros con la información de seguridad de la red, etc.

2.2.4 Análisis de Vulnerabilidades

El proceso de análisis de vulnerabilidades implica reconocer, medir y priorizar las vulnerabilidades de un sistema.

A continuación se indica el procedimiento para un análisis de vulnerabilidades:

- Comprobar si el equipo está activo.
- Escanear puertos.
- Identificar las vulnerabilidades potenciales y generar un reporte.
- Clasificar las vulnerabilidades y determinar un plan de acciones para su mitigación.

- Clasificar y priorizar los activos de la empresa e iniciar la gestión de riesgos.
- Documentar las acciones realizadas y generar un informe de los resultados.
- Iniciar un proceso continuo de seguridad.

2.2.4.1 Clasificación de vulnerabilidades

- Errores de configuraciones.
- Instalaciones por defecto.
- Buffer overflows.
- Servidores sin parches.
- Contraseñas por defecto.
- Servicios abiertos.
- Fallas en las aplicaciones.
- Fallas en los Sistemas Operativos.
- Fallas en los Diseños.

El análisis de Vulnerabilidades es un examen para identificar las debilidades de un sistema o aplicación que podrían ser aprovechadas por un atacante. De igual forma es puesta a prueba la efectividad de los procedimientos y los controles de seguridad ante posibles ataques.

2.2.4.2 Herramientas para el Análisis de Vulnerabilidades

- QUALYS Scanner
- Cycorp Cycsecure Scanner
- eEye Retina Network Security Scanner
- Foundstone Professional Scanner
- GFI LANguard Network Security Scanner
- ISS Internet Scanner

- Saint Vulnerability Scanner
- Symantec Netrecon Scanner
- Shadow Security Scanner
- Open Source Nessus

Antes de utilizar cualquier herramienta, es importante comprender su funcionamiento, que este actualizado y haberlo probado en un ambiente de laboratorio. El análisis de vulnerabilidades se debe realizar de forma periódica.

2.2.5 Prueba de Penetración Externa

El análisis y las pruebas de intrusión externa validan las fortalezas y debilidades de la organización de forma interna y externamente a través de Internet.

Pasos para realizar una Prueba de Penetración Externa

1. Realizar un inventario de la infraestructura externa de la organización.
2. Crear la topología de la red.
3. Identificar las direcciones IP de los elementos de la organización (Página Web, Servidor de correo, Servidor DNS, etc.). Herramientas: NeoTrace, IP Prober.
4. Identificar la trayectoria del tráfico TCP/UDP hacia los servicios de la organización. Herramientas: IGI, Pathchirp, Pathrate, Pathload, Tulip, Scriptroute, Netperf.
5. Identificar la localización física de los servidores. Herramienta: NeoTrace.
6. Validar el uso de IPv6. Herramienta: 46Bouncer.
7. Buscar información acerca del registro de dominio de la organización. Herramientas: All-Nettools.com, DNSstuff, Whois search.

8. Buscar la dirección IP de la organización en listas negras en Internet. Herramientas: SAM SPADE, ARIN DATABASE.
9. Identificar el ISP de la organización.
10. Listar los puertos abiertos y cerrados de los servicios externos de la organizació. Herramientas: Superscan, Nmap, Firewalk, Hackershield, Hostscan, Internet Scanner, Nessus, Netcat, Netcop, Netscan Tools, Vulnerability Scanning: SAINT, SATAN, SARA (Security Auditor's Research Assistant), Strobe, Super Scan/Fscan, Twwwscan, Whisker, Winscan.
11. Listar los puertos sospechosos que se muestren en estado half open/close.
12. Escanear todos los puertos (65,536) de los servicios disponibles desde Internet.
13. Utilizar el SYN scan hacia los equipos y observar su comportamiento (puertos abierto, cerrados o filtrados). Los puertos en estado filtrado son reconocidos por el error inalcanzable ICMP de tipo 3, código 1, 2, 3, 9, 10 ó 13.
14. Utilizar el XMAS scan hacia los equipos y observar su respuesta. La herramienta envía paquetes TCP con las banderas activas de FIN, URG y PSH, si no obtenemos ninguna respuesta de parte del equipo, el puerto está abierto, si el equipo remoto contesta con RST/ACK, el puerto está cerrado.
15. Utilizar el FIN scan hacia los equipos y observar su respuesta.
16. Utilizar el NULL scan hacia los equipos y observar su respuesta.
17. Utilizar el método de Firewalk sobre el router que conforma el Gateway de la organización en cuestión y de los resultados de las pruebas suponer la ACL en el router.
18. Validar la predicción del número de secuencia de los paquetes TCP. Herramienta: Nmap.
19. Validar el uso de protocolos estándar y no estándar.

20. Identificar el sistema operativo en cada uno de los equipos de la organización. Herramientas: Nmap, Telnet, Netcat, Netcraft, OS fingerprinting tool.
21. Validar la aplicación de parches al sistema operativo de los equipos. Herramienta: Nessus.
22. Ubicar la localización del registro de DNS e intentar aplicar DNS hijacking.
23. Descarga las aplicaciones del sitio Web de la organización y aplicar ingeniería inversa al código binario. Herramientas: IDA PRO Java Engineer, FlashSaver, REC Decompiler.
24. Aplicar distintos URL strings al sitio Web de la organización y analizar las diferentes respuestas.
25. Examinar las cookies generadas por el servidor.
26. Examinar el control de acceso utilizado en la aplicación Web (formas de autenticación, Windows Authentication, Biometrics Authentication, Secret question authentication, Session based authentication, Digital certificates, Microsoft single-sign on).
27. Aplicar ataques de fuerza bruta de inyecciones URL y session tokens a los sitios web de la organización. Los strings son inyectados en varios campos de la URL, los cuales pueden ser: sessions, forms, User, ID, Login, Access, etc.
28. Buscar información sensible en el código fuente del sitio Web (Web Authors, Developer Information, User Comments, Login information, Temp Variables, Revision Numbers, Project deadline, Dates).
29. Intentar URL encoding sobre los sitios web.
30. Intentar ataques de buffer overflow en los campos de entrada. Herramientas: Ntomax, Hailstorm.
31. Intentar técnicas de Cross-site scripting (XSS).
32. Grabar y reproducir el tráfico hacia el sitio Web y analizar el tipo de respuesta. Herramientas: Cruise Control, Web LOAD, E-Test Suite.

33. Intentar varias técnicas de SQL injection.
34. Examinar los campos ocultos (Price, Username, Password, Session, URL characters, Special instructors).
35. Analizar los mensajes de bienvenida, mensajes de error y mensajes de depuraciones.
36. Aplicar Banner grabbing a los servidores Web, E-mail, POP3, FTP, etc. Herramientas: httprint, GNIT NT, Netcat.

2.2.6 Prueba de Penetración a la Red Interna

1. Mapear la red interna para identificar el número de subredes, el número de equipos y los sistemas operativos que se está ejecutando en cada equipo.
2. Escanear los equipos activos de la red interna. Herramientas: Angry IP, Network Scanner.
3. Escanear de forma individual a los equipos, tratando de identificar puertos vulnerables como 80, 21, 139, 137 y 145.
4. Tratar de obtener acceso explotando vulnerabilidades conocidas en los equipos utilizando herramientas de hacking para comprometerlos. Herramientas: Nessus, Retina, GFI LANguard NSS.
5. Intentar establecer null sessions en los equipos.
   C:\>net use \\192.168.6.8\IPC$ “” /u:””
6. Enumerar usuarios e identificar dominios en la red.
   Herramientas: GetAcct, Winfingerprint. Ej. C:\Net View /domain
7. Realizar sniffing a la red. Herramientas: Wireshark, Tcpdump, Etherpeek.
8. Realizar sniffing a las contraseñas de POP3, FTP y Telnet. Herramientas: Dsniff, Password Sniffer.
9. Realizar sniffing a los mensajes de email. Herramienta: Mailsnarf.

10. Realizar ataques reproduciendo los LM Manager Hashes para utilizar la contraseña obtenida en los equipos. Herramientas: LOphtcrack, Win Proxy tool.
11. Intentar ARP poisoning y MAC Flooding a los switches de la red. Herramienta: Arpspoof, Arpoison, Ettercap, Parasite, Macof.
12. Intentar el ataque man-in-the-middle (MITM). Herramientas: Ettercap, Cain&Abel.
13. Intentar DNS Poisoning. Herramientas: DNSA, Dnsspoof, TinyDNS, DNSCache.
14. Intentar ingresar a las consolas de los equipos, utilizando las contraseñas por default.
15. Iniciar los equipos utilizando un Live CD (Knoppix) para robar el archivo SAM.
16. Tratar instalar keylogger en los equipos para robar contraseñas. Herramientas: Instant Password Finder, Realtime-Spy, Spy Agent, Elite Remote Keylogger.
17. Tratar instalar keylogger en hardware en los equipos para robar contraseñas.
18. Intentar instalar un spyware en los equipos, para monitorear la información del usuario hacia Internet.
19. Intentar instalar un Troyano en los equipos, para instalar herramientas adicionales. Herramientas: Beast, Netcat.
20. Intentar crear una cuenta de usuario con privilegios, sin el conocimiento de los usuarios.
21. Tratar de realizar un bypass del antivirus instalado en los equipos.
22. Tratar de propagar un virus utilizando los equipos de la red.
23. Intentar instalar Rootkits en los equipos.
24. Ocultar datos sensibles en los equipos, tales como códigos fuente fotos, documentos en Word, hojas de cálculo.

25. Ocultar herramientas de hacking en los equipos. Herramientas: AB Hide Folder, Stealth Folder Hider, Folder Security Personal.
26. Utilizar varias técnicas de esteganografía para ocultar archivos en los equipos. Herramientas: Image Hide, Snow.
27. Intentar escalar los privilegios al usuario de actual nivel a uno de administración.
28. Capturar tráfico POP3, SMTP, IMAP, FTP, RDP, VoIP.
29. Capturar tráfico HTTP y HTTPS. Herramientas: HTTP Analyzer utility, EffeTech HTTP Sniffer.
30. Realizar spoof de MAC address.
31. Intentar session hijacking sobre tráfico de Telnet, FTP y HTTP.

2.2.7 Pruebas de Penetración a Switches y Routers

Pasos para realizar pruebas de penetración a routers:

1. Identificar el hostname del router. Herramientas: Nslookup, Dig, Host.
2. Escanear los puertos del router.
3. Identificar el sistema operativo del router y su versión. Herramienta: Nmap.
4. Identificar los protocolos que se están ejecutando en el router.
5. Intentar el robo de paquetes del router.
6. Validar sí el router tiene una mala configuración. Herramienta: RATS (Rough Auditing Tool for Security).
7. Evaluar las conexiones VTY/TTY. Las conexiones VTY/TTY son utilizadas para conectarse directamente al router, para lo cual es necesario tener acceso físico.
8. Evaluar los modos de ejecución del router. Validar que los modos usuario y privilegiado tengan configurada una contraseña.
9. Evaluar la configuración SNMP en el router.

10. Evaluar la conexión TFTP.
11. Validar sí el servicio de Finger se está ejecutando en el router.
12. Validar sí el Cisco Discovery Protocol (CDP) se está ejecutando en el router.
13. Evaluar el protocolo NTP.
14. Evaluar el acceso al router a través del puerto de consola. Solo es posible sí se tiene acceso físico al router.
15. Utilizar las técnicas loose and strict source routing. Source routing es utilizado para mapear la red, solucionar problemas, validar el rendimiento de la red y como técnica de hacking, consiste en definir la trayectoria que debe tomar el paquete de datos para viajar a través de la red.
16. Intentar IP spoofing.
17. Evaluar el manejo de errores IP. Utilizando ICMP redirect para obtener la mejor ruta para alcanzar un determinado destino.
18. Probar ataques ARP. Herramientas: Ettercap, arpsoof.
19. Evaluar RIP. Herramientas: Lophtcrack, Jonh the Ripper.
20. Evaluar el protocolo OSPF, a través de ataques de fuerza bruta.
21. Evaluar el protocolo BGP, a través de ataques predicción de números de secuencias TCP. Herramientas: Hunt, T-sight.
22. Evaluar el protocolo EIGRP, a través de ataques de fuerza bruta y diccionario.
23. Evaluar el ataque de DoS en el router, a través de ataques de paquetes malformados e inundación de paquetes.
24. Evaluar el acceso http del router.
25. Evaluar a través del ataque HSRP (Hot Standby Routing Protocol).

Pasos para realizar pruebas de penetración switches:

1. Evaluar el tamaño del cache de direcciones. Herramientas: IxScriptMate.

2. Evaluar la integridad de datos y la corrección de errores. Verificar si el switch envía estos paquetes malformados.
3. Evaluar el valor back-to-back del switch, para determinar el tamaño más grande de las tramas que puede manejar el switch.
4. Evaluar la pérdida de tramas.
5. Evaluar la latencia.
6. Evaluar el rendimiento del switch.
7. Evaluar el filtrado de tramas mal formados, tales como tramas de gran tamaño, tramas con errores de CRC, fragmentación de tramas. Herramienta: IxScriptMate.
8. Evaluar el Fully Meshed, consiste en determinar el total de tramas que puede manejar el switch cuando recibe tramas en todos los puertos.
9. Evaluar la funcionalidad de QoS (Quality of Service).
10. Evaluar el rendimiento del protocolo Spanning Tree en la red.
11. Evaluar el rendimiento del protocolo OSPF.
12. Evaluar el ataque VLAN hopping.
13. Evaluar la inundación de la tabla de MAC address. Herramienta: Macof.
14. Evaluar el ataque de ARP.
15. Evaluar el ataque VTP (VLAN Trunking Protocol).

2.2.8 Prueba de Penetración a Firewalls

Pasos para realizar una prueba de penetración a Firewalls:

1. Ubicar el firewall. Herramienta Hping.
2. Identificar el rango de la red. Herramienta: tracert.
3. Escanear los puertos del firewall. Herramienta: Nmap.
4. Identificar el tipo y la versión (grab the banner) del firewall. Herramienta: Netcat.

5. Enviar paquetes malformados y observar la respuesta del firewall. Herramienta: Hping.
6. Enumerar el control de acceso. Herramienta: Nmap.
7. Identificar la arquitectura del firewall. Herramienta: Hping.
8. Evaluar las políticas del firewall. Herramientas: Hping, firewalking.
9. Evaluar el firewall utilizando la herramienta firewalking.
10. Evaluar la redirección de puertos. Herramientas: Fpipe, Datapipe.
11. Evaluar el firewall de ambos lados. Utilizar el tunneling de protocolos, realizar escaneos de vulnerabilidades, utilización de paquetes fragmentados y spoofeados, utilizar firewalking y analizar la respuesta del firewall en cada uno de los casos, desde el exterior hacia la red interna y viceversa.
12. Evaluar al firewall abierto desde el exterior.
13. Probar los canales encubiertos.
14. Evaluar el firewall protegido desde el exterior.
15. Evaluar aplicar el HTTP tunneling. Herramientas: HTTPORT, HTTHOST.
16. Evaluar específicas vulnerabilidades del firewall. Aprovechar la mala configuración y/o la falta de parches instalados para comprometer al firewall.

2.2.9 Pruebas de Penetración a IDSs

Pasos para realizar una prueba de penetración a IDSs:

1. Intentar ataques de agotamiento de recursos. Validar si hay un momento en que se degrada el rendimiento del IDS.
2. Evaluar al IDS con ataques de ARP Flood.
3. Evaluar al IDS con ataques de MAC Spoofing.
4. Evaluar al IDS con ataques de IP Spoofing.

5. Evaluar con el envío de paquetes a direcciones Broadcast.
6. Evaluar con el envío de paquetes inconsistentes.
7. Evaluar con paquetes IP fragmentados.
8. Evaluar con fragmentos duplicados.
9. Evaluar con fragmentos traslapados.
10. Evaluar con el ping de la muerte.
11. Evaluar con paquetes de tamaños extraños.
12. Evaluar la evasión a través de la manipulación del TTL.
13. Evaluar el envío de paquetes al puerto 0.
14. Evaluar con el UDP Checksum.
15. Evaluar con retransmisiones de TCP.
16. Evaluar al IDS con la manipulación de las banderas de TCP.
17. Evaluar con las banderas de TCP.
18. Evaluar al IDS con el envío de SYN Floods.
19. Evaluar con la predicción inicial de número inicial de secuencia.
20. Evaluar con Backscatter. El término Backscatter representa la respuesta de paquetes SYN/ACK ante un ataque de inundación de SYNs.
21. Evaluar al IDS con paquetes ICMP.
22. Evaluar al IDS utilizando canales encubiertos.
23. Evaluar con TCPReplay. TCPReplay tiene la capacidad de reproducir un tráfico previamente capturado en un archivo de TCPdump.
24. Evaluar con TCPOpera. TCPOpera puede replicar tráfico con diferentes variaciones de un archivo TCPDump
25. Evaluar con Method Matching.
26. Evaluar al IDS con URL Encoding.
27. Evaluar al IDS con doble slashes.
28. Evaluar al IDS con Reverse Traversal.
29. Evaluar con referencia a directorios.
30. Evaluar con una prematura Request Ending.

31. Evaluar al IDS Parameter Hiding.
32. Evaluar con HTTP-Misformatting.
33. Evaluar con URLs largas.
34. Evaluar con DoS con sintaxis de directories de windows.
35. Evaluar con NULL Method Processing.
36. Evaluar con Case Sensitivity.
37. Evaluar Session Slicing.

Para cada uno de los ataques presentados, observar el comportamiento del IDS ante cada uno estos.

2.2.10 Prueba de Penetración a Redes Inalámbricas

Pasos para realizar una prueba de penetración a redes inalámbricas:

1. Descubrimiento de Access Points no autorizados.
2. Realizar sniffing el tráfico de las redes Wireless.
3. Evaluar el cifrado (WEP, WPA, WPA2 y EAP).
4. Intentar aplicar técnicas de cracking al Static WEP Keys.
5. Aplicar ataque de fuerza bruta.
6. Intentar aplicar el ataque de MAC Address Spoofing.
7. Saturar la señal de la red inalámbrica.
8. Intentar el ataque MITM.
9. Intentar generar mucho tráfico en pocos minutos para poder aplicar técnicas de Cracking al la clave de WEP.
10. Intentar inyectar paquetes cifrados hasta que sean aceptados por utilizar la clave correcta.
11. Intentar descifrar un solo paquete. Utilizar la herramienta “Called Chopchop” que descifrar un solo paquete sin la información de la clave WEP.

Herramientas: AiroPeek, AirSnort, Dstumbler, Dwepdump, ISS Wireless Scanner, Kismet, NetStumbler, Sniffer Wireless, WEPCrack, Aircrack-ng, KisMAC, MiniStumbler, AirMagnet, WirelessMon.

2.2.11 Denegación de Servicio (DoS)

Estos son los pasos para aplicar un DoS en una prueba de penetración:

1. Evaluar a los servidores con cargas pesadas. Esto se realiza incrementando la cantidad de peticiones hasta superar el límite que el servidor puede manejar.
   Herramientas: Web Applications Stress (WAS), Jmeter, Testload.
2. Verificar si los sistemas o dispositivos son vulnerables al DoS.
   Herramientas: NMAP, GFI LANguard.
3. Ejecutar el ataque de SYN en los servidores. Herramientas: Trinoo, Tribe Flood Network, TFN2K, Synful, Synk4
4. Ejecutar el ataque port flooding sobre los servidores. Herramientas: Mutilate, Pepsi5.
5. Ejecutar el ataque de fragmentación de IP en los servidores. Herramientas: Syndrop, Jolt2.
6. Ejecutar el ping de la muerte. Herramienta: ping.
7. Ejecutar el ataque teardrop. Herramientas: WinNuke. Ssping.
8. Ejecutar el ataque smurf (ping flooding o ICMP storm). Herramienta: Papasmurf.
9. Ejecutar un bombardeo de emails en los servidores de correo. Herramientas: Mail Bomber, Attache Bomber, Advanced Mail Bomber.
10. Inundar con información falsa las formas y los libros de visitas del sitio web.
11. Hacer pedidos grandes en el sitio web y cancelar antes de llegar a la pantalla de pago.

Herramientas: ISS Internet Scanner, Mercury Quick Test Professional, Flame Thrower Stress Testing Tool, Avalanche, Pylot, vPerformer, Curl-Loader, RealityLoad XF On-Demand Load Testing, StressTester, The Grinder, Proxy Sniffer, Funkload, Loadea, LoadManager, TestLOAD, NeoLoad, PowerProxy, webStress, HostedToolbox, Test Complete Enterprise, WebPartner Test and Performace Center, QTest, LoadDriver, Test Perspective Load Test, SiteTester1, httperf, NetworkTester, WAPT, Microsoft Application Center Test, ANTS, Apache JMeter, TestMaker, Webhammer, SiteStress, Siege, Jblitz, WebServer Stress Tool, Web Polygraph, OpenSTA, PureLoad, ApacheBench, Torture, WebSpray, eValid, WebPerformace Trainer, WebSuite, FORECAST, e-Load, http-Load, AQLoad, Portent Web Load test Tool, SilkPerformer, Radview's WebLoad, Loadrunner, Java Test Tools, WebInspect.

2.2.12 Password Cracking

Pasos para aplicar Password Carcking en pruebas de penetración:

1. Extraer los archivos /etc/passwd y /etc/shadow en los sistemas Linux.
2. Extraer el archivo C:\winnt\system32\etc\SAM en los sistemas Windows. Herramientas: SAMDUMP, PWDUMP y Lophtcrack.
3. Identificar el perfil del usuario del equipo. Obtener información personal del usuario.
4. Construir un diccionario con una lista de palabras, basada con la información recopilada del usuario del equipo previamente. Herramientas: Dictionary Maker, Pass List.
5. Intentar adivinar la contraseña.
6. Aplicar un ataque de fuerza bruta, utilizando la lista hecha previamente. Herramientas: Brutus, Lophtcrack y Munga Bunga, Password Cracker.

7. Utilizar herramientas automáticas de cracking para romper las contraseñas de los archivos protegidos. Herramientas: Brutus, Cerberus Internet Scanner, Crack, CyberCop Scanner, Inactive Account Scanner, Legion and NetBIOS Auditing Tool (NAT), LOphtcrack, John the Ripper, SAMDump, PWDump, PWDump2, PWDump3, SecurityAnalyst, TeeNet, WebCrack.

2.2.13 Ingeniería Social en una Prueba de Penetración

Pasos para conducir Ingeniería Social en una prueba de penetración:

1. Intentar técnicas de ingeniería social utilizando el teléfono.
2. Intentar ingeniería social vishing. Vishing es una combinación de phishing y tecnología de Voz sobre IP.
3. Intentar ingeniería social por e-mail.
4. Intentar ingeniería social utilizando el sistema tradicional de correo.
5. Intentar ingeniería social en persona.
6. Intentar ingeniería social utilizando dumpster diving.
7. Intentar ingeniería social con un cómplice con información privilegiada.
8. Intentar ingeniería social utilizando shoulder surfing. Shoulder surfing consiste en observar por encima de sus hombros el momento en que el usuario teclee su usuario y contraseña.
9. Intentar ingeniería social con la información en el escritorio del usuario.
10. Intentar ingeniería social por extorsión y chantaje.
11. Intentar ingeniería social utilizando el sitio web. Consiste en enviar un correo al usuario con el link de una página Web falsa, pero casi igual a la original.
12. Intentar el robo de identidad y ataques de phishing.

13. Tratar de obtener imágenes de satélite y planos del edificio. Ayuda a ubicar las puertas y ventanas del edificio.
14. Tratar de obtener detalles de los usuarios de sitios de redes sociales. Por ejemplo Orkut, Facebook, Hi5, Myspace.
15. Monitorear y capturar las conversaciones teléfonicas.
16. Utilizar video cámaras para capturar imágenes.
17. Utilizar sistemas de seguimiento para monitorear vehículos de motor. Pro Trak GPS, RF Scout GPS Tracking System.
18. Identificar a los empleados descontentos y entablar una conversación con ellos para extraerles información confidencial.

2.2.14 Robo de Laptops, PDAs y Teléfonos Celulares para una Prueba Penetración

Pasos para realizar una prueba de penetración a los dispositivos obtenidos:

1. Identificar los datos sensibles que tiene el dispositivo. Buscar en documentos en Word y en Excel, mensajes de e-mail, información referente a proyectos, etc.
2. Buscar contraseñas.
3. Buscar documentos relacionados con la infraestructura o finanzas de la compañía.
4. Extraer el directorio de direcciones y números telefónicos.
5. Extraer horarios y citas.
6. Extraer aplicaciones instaladas en ese dispositivo.
7. Extraer mensajes de e-mail de los dispositivos.
8. Obtener acceso a los recursos del servidor en base a la información extraída.
9. Intentar ingeniería social con la información extraída.

2.2.15 Pruebas de Penetración a Aplicaciones

Pasos para realizar pruebas de penetración a aplicaciones Web:

1. Aplicar técnicas de fingerprint al ambiente de la Aplicación Web.
2. Investigar las salidas de HEAD y de las solicitudes al OPTIONS Http.
3. Investigar los formatos y la redacción del código 404 y otros errores de la página web.
   Herramienta: ColdFusion.
4. Tratar de reconocer los tipos de archivos, extensiones y directorios.
   Extensiones: Active Server Page (.ASP), HTML page (.HTM), Program and/or Extension Format (.PHP), Executable File Format (.EXE).
5. Examinar la fuente de la página disponible, para determinar el tipo de aplicación sobre la cual está funcionando el sitio web.
6. Manipular las entradas para provocar un Scripting Error.
7. Evaluar el trabajo interno de una aplicación Web, para determinar sobre que lenguaje de programación fue realizado el sitio web.
8. Evaluar la conectividad con la Base de Datos. Verificar si la aplicación web tiene acceso al servidor de la Base de Datos con privilegios de administrador.
9. Evaluar el código de la aplicación.
10. Evaluar la utilización de peticiones GET y POST en la aplicación Web.
11. Evaluar ataques de manipulación de parámetros al sitio Web.
12. Evaluar la manipulación del URL.
13. Evaluar el uso de Cross Site Scripting. Herramientas: Paros proxy, Fiddler, Burp proxy, TamperIE.
14. Evaluar el uso Hidden Fields. Consiste en descargar el código fuente del sitio Web, guardar la página web en un equipo local, buscar el parámetro “type=hidden”, guardar el cambio, finalmente ingresar a la nueva página y revisar los resultados del cambio.

15. Evaluar el ataque a las cookies. En la cookies es posible encontrar la siguiente información: contraseñas del usuario, la velocidad de las transacciones, monitorear su comportamiento al navegar.
16. Evaluar ataques de Buffer Overflows.
17. Evaluar el uso de datos malos.
18. Evaluar el Client-Side Scripting. Consiste en copiar la URL generada después de un inicio de sesión válida, pegar la URL en una nueva sesión del navegador y observar el resultado.
19. Evaluar el uso de vulnerabilidades conocidas. Herramienta: Bugtraq.
20. Evaluar el uso de Race Conditions. Evaluarlo en aplicaciones que utiliza múltiples hilos para alcanzar un procesamiento simultáneo.
21. Evaluar el uso con User Protection a través de la configuración del navegador.
22. Evaluar las vulnerabilidades por la ejecución de comandos. Hay oportunidades de provocar el fallo de una aplicación a causa por la ejecución algunos comandos de forma arbitraria sí la aplicación web no filtrar adecuadamente los datos que puede ingresar el usuario.
23. Evaluar los ataques de SQL Injection.
24. Evaluar el uso del Blind SQL Injection. Blind SQL injection es idéntico al ataque normal al SQL injection, excepto que un atacante intenta aprovechar el mensaje de error que recibe de una aplicación, recibe en su lugar una página genérica.
25. Evaluar el uso de ataques de Session Fixation. Session Fixation es una técnica de ataque en donde obliga al ID de la sesión del usuario a valor de forma explícita.
26. Evaluar el uso de Session Hijacking. Herramientas: Juggernaut, Hunt, TTY Watcher, T-Sight.
27. Evaluar el ataque XPath Injection. XPath es un lenguaje de programación para documentos XML.

28. Evaluar el uso de ataques de Server Side Include (SSI) Injection. SSI Injection es una técnica de explotación del lado del servidor que le permite al atacante enviar código a una aplicación web, que posteriormente será ejecutado localmente por el servidor web.
    <!--#exec cmd="/bin/ls /" -->
    <!--#INCLUDE VIRTUAL="/web.config"-->
29. Evaluar el uso de fallas de lógica. Una falla de lógica es una forma de mal funcionamiento o error en la lógica de las aplicaciones web, mientras trata de ejecutar correctamente una bifurcación condicional.
30. Evaluar el uso de ataques binarios. Las aplicaciones Web desarrolladas en un lenguaje en donde utilizan buffers estáticos (como son C/C++) podrían ser vulnerables a ataques tradicionales de binarios como son los formatos de cadena de errores y buffer overflows.
31. Evaluar el uso de XML Structural. Consite en enviar mensajes XML largos o mal formados al servidor.
32. Evaluar el uso de XML Content-level. Herramienta: Webscarab.
33. Evaluar el uso de ataques de parámetros WS HTTP GET/REST.
34. Evaluar el uso de Naughty SOAP attachments.
35. Evaluar el uso de WS Replay. Herramientas: WebScarab, TCPReplay.

2.2.16 Pruebas de Penetración a la Seguridad Física

Pasos para conducir una prueba de penetración a la Seguridad Física de una organización:

1. Mapear las posibles entradas.
2. Mapear el perímetro físico.
3. Penetrar cerraduras usados por puertas y closets.
4. Observar desde exterior.

5. Penetrar a los lugares en donde se encuentren los servidores, cables y alambres.
6. Intentar el bloqueo de técnicas recogidas.
7. Sistemas de detección de fuego.
8. Sistemas de aire acondicionado.
9. Intercepción electromagnética.
10. Evaluar sí la organización tiene una política de seguridad física.
11. Activos físicos.
12. Evaluar riesgos.
13. Evaluar sí algún documento importante se encuentra en las instalaciones.
14. Validar como estos documentos son protegidos.
15. Acceso de los empleados.
16. Evaluar el ID de la radio frecuencia (RFID).
17. Acceso físico a las instalaciones.
18. Documentar el proceso.
19. Evaluar a las personas en las instalaciones.
20. ¿Quién está autorizado?
21. Evaluar las puertas contraincendios.
22. Verificar las conexiones de red activas en las salas de reuniones.
23. Verificar las conexiones de red activas en el vestíbulo de la organización.
24. Verificar la existencia de información sensible en las salas de reuniones.
25. Verificar la salida de la recepcionista y/o guardia de seguridad del vestíbulo.
26. Validar a las impresoras accesibles en el vestíbulo.
27. Obtener la lista de teléfonos de la recepcionista del vestíbulo.
28. Escuchar las conversaciones de los empleados en áreas comunes, como en la cafetería.

29. ¿Se puede entrar en un espacio en el techo y entrar a salas seguras?
30. Validar sí es visible sensores de alarmas en puertas y ventanas.
31. Validar en áreas visibles información sensible.
32. Tratar de observar a espaldas del usuario cuando estos ingresan sus credenciales a sus equipos.
33. Tratar de video grabar a un usuario ingresando sus credenciales.
34. Validar sí las puertas exteriores son cuidadas o monitoreadas.
35. Validar sí rutinas de patrullaje tiene huecos en su cobertura.
36. Interceptar y analizar la comunicación entre los guardias.
37. Intentar pasar a cuestas en las puertas de vigilancia.
38. Intentar utilizar identificaciones falsas para obtener acceso.
39. Evaluar formas de entrar después de horas de oficina.
40. Identificar todos los puntos de entrada no vigilados.
41. Revisar las puertas inseguras.
42. Revisar las ventanas inseguras.
43. Intentar eludir los sensores configurados en las puertas y las ventanas.
44. Intentar Dumpster Driving en el área de basura fuera de la compañía.
45. Utilizar binoculares desde fuera del edificio y verificar sí es posible observar lo que está pasando dentro del edificio.
46. Utilizar sensores activos de voz de alta frecuencia para escuchar las conversaciones privadas del personal de la organización.
47. Vestirse como empleado de FedEx/UPS e intentar obtener acceso al edificio.

2.2.17 Pruebas de Penetración a Base de Datos

Pasos para realizar pruebas de penetración a Base de Datos:

1. Escanear los puertos por default utilizados por las Bases de Datos.

2. Escanear los puertos que no son por default utilizados por las Bases de Datos.
3. Identificar el nombre de la instancia utilizada por la Base de Datos.
4. Identificar el número de la versión utilizada por la Base de Datos.
5. Tratar aplicar la técnica de fuerza bruta para obtener la contraseña del hash de la Base de Datos.
6. Realizar sniffing al tráfico relacionado con la Base de Datos en la red local.
7. Evaluar Microsoft SQL server:
    a. Evaluar el acceso directo por interrogación.
    b. Escanear los puertos (1433 TCP/UDP) de Microsoft SQL Server.
    c. Evaluar el SQL Server Resolution Service (SSRS).
    d. Evaluar el ataque Buffer Overflow en la función pwdencrypt().
    e. Evaluar el ataque Heap/Stacks Buffer Overflow en SSRS.
    f. Evaluar el ataque Buffer Overflows en Extended Stored Procedures.
    g. Evaluar el Service Account Registry Key.
    h. Evaluar el Stored Procedure para ejecutar el Web Task.
    i. Utilizar el ataque SQL Injection.
    j. Intentar el Blind SQL Injection.
    k. Google Hacks.
    l. Intentar ataques Direct-exploit.
    m. Intentar el Retrieve Server Account List.
    n. Utilizar las contraseñas por default para ingresar al OSQL.
    o. Intentar retrieve Sysxlogins table.
    p. Evaluar utilizar técnicas de fuerza bruta para obtener el acceso a las cuenta del SA.
8. Evaluar Oracle Server:
    a. Escanear los puertos 1433 TCP/UDP.
    b. Validar el estatus del proceso TNS listener en servidor de Oracle.

c. Tratar ingresar con las contraseñas por default de las cuentas.
d. Tratar de enumerar los SIDs.
e. Utilizar el SQL plus para enumerar las tablas del sistema.

9. Evaluar MySQL Server Database:
   a. Escanear los puertos TCP/UDP.
   b. Extraer la versión de la Base de Datos utilizada.
   c. Tratar de ingresar a la Base de Datos con las cuentas y contraseñas por default.
   d. Utilizar ataques de fuerza bruta con el uso de ataques de diccionario.
   e. Extraer las tablas de los usuarios y del sistema de la Base de Datos.

2.2.18 Pruebas de Penetración a VoIP

Pasos para realizar las pruebas de penetración a VoIP:

1. Ejecutar espionaje.
2. Evaluar realizar los ataques de Flooding y de lógica.
3. Evaluar realizar el ataque de DoS.
4. Evaluar realizar los ataques Call Hijacking y de redirección.
5. Evaluar realizar los barridos de ICMP ping.
6. Evaluar el uso de ARP pings.
7. Evaluar el uso de escaneos TCP pings.
8. Evaluar el barrido de SNMP.
9. Evaluar el uso de Port Scanning y el descubrimiento de servicios.
10. Evaluar el uso de la identificación de equipos y dispositivos.
11. Evaluar la utilización de Banner Grabbing.
12. Evaluar la utilización de la enumeración de extensiones.

13. Evaluar el uso del escaneo automático de OPTIONS. Herramientas: Sipsak.
14. Evaluar el uso del escaneo automático de REGISTER, INVITE y OPTIONS con SIPSCAN contra SIP Server.
15. Evaluar el uso de la enumeración de TFTP Servers.
16. Evaluar el uso de la enumeración de SNMP.
17. Evaluar el uso el sniffing a la configuración de la transferencia de archivos del TFTP.
18. Test for Number Harvesting and Call Pattern Tracking.

2.2.19 Pruebas de Penetración a VPNs

Estos son los pasos para realizar una prueba de penetración a VPNs:

1. Escanear los puertos 500 UDP (IPSEC), 1723 TCP (PPTP), 443 TCP (SSL).
2. Realizar fingerprinting.
   - Obtener el IKE handshake.
   - UDP Backoff fingerprinting.
   - Vendor ID fingerprinting.
   - Evaluar el uso de modo agresivo IKE.
3. Utilizar el PSK Crack.
4. Evaluar el uso de cuentas de usuario por default.
5. Evaluar el uso de SSL VPN.

2.2.20 War Dialing

War Dialing es un método de escaneo automático de números telefónicos empleando un módem para encontrar computadoras conectadas a estos. Este escaneo se realiza empleando programas llamados war dialers.

Los resultados del War Dialing podrían incluir un gran número de módems activos, sistemas de Private Branch Exchange (PBX).

- Recolectar los datos en una Base de Datos.
- Un número telefónico que está constantemente ocupado podría tener un modem u otro recurso críticos.
- Categorizar los carriers.
- Sí un War Dialing detecta cualquier dispositivo no autorizado, es necesario remover o apagar ese dispositivo.

Herramientas: A-Dial, Assault dialer, Autoscan, BASTap, Bbeep, BlueDial, Carrier, CATCALL, Code Thief Delux, CiberPhreak, Deluxe Fone-Code Hacker, Demon Dialer, Dialing Demon, Doo Tools, DTMF_d, Fear's Phreaker Tools, GunBelt, HyperTerm, LapLink, Mhunter, OkiPad, PBX Scanner, PCAnywhere, PhoneSweep, PhoneTag, PhreakMaster, Procomm Plus, Professor Falken's Phreak Tools, Scavenger-Dialer, Super Dial, SecureLogix, THC-scan, The Little Operator, ToneLoc, Ultra-Dial, VrACK, WildDialer, X-DialeR, Zhacker.

2.2.21 Detección de Virus y Troyanos

Pasos para detectar virus y troyanos:

1. Utilizar el comando "netstat –na" para detectar conexiones que tiene establecida algún troyano, revisar si existen conexiones con puertos extraños.
2. Revisar el administrador de tareas de Windows. Revisar si existe algún proceso extraño ejecutándose en el equipo.
3. Verificar si algún programa de anti-virus se está ejecutando en el equipo. Sí existe algún programa, realizar un escaneo a todo el equipo. Herramientas: HitjackThis.

4. Detección de virus en el sector de arranque.

2.2.22 Pruebas de Penetración a la Gestión de Logs

Pasos para realizar pruebas de penetración a la administración de Logs:

1. Escanear los archivos de los logs. Herramientas: Sawmill, bcnumsg.
2. Tratar de inundar al syslog server con logs falsos.
3. Tratar de utilizar mensajes de ataques (Buffer Overflow) al syslog server.
4. Ejecutar el ataque Man-in-the-middle (MITM). De esta forma es posible modificar o destruir el tráfico hacia el syslog server.

2.2.23 Comprobación la Integridad de los archivos

Paso para comprobar la integridad de un archivo:

1. Revisar sí el archivo se descomprime adecuadamente. De no hacerlo, esto indica que el archivo esta corrupto.
2. Comprobar la integridad de un archivo con su valor CRC (Cyclic Redundancy Check).
3. Comprobar la integridad de un archivo con su valor HASH.

Herramientas: cvf, cksum, DySFV, FastSn, FlashSFV, HashCalc, jHashCalc, Jacksum, md5sum, sha1sum, TeraCopy, wxChecksums, SuperSFV, SFV Checker.

2.2.24 Pruebas de Penetración a Bluetooth y Dispositivos de Mano

Pasos para aplicar una prueba de penetración a un equipo iPhone:

1. Tratar aplicar jailbreaking al equipo iPhone. Jailbreaking es el proceso para desbloquear los dispositivos IPhone e iPod touch para permitir la instalación de aplicaciones de terceros. Herramientas: iFuntastic, iDemocracy, iActivator, iNdependence.
2. Tratar de desbloquear el iPhone. Herramientas iPhoneSimFree, anySIM.
3. Tratar de activar el correo de voz en el iPhone desbloqueado.
4. Tratar de atacar el iPhone utilizando Metasploit. Utilizando Metasploit se puede tener control remoto del iPhone, adquirir el acceso a root, acceder a los archivos de forma remota, acceder a los e-mails y revisar el historial del navegador.
5. Validar sí el nombre del Access Point es el mismo para la clave de cifrado.
6. Validar sí se puede enviar datos malformados al dispositivo.
   Herramienta: MobileSafari.
7. Comprobar si la información asignada a la memoria básica puede ser extraída.
   Herramientas: Jailbreaking, iPhoneInterface, CrahsReporter.

Pasos para aplicar una prueba de penetración a un equipo BlackBerry:

1. Intentar aplicar blackjacking a la BlackBerry. Blackjacking es una técnica utilizada para robar la conexión a la BlackBerry. Herramienta: BBProxy.
2. Intentar un ataque enviando un archivo imagen TIFF. BlackBerry presenta problemas para manipular los archivos imágenes TIFF, este tipo archivos pueden causar ataques de DoS cuando son abiertos por el usuario.

Pasos para aplicar una prueba de penetración a un equipo Personal Digital Assistant (PDA):

1. Validar sí es posible aplicar cracking a la contraseña del dispositivo. En dado caso que el usuario utilice una contraseña de protección para acceder a su información personal.
   Herramientas: Brutus, Hydra.
2. Intentar ataques a ActiveSync. ActiveSync es una aplicación utilizada para sincronizar la comunicación entre la PDA basada en Windows y una computadora de escritorio. Al comprometer esta aplicación, el ataque puede revisar o robar la información privada del usuario o instalar otras herramientas en la PDA. Herramientas: Brutus, Cain&Abel.
3. Validar sí el puerto Infrarrojo está activado. Sí esta activado, es posible enviarle un software malicioso al usuario y para extraer su información personal.
4. Verificar sí es posible descifrar los datos cifrados. Herramientas: Crank, Jipher.

Pasos para aplicar una prueba de penetración a la comunicación Bluetooth:

1. Validar sí es posible aplicar cracking al PIN. Herramientas: Brutus, Hydra, BTCrack.
2. Intentar ejecutar el ataque de Blueprinting. El objetivo es obtener el Bluetooth device address (BD_ADDR), Service description records y el modelo del dispositivo.
3. Validar sí es posible extraer el Service Discovery Profiles (SDP). Con el SDP muestra detalles los servicios habilitados en el dispositivo. Herramienta: SDP tool, BTScanner.
4. Intentar ataques de emparejamiento de código. El emparejamiento consiste en conectarse a otro dispositivo mediante una sincronización.

5. Intentar el ataque man-in-the-middle (MITM). Consiste en acceder a la clave de enlace (llave secreta) y la clave de la unidad (BD_ADDR).
6. Intentar el ataque BlueJacking. Consiste enviarle mensajes entre los dispositivos móviles.
7. Intentar un ataque BTKeylogging. Se realiza el ataque sí el teclado del dispositivo tiene un código PIN fijo y si el atacante conoce el BD_ADDR.
8. Intentar un ataque Bluesmacking (ping de la muerte).
9. Intentar un ataque BluSnarfing. Consiste en robar información de los dispositivos wireless a través de una conexión de Bluetooth.
10. Intentar un ataque BlueBug. Consiste en explotar las vulnerabilidades de los dispositivos que tiene habilitado el servicio de Bluetooth. Herramienta: Bluediving.
11. Intentar un ataque BlueSpam.

2.2.25 Pruebas de Penetración a las Telecomunicaciones y a la Comunicación de Banda Ancha

Pasos para realizar una prueba de penetración a las telecomunicaciones y a la comunicación de banda ancha:

1. Validar sí hay un dispositivo firewall instalado en la red.
   - Validar sí están instalados firewalls personales y de hardware.
   - Validar si dichos firewalls cuenta con un módulo para prevención de intrusos ó detectan software inválido.
   - Validar sí el registro de actividades del firewall está activado.
   - Validar sí el firewall está en modo de sigilo. En este modo, el sistema no responderá sus puertos seleccionados, es decir, evitará ser detectados por herramientas de escaneo.
2. Validar sí el navegador está correctamente configurado.

- Validar sí el navegador sí tiene la configuración por default. Una inadecuada configuración del navegador podría ser vulnerable a ataques.
- Revisar los plug-ins del navegador. Los plug-ins son vulnerables a ataques, sobretodo sí son instalados de sitios inseguros.
- Revisar sí los active codes están habilitados. Los controles de ActiveX son vulnerables a ataques.
- Validar sí la versión del navegador está actualizado.
- Revisar sí las cookies están habilitados. Los atacantes se roban las cookies porque contienen información importante de los sitio web visitados por los usuarios, como nombres de usuario y contraseñas. Para protegerse contra estos ataques es recomendable borrar o deshabilitar las cookies.
- Revisar sí los scripting languages están habilitados. Tales como Javascript ó Vbscript, que pueden ser modificados por los atacantes y ser enviados como scripts maliciosos a las computadoras de los usuarios.

3. Revisar la configuración de los sistemas operativos.
    - Revisar sí el sistema operativo y el software de las aplicaciones están actualizados.
    - Revisar sí la opción de compartir archivos e impresoras está habilitado.
    - Revisar sí el anti-virus estás habilitado.
    - Revisar la configuración del anti-virus. Configurar el anti-virus para la revisión de todos los archivos y correos electrónicos entrantes.
    - Revisar sí el anti-spyware está habilitado.

4. Revisar la red inalámbrica, monitorear teléfonos y VPNs. Herramientas: Wiretapping Professional, Wire Tap Pro, WarLinux, AirFart, Aircrack, WEPCrack.
    - Revisar las políticas de configuración de las VPNs, relacionadas con la selección del tipo de cifrado.
    - Intentar monitorear las llamadas telefónicas y el internet.
    - Intentar realizar War Driving. Consiste en buscar redes inalámbricas sobre un vehículo en movimiento utilizando una laptop con antena Wi-Fi para detectar las redes.

2.2.26 Pruebas de Penetración a la Seguridad de E-mail

Pasos para realizar pruebas de penetración a la seguridad de e-mail:

1. Tratar de obtener el ID y contraseña del e-mail. Herramientas: John the Ripper, RainbowCrack, Brutus, WebCracker, ObiWan.
2. Validar sí hay algún software anti-phishing habilitado.
3. Validar sí hay alguna herramienta anti-spamming habilitado.
4. Tratar de ejecutar un e-mail bombing.
5. Ejecutar una prueba de vulnerabilidad ante extensiones CLSID. Consiste en ocultar de la extensión de los archivos adjunto, por consiguiente es posible que se trate de cualquier tipo de archivo.
6. Ejecutar pruebas de vulnerabilidad con archivos adjuntos VBS.
7. Ejecutar pruebas de vulnerabilidades con doble extensión.
8. Ejecutar pruebas de vulnerabilidad con nombres de archivos largos.
9. Ejecutar pruebas de vulnerabilidad a ActiveX.
10. Ejecutar pruebas de vulnerabilidad de Iframe remote.
11. Ejecutar pruebas de vulnerabilidad a los encabezados de los archivos MIME.

12. Ejecutar pruebas de vulnerabilidad a extensiones de archivos mal formados.
13. Ejecutar pruebas de explotar alguna vulnerabilidad para tener acceso.
14. Ejecutar pruebas de vulnerabilidad con mensajes fragmentados.
15. Realizar una prueba un adjunto bastante grande.

2.2.27 Parches de Seguridad en Pruebas de Penetración

Los parches de seguridad en pruebas de penetración consisten en diferentes pasos que son los siguientes:

1. Validar sí la organización cuenta con un equipo validador de parches.
   Preguntar al equipo de administración sí tiene asignado a personal que se encargue de las siguientes actividades:
   - Adquirir los parches de seguridad del proveedor.
   - Probar los parches.
   - Instalar los parches en el sistema informático administrado.
2. Comprobar sí el entorno de seguridad está actualizado.
   Con la instalación de los parches más recientes, los nuevos tipos de vulnerabilidades surgen también. Los nuevos parches pueden afectar el entorno de seguridad. Para evitar esto, es imprescindible actualizar el entorno de seguridad junto con la instalación de un nuevo parche.
   Para comprobar si el entorno de seguridad está actualizado, intente alguna acción perjudicial en el sistema y comprobar si las condiciones de seguridad, como firewalls, antivirus y herramientas de seguridad, detectan tales acciones.
3. Comprobar sí la organización utiliza herramientas automatizadas de gestión de parches.
4. Comprobar la última fecha de instalación de parches.

5. Validar sí los parches son probados primero en sistemas que no están en producción. Es importante probar los parches en un sistema que no está en producción, ya que sí existe alguna vulnerabilidad presente en el parche, es posible evitar afectar a los sistemas de producción e interrumpir su trabajo normal.
6. Comprobar el mecanismo de autenticación de vendedor.

   El vendedor ofrece un mecanismo de autenticación diferente al descargar el parche. La autenticación ayuda asegurar que los parches son de una fuente confiable. Comprobar sí para la descarga de parches es utilizado algún método de autenticación.

   Los métodos de autenticación pueden ser:

   - Sumas de verificación criptográficas.
   - Firmas PGP (Pretty Good Privacy).
   - Certificados Digitales.
7. Comprobar sí los parches descargados contienen virus.

   Hay posibilidades de que los parches puedan contener virus. La instalación de estos parches puede afectar al sistema, por lo que antes de instalar dichos parches, deben ser escaneados con un anti-virus.
8. Comprobar las dependencias de los nuevos parches.

   Es necesario verificar sí los parches están instalados en la secuencia adecuada, en el caso de existir dependencias. También es necesario verificar sí estos nuevos parches desinstalan o desactivan otro parche.

2.2.28 Pruebas de Penetración al Robo de Información

Pasos para realizar una prueba de penetración al Robo de Información:

1. Validar la disponibilidad física de USBs.
2. Validar sí las unidades de USB están habilitadas.

3. Tratar de habilitar las unidades de USB.
4. Validar sí la USB solicita contraseña.
5. Validar sí la comunicación por Bluetooth está habilitada.
6. Validar sí la comunicación por firewire está habilitada.
7. Validar sí los puertos 20 y 21 de FTP están habilitados.
8. Validar sí hay disponible un slot de memoria y sí está habilitado en el sistema.
9. Verificar sí los usuarios utilizan dispositivos con cámaras dentro de áreas restringidas.
10. Verificar sí el sistema tiene algún driver de alguna cámara instalado.
11. Verificar sí hay algún software anti-malware habilitado en el equipo.
12. Verificar sí hay datos cifrados que pueden ser descifrados.
13. Verificar sí los componentes de hardware internos están asegurados.
14. Verificar sí el tamaño de los correo y de los archivos adjuntos están restringidos.

Herramientas para la protección de datos: VIP Privacy, Safed Protector, Reconnex's iguard, Data Protection Software, FolderAccess, VISOCO Data Protection Master, CryptEnCrypt, Steganos Security Suite, Private InfoKeeper, QwikSecure File Protction System.

2.2.29 Entrega de documentación

El informe de la documentación debe consistir en:

- Resumen de la ejecución de la prueba: El resumen debe detallar la información general del proceso de la prueba de penetración.
    - Sinopsis de la organización: Se indica una breve descripción de la organización y de su red.
    - Propósito de la evaluación: La razón por la cual se está realizando la prueba.

- Descripción del sistema.
- Resumen de la Evaluación.
- Las principales conclusiones y recomendaciones. Los principales resultados y problemas que pueden llegar a ser el blanco de ataques en el futuro deben ser incluidos en el informe final. Las acciones que se recomiendan para mitigar las vulnerabilidades, debe también incluirse en el informe.

- Alcance del proyecto: Determinar el alcance del proyecto que especifica los detalles del proceso de prueba.
- El resultado del análisis: Con base en el alcance del proyecto, analizar el resultado del proceso de pruebas utilizando las direcciones IPs, puertos, las pruebas realizadas y el análisis de las vulnerabilidades.
- Recomendaciones: Dentro de los servicios de una prueba de penetración debe recomendar las medidas adecuadas entre las opciones disponibles que pueden ser tomadas para cerrar los problemas descubiertos. Estas recomendaciones sugeridas deben remediar la vulnerabilidad descubierta. Dependiendo del resultado, especifique las recomendaciones para corregir los problemas.
- Apéndices: Preparar los apéndices que incluyen capturas de pantalla, salidas de logs e información del contacto, herramientas utilizadas.

2.2.30 Sintésis de la metodología de EC-Council LPT

La metodología de EC-Council LPT consiste de 26 módulos, los cuales se van aplicando de forma secuencial. Sus módulos de pueden clasificar de acuerdo en dos partes: la primera relacionada con técnicas de hacking y la segunda conformada por dispositivos y tecnologías de redes.

En las técnicas de hacking entran los siguientes módulos:

- Recopilación de Información
- Análisis de Vulnerabilidades
- Prueba de Penetración Externa
- Prueba de Penetración Interna
- DoS
- Password Cracking
- Ingeniería Social
- War Dialing

Los siguientes módulos conforman actividades y distintas técnicas de hacking orientadas a objetivos específicos. Los módulos que hacen referencia a dispositivos y tecnologías de redes:

- Routers y Switches
- Firewall
- IDS
- Red Inalámbrica
- Robo de Laptops, PDAs y Teléfonos Celulares
- Aplicación (sitio Web)
- Seguridad Física
- Base de Datos
- VoIP
- VPN
- Detección de Virus
- Administración de Logs
- Comprobación de Integridad de Archivos
- Bluetooth y Dispositivos de Mano
- Telecomunicaciones y Comunicaciones de Banda Ancha
- Seguridad de E-mail

- Parches de Seguridad
- Robo de Datos

La metodología de EC-Council pretende reunir y ensamblar las distintas técnicas de hacking, así como la forma de evaluar los distintos elementos que conforman la infraestructura de una organización.

2.3 OSSTMM (Open Source Security Testing Methodology Manual)

2.3.1 Definiciones

La metodología utiliza una serie de términos los cuáles se deben asimilar para entender el procedimiento que implica aplicar la metodología e interpretar los resultados obtenidos de las pruebas de seguridad realizadas:

Activo: puede ser cualquier cosa que tiene un valor por sí mismo.

Los canales: son los medios específicos de la interacción con los activos. Se definen tres canales: COMSEC (Seguridad de comunicaciones), PHYSSEC (Seguridad Física), y SPECSEC (Seguridad de Espectro).

Las clases: Son definidas como áreas de estudio, de investigación o de operación. Son definidos cinco canales: Humano, Físico, Comunicaciones Inalámbricas, Telecomunicaciones y Redes de Datos.

El ámbito: Es el total de posibles ambientes operativos de seguridad de cualquier interacción con cualquier otro activo que puede incluir los componentes físicos así como medidas de seguridad. El ámbito está compuesto por los tres canales.

Vector: Es la dirección de una interacción.

Superficie de Ataque: Es la falta de separaciones específicas y controles funcionales que existen para un determinado vector.

Vector de Ataque: Es un sub-ámbito de un vector, creado con el fin de enfocarse a las pruebas de seguridad de un ámbito complejo. Consiste en descomponer recursivamente un problema en dos o en más sub-problemas del mismo tipo (o afines), hasta que estos se convierten en simples como para ser resueltos directamente.

Controles: Es la garantía de que los activos físicos y de información, así como los propios canales están protegidos de diversos tipos de interacciones no válidas tal como es definido por el canal. Se han definido diez controles, los cinco primeros son la Clase A ó controles de interacciones. Por último, los cinco controles de Clase B ó controles de procedimientos.

Limitaciones: Este es el estado actual de los límites percibidos y conocidos por los canales, las operaciones y controles que se han verificado en la auditoría. Las limitaciones se clasifican sobre la base de la consecuencia de la acción operativa.

Operaciones: Las operaciones son la falta de seguridad en algo que tiene que ser interactivo, útil, abierto al público, o disponible.

Seguridad Perfecta: El balance exacto de la seguridad y los controles con las operaciones y limitaciones.

Seguridad Operativa (OpSec): Es una combinación de separación y controles. Para separar la amenaza de los activos es evitar una posible interacción. Llamamos seguridad a la separación de un activo y una amenaza, y así como el control de una amenaza o sus efectos.

Porosidad: Todos los puntos interactivos, operaciones, que se clasifican como visibilidad, accesibilidad o la confianza.

Visibilidad: La visibilidad es un método de cálculo de oportunidad. Es cada activo conocido que existe dentro de un ámbito. Los activos desconocidos solo están en peligro de ser descubiertos en vez de estar en peligro de ser blancos.

Acceso: Es la posibilidad de interactuar directamente con un activo es acceder. El acceso se calcula por el número de lugares diferentes, donde la interacción puede ocurrir.

Confianza: Es la interacción directa con un activo dentro de un ámbito sin que haya de por medio una autenticación.

Seguro: Una forma de protección donde se controla la amenaza o se mitigan sus efectos al mínimo a un nivel aceptable por el propietario o administrador de los activos.

Seguridad: Una forma de protección en donde es realizada una separación entre los activos y la amenaza. Con el fin de asegurar, el activo se retira de la amenaza o la amenaza se elimina del activo.

Rav (Risk Assessment Values): El Rav es una medida a escala de una superficie de ataque, la cantidad de interacciones sin control con un objetivo, que es calculado por el equilibrio cuantitativo entre la porosidad, limitaciones y controles. En esta escala, 100 rav (también a veces se muestra como el 100% RAV) es un equilibrio perfecto y menos de 100 rav son pocos controles y por lo tanto una mayor superficie de ataque. Más de 100 rav muestra más controles que los necesarios que podría ser un problema, ya que los controles suelen añadir las interacciones dentro de un ámbito, así como en complejidad y los problemas de mantenimiento.

Objetivo: Lo que en el ámbito es atacado, que está compuesto por el activo y todas las protecciones que el activo podría tener.

Vulnerabilidad: Es una de las clasificaciones de la limitación en donde una persona o un proceso puede acceder, denegar el acceso a los demás ó se esconde en sí o a los activos dentro del ámbito.

2.3.2 Las Clases y los Canales en un Ámbito

Tabla 2 Clases y los Canales en un Ámbito. (Obtenido del manual de OSSTMM 3.1)

Clases	Canales	Descripción
Seguridad Física (PHISSEC)	Humano	Comprende el elemento humano de la comunicación en dónde la interacción es ya sea física o psicológica.
	Físico	Comprende el elemento tangible de la seguridad en donde la interacción requiere de un esfuerzo físico o un transmisor de energía que manipular.
Seguridad de Espectro (SPECSEC)	Comunicaciones Inalámbricas	Comprende todas la comunicaciones electrónicas, señales, y las emanaciones que se producen en el Espectro Electromagnético (EM) conocido. Esto incluye ELSEC como Comunicaciones Electrónicas, SIGSEC como señales, y EMSEC que son emanaciones sin ataduras de cables.
Seguridad de Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicación, digitales o analógicos, donde la interacción se lleva a cabo a través del teléfono o de teléfonos establecidos como líneas de red.
	Redes de Datos	Comprende todos los sistemas

		electrónicos y redes de datos, donde la interacción se lleva a cabo a través de cables y en líneas de red cableada.

2.3.3. Controles

Los controles son los medios para influir en el impacto de las amenazas y sus efectos cuando la interacción es necesaria. Existen dos tipos de Controles: de Interacciones y de Procesos.

2.3.3.1 Controles de Interacciones

Estos controles influyen directamente a la visibilidad, el acceso y las interacciones confiables. Las categorías de la Clase A son:

1. La Autenticación es un control a través de la solicitud de credenciales basado en la identificación y la autorización.
2. La Indemnización es un control a través de un contrato entre el propietario de los activos y la parte con la interactúan. Este contrato podrá ser en forma de una advertencia visible como un precursor de la acción legal si las normas establecidas no son seguidas o sí falla la protección específica.
3. La Resistencia es un control sobre todas las interacciones de mantener la protección de los activos en el caso de corrupción o de una falla.
4. La Subyugación o Sometimiento es un control para asegurar que las interacciones se producen sólo en función de los procesos definidos.
5. La Continuidad es un control sobre todas las interacciones para mantener la interactividad con los activos en caso de corrupción o falla.

2.3.3.2 Controles de Procesos

Estos controles no influyen directamente en las interacciones solo para proteger los activos una vez que la amenaza está presente. Los controles de Clase B son:

6. No repudio es un control que impide que una de las partes que interactúa de negar su participación ó papel en cualquier interactividad.
7. La Confidencialidad es un control para asegurar un activo mostrado o intercambiado entre las partes en interacción no pueda ser conocido fuera de estas partes. La información comunicada es protegida.
8. La privacidad es un control para asegurar los medios de cómo un activo es accedido, mostrado o intercambiado entre las partes no puede ser conocido fuera de estas partes. Los procesos de comunicación son protegidos.
9. La integridad es un control para asegurar que las partes que interactúan tengan el conocimiento de cuando los activos y los procesos han cambiado.
10. Alarma es un control para notificar que una interacción está ocurriendo o ha ocurrido.

2.3.4 Limitaciones

El estado de la seguridad en lo que respecta a los defectos conocidos y restricciones en el ámbito de operaciones es llamado **Limitación**. Se trata de los agujeros, las vulnerabilidades, debilidades y problemas en mantener la separación entre un activo y una amenaza o en asegurar que los controles continúen trabajando correctamente.

Las limitaciones han sido clasificadas en cinco categorías:

1. La vulnerabilidad es la falla o el error que: (a) niega el acceso a los activos a las personas o procesos autorizados, (b) permite un acceso privilegiado a los activos a personas o procesos no autorizados, o (c) permite que personas o procesos no autorizados ocultar activos o a sí mismos dentro de un ámbito de aplicación.
2. La debilidad es la falla o error que altera, disminuye, abusa, o anula en particular los efectos de los cinco controles de interactividad (Clase A).
3. La preocupación es la falla o error que altera, disminuye, abusa, o anula los efectos del flujo o la ejecución de los cinco controles de proceso (Clase B).
4. La exposición es una acción injustificada, falla o error que proporciona una visibilidad directa o indirecta de los objetivos o los activos dentro del canal de ámbito elegido.
5. Anomalía es cualquier elemento identificable o no, el cual no ha sido controlado y no puede ser considerado en las operaciones normales.

2.3.5 Mapeo de los Controles, Operaciones y Limitaciones

Tabla 3 Mapeo de los Controles, Operaciones y Limitaciones. (Obtenido del manual de OSSTMM 3.1)

<table>
<tr><th colspan="2">Categoría</th><th>Seguridad Operativa</th><th>Limitaciones</th></tr>
<tr><td colspan="2" rowspan="3">Operaciones</td><td>Visibilidad</td><td>Exposición</td></tr>
<tr><td>Acceso</td><td rowspan="2">Vulnerabilidad</td></tr>
<tr><td>Confianza</td></tr>
<tr><td rowspan="3">Controles</td><td rowspan="3">Clase A – Interactivo</td><td>Autenticación</td><td rowspan="3">Debilidad</td></tr>
<tr><td>Indemnización</td></tr>
<tr><td>Resistencia</td></tr>
</table>

2.3.6 Reglas de Contrato

Estas reglas definen las directrices operativas de las prácticas aceptables de comercialización y venta de pruebas, y el manejo de los resultados de las pruebas contratados.

A. Ventas y Marketing

1. El uso del miedo, la incertidumbre, la duda y el engaño no pueden ser utilizado en las presentaciones de ventas o marketing, páginas web, materiales de apoyo, informes o análisis de las pruebas de seguridad con el propósito de vender o proporcionar pruebas de seguridad. Esto incluye pero no se limita a destacar crímenes, hechos, glorificar crímenes o perfiles de hacker, y estadísticas para motivar las ventas.
2. Ofrecer servicios gratuitos para fallar en la prueba de penetración al objetivo está prohibido.
3. Organizar concursos para realizar cracking, hacking y violaciones a sistemas para promover las garantías de seguridad para la venta y la comercialización de pruebas de seguridad o de productos de seguridad están prohibidos.

4. Nombrar a clientes pasados o presentes en la comercialización o la venta para los clientes potenciales solo se permite si el trabajo para el cliente fueron específicamente los mismos que se comercializan o se venden y el cliente nombrado ha proporcionado la autorización por escrito por escrito para hacerlo.
5. Es requerido que a los clientes se les aconseja con la verdad y a los hechos en lo que respecta a su seguridad y medidas de seguridad. La ignorancia no es excusa para la consultoría deshonesto.

B. Evaluación/Estimación de Entrega

6. La realización de pruebas de seguridad en contra de cualquier ámbito sin el permiso explícito por escrito del propietario de destino o autoridad competente está estrictamente prohibido.
7. Las pruebas de seguridad a sistemas, obviamente muy inseguros e inestables, están prohibidos hasta que la adecuada infraestructura de seguridad se ha puesto en marcha.

C. Contratos y negociaciones

8. Con o sin un contrato de acuerdo de Confidencialidad, el pentester de seguridad es requerido garantizar la confidencialidad y no divulgación de información de clientes y resultados de las pruebas.
9. Los contratos deben limitar la responsabilidad del costo del trabajo, a menos que la actividad maliciosa ha sido demostrado.
10. Los contratos deben explicar con claridad los límites y peligros de la prueba de seguridad como parte del contrato de trabajo.
11. En el caso de las pruebas a distancia, el contrato debe incluir el origen de los analistas por su dirección, número de teléfono o la dirección IP.

12. El cliente debe presentar un contrato firmado que establece el permiso para realizar las pruebas con el indulto de los pentesters en el ámbito y responsabilidad de los daños que el costo del servicio de la prueba de penetración, con la excepción en donde se ha demostrado actividad maliciosa.
13. Los contratos deben contener los nombres de contacto de emergencia y sus números telefónicos.
14. El contrato debe incluir permisos claros y específicos para las pruebas que involucran fallas de supervivencia, de denegación de servicio, análisis de procesos e ingeniería social.
15. Los contratos deben contener el proceso para futuros contratos y de cambios al contrato de trabajo.
16. El contrato debe contener una verificación de conflictos de intereses para la realización de una prueba de seguridad y del reporte.

D. Definición del alcance.

17. El alcance debe estar claramente definido contractualmente antes de verificar los servicios vulnerables.
18. La prueba debe explicar claramente los límites de las pruebas de seguridad de acuerdo con el ámbito de aplicación.

E. Plan de Pruebas

19. El plan de pruebas no puede contener los planes, procesos, técnicas o procedimientos que están fuera del área de experiencia o nivel de competencia del analista.

F. Pruebas de Procesos

20. El pentester debe respetar y mantener la seguridad, la salud, el bienestar y la privacidad de los ciudadanos tanto dentro como fuera del ámbito de aplicación.
21. El pentester siempre debe operar dentro de la ley de la ubicación física de los objetivos además de las normas y leyes que regulan la ubicación del pentester en las pruebas.
22. Para prevenir aumentos temporales en la seguridad durante las pruebas, solo se notifica a las personas clave durante la prueba. A juicio del cliente el cual discierne quienes son las personas clave, sin embargo, es asumido que serán informados los encargados de la información y sus políticas, los administradores de los procesos de seguridad, personal de respuesta a incidentes, y el personal de operaciones de seguridad.
23. Sí es necesario para las pruebas con privilegios, el cliente debe proporcionar dos, separados, acceso a tokens ya sean contraseñas, certificados, números seguros de ID, insignias, etc. y que deberían ser de usuarios con típicos privilegios los que están siendo probados en lugar de accesos vacíos o seguros.
24. Cuando la prueba incluye con privilegios conocidos, el analista debe probar primero sin privilegios antes de realizar la prueba con privilegios.
25. Los pentesters deben de conocer sus herramientas, como trabajan y haberlas probado en área de pruebas restringido antes de usarlas en la organización del cliente.
26. La realización de pruebas en las cuales se tiene la intención de probar la denegación de un servicio o proceso, o la supervivencia sólo se puede hacer con el permiso explícito y sólo en el ámbito donde se lleva a cabo ningún daño fuera del alcance o de la comunidad.

27. En las pruebas en donde se involucran personas sólo puede llevarse a cabo sobre las prácticas identificadas en el ámbito de aplicación y no puede incluir personas privadas, clientes, socios, asociados, o de otras entidades externas sin el permiso escrito de estas entidades.
28. Durante la verificación de limitaciones, tales como las infracciones encontradas, vulnerabilidades con la tasa de explotación conocida o alta, las vulnerabilidades que son explotables por completo, accesos sin monitorear o imposibles de encontrar, o que de inmediato podría poner en peligro vidas, des cubiertos durante las pruebas deben ser reportadas al cliente con una solución práctica tan pronto como han sido encontradas.
29. Cualquier forma de prueba de inundación, en donde un ámbito es abrumado desde una fuente más grande y más fuerte está prohibido sobre canales de propiedad no privada, por ejemplo Internet.
30. El pentester no puede salir del ámbito del ámbito de aplicación en una posición de menos “Seguridad Actual” de lo que era cuando fue proporcionada.

G. La Presentación de informes

31. El pentester debe respetar y mantener la privacidad de todos los individuos en los resultados obtenidos.
32. En los resultados que involucran a personas sin entrenamiento en seguridad o que no pertenezcan al personal de seguridad, sólo serán reportados a través de la no identificación o por medios estadísticos.
33. El pentester no puede firmar los resultados de las pruebas ni los reportes de pruebas de seguridad en los que no estuvo directamente involucrado.
34. Los reportes deben ser objetivos y sin mentiras.

35. Las notificaciones al cliente son necesarias cada vez que el pentester cambia el plan de las pruebas, cambia el lugar de origen de las pruebas, tiene resultados bajos en confianza, o cualquier problema que se ha producido en las pruebas. Las notificaciones deben ser siempre antes de que las pruebas se vuelvan a ejecutar, son peligrosas o de mucho tráfico, y las actualizaciones del progreso de las pruebas deben de ser de forma periódica.
36. Las soluciones y recomendaciones incluidas en el reporte, deben ser válidos y prácticos.
37. Los reportes deben marcar claramente todas las incógnitas y las anomalías.
38. Los reportes deben establecer claramente los descubrimientos exitosos de fallas en las medidas de seguridad así como de limitaciones en los controles.
39. Los reportes deben de utilizar sólo métricas cuantitativas para medir la seguridad. Estas métricas deben basarse en hechos y evitar las interpretaciones subjetivas.
40. El cliente debe recibir una notificación cuando el reporte le es enviado y a su vez el cliente debe confirmar la recepción de la entrega.
41. Todos los canales de comunicación para la entrega del informe deben ser confidenciales, de extremo a extremo.
42. Los resultados y los reportes no pueden ser utilizados para fines comerciales.

2.3.7 Métricas de Seguridad Operacional

Una métrica operativa es una medida constante que nos informa de un recuento de hechos, en el caso de esta metodología la métrica utilizada es el Rav, el cual es una descripción imparcial y objetiva de una superficie de ataque.

El Rav es en realidad varios cálculos por separado de la Porosidad, Controles y Limitaciones, que cuando son combinados mostrará el tamaño de la superficie de ataque de dos maneras prácticas. La primera manera es en un cálculo directo. Es el cálculo del Delta, un número que describe la exposición específica de ese objetivo. Esto es útil para determinar cómo una persona, cosa o proceso va a cambiar la seguridad operacional de un nuevo ámbito o como una comparación entre varios objetivos ó uno solo. Esta es también la forma más fácil de ver la seguridad perfecta, el equilibrio perfecto entre la Porosidad, Controles y Limitaciones.

Un delta positivo indica que se gasta mucho en controles, en general, o incluso hay un exceso de gastos esta en demasiada cantidad de un tipo de control. Una delta negativa muestra una falta de controles o controles de sí mismos con las limitaciones que no pueden proteger adecuadamente el objetivo.

La segunda forma práctica para mostrar la superficie de ataque es para entender el panorama general. Esto es representado como la Seguridad Actual. Cuando el cálculo del Delta se basa en un equilibrio perfecto, el cálculo de la Seguridad Actual utiliza el Delta, pero también incluye controles adicionales y redundantes para proporcionar una métrica más amigable y familiar.

El Rav se deriva de tres categorías definidas dentro del ámbito: Seguridad Operacional, Controles y Limitaciones de Seguridad.

2.3.7.1 Porosidad

La Seguridad Operacional ($SegOp_{sum}$), también conocida como la porosidad del ámbito, es el primero de los tres factores de seguridad real que debe ser

determinada. En principio, se mide como la suma de la visibilidad del alcance (P_V), el acceso (P_A) y la confianza (P_C).

$$SegOp_{sum} = P_V + P_A + P_C \qquad (2.1)$$

Al calcular el Rav, es necesario determinar el valor de la Seguridad Operacional base, $SecOp_{base}$. El valor de la Seguridad Operacional base está dada por la siguiente ecuación:

$$SegOp_{base} = \log^2 (1 + 100 \times SegOp_{sum}) \qquad (2.2)$$

2.3.7.2 La Fórmula de Controles

El siguiente paso en el cálculo del Rav es definir los Controles, los mecanismos de seguridad establecidos para proteger las operaciones. En primer lugar se suman los Controles, C_{sum} , debe ser determinada por la suma de las diez categorías de Controles.

Tabla 4 Clasificación de Controles. (Obtenido del manual de OSSTMM 3.1)

Controles	Clase A	Autenticación	C_{Au}
		Indemnización	C_{Id}
		Resistencia	C_{Re}
		Sometimiento	C_{So}
		Continuidad	C_{Ct}
	Clase B	No Repudio	C_{NR}
		Confidencialidad	C_{Cf}
		Privacidad	C_{Pr}

		Integridad	C_{It}
		Alarma	C_{Al}

Así, la suma de los Controles está dada de la siguiente forma:

$$C_{sum} = C_{Au} + C_{Id} + C_{Re} + C_{So} + C_{Ct} + C_{NR} + C_{Cf} + C_{Pr} + C_{It} + C_{Al} . \quad (2.3)$$

2.3.7.3 Los Controles Faltantes (CF)

Dado que la combinación que cada uno de los 10 Controles equilibra el valor de 1 de la pérdida de *SecOp* (visibilidad, acceso, confianza) es necesario para determinar la cantidad de controles que faltan, CF_{sum} , con el fin de evaluar las Limitaciones de la Seguridad. Esto debe hacerse de forma individual para cada una de las diez categorías de los controles.

Por ejemplo, para determinar los controles que faltan para la Autenticación (CF_{Au}) hay que restar la suma de los controles (Au_{sum}) del alcance de la $SegOp_{sum}$. Los Controles Faltantes no pueden ser nunca menor que cero, por lo tanto:

$$\text{IF } SegOp_{sum} - Au_{sum} \leq 0$$

$$\text{THEN } CF_{Au} = 0$$

$$\text{ELSE } CF_{Au} = SegOp_{sum} - Au_{sum}$$

El resultado total de control faltante de cada uno de los diez controles debe ser sumado para llegar al valor total del control Faltante (CF_{sum}) como se muestra a continuación:

$$CF_{sum} = CF_{Au} + CF_{Id} + CF_{Re} + CF_{So} + CF_{Ct} + CF_{NR} + CF_{Cf} + CF_{Pr} + CF_{It} + CF_{Al} . \quad (2.4)$$

2.3.7.4 Controles Reales

Los controles reales se obtienen de la siguiente forma:

$$CR_{sum} = SegOp_{sum} - CF_{sum} . \qquad (2.5)$$

Los controles reales se utilizan para medir la ubicación ideal de los controles. El valor base también ayuda a eliminar la influencia de una colocación desproporcionada de los controles de seguridad. Los Controles de Verdad Base (CV_{base}) son expresados de la siguiente forma:

$$CR_{base} = \log^2 (1 + 10 \times SegOp_{sum} - CF_{sum} \times 0.1). \qquad (2.6)$$

2.3.7.5 Cobertura Real

Basado en la misma idea que los controles reales, la Cobertura Real (*CobReal*) se puede utilizar para medir el porcentaje de controles en el lugar que respecta a la cantidad óptima y la ubicación de los controles. La Cobertura Real (*CobReal*) se obtiene a partir del total de los Controles Faltantes (CF), como se muestra en la siguiente ecuación:

$$\text{IF } SegOp_{sum} = 0$$

$$\text{THEN } CobReal = 0$$

$$\text{ELSE } CobReal = 1 - \frac{CF_{sum}}{10 \times SegOp_{sum}} \qquad (2.7)$$

2.3.7.6 Controles Totales

Se debe tener en cuenta todos los controles en su lugar, independientemente de una distribución equilibrada. Este valor es importante para medir el valor de la autenticación de dos factores. Los Controles Totales base (CT_{base}) se expresa de la siguiente forma:

$$CT_{base} = \log^2\left(\frac{1+10}{10\times C_{sum}}\right) \qquad (2.8)$$

2.3.7.7 La Fórmula de las Limitaciones

Las limitaciones son valoradas de forma individual. La valoración de las vulnerabilidades, debilidades y preocupaciones se basan en una relación entre la Porosidad o $SegOp_{sum}$, los Controles. Una Exposición o Anomalía no plantea ningún problema a menos que una sola vulnerabilidad, debilidad o preocupación también está presente, ya que de lo contrario no tiene ningún efecto sobre la seguridad y por lo tanto no tiene ningún valor en el Rav.

En la siguiente tabla de valores se utiliza para calcular la variable $LimSeg_{sum}$, como un paso intermedio entre las entradas de las Limitaciones de la Seguridad y la variable $LimSeg_{base}$, que es la entrada de limitaciones de seguridad básicos para la ecuación de Rav.

IF $SegOp_{sum} = 0$

THEN $CobF = 0$ (Cobertura Faltante)

ELSE $CobF = CF_{sum} \times 0.1 / SegOp_{sum}$ (2.9)

Tabla 5 Cálculo de las Limitaciones. (Obtenido del manual de OSSTMM 3.1)

Entrada	Cálculo de las variables	Variables
Vulnerabilidad L_V	$\frac{(SegOp_{sum} + CF_{sum})}{SegOp_{sum}}$	CF_{sum}: suma de los Controles Faltantes
Debilidad L_D	$\frac{(SegOp_{sum} + CF_A)}{SegOp_{sum}}$	CF_A: suma de los Controles Faltantes en los Controles de Clase A

Preocupación L_P	$\frac{(SegOp_{sum} + CF_B)}{SegOp_{sum}}$	CF_B: suma de los Controles Faltantes en los Controles de Clase B
Exposición L_E	$\frac{((P_V + P_A) \times CobF + L_V + L_D + L_P)}{SegOp_{sum}}$	P_V: suma de la Visibilidad P_A: suma de Accesos $CobF$: Porcentaje de la Cobertura Faltante
Anomalía L_A	$\frac{(P_T \times CobF + L_V + L_D + L_P)}{SegOp_{sum}}$	P_T: suma de la Visibilidad $CobF$: Porcentaje de la Cobertura Faltante

2.3.7.8 Limitaciones de Seguridad Base

El total de las Limitaciones de Seguridad, $LimSeg_{sum}$, se calcula como la suma total de cada entrada multiplicada por su correspondiente valor estimado según se define en la tabla 2.4.

$$LimSeg_{sum} = \left(L_V \times \frac{(SegOp_{sum} + CF_{sum})}{SegOp_{sum}}\right) + \left(L_D \times \frac{(SegOp_{sum} + CF_A)}{SegOp_{sum}}\right) + \left(L_P \times \frac{(SegOp_{sum} + CF_B)}{SegOp_{sum}}\right) + \left(L_E \times \frac{((P_V + P_A) \times CobF + L_V + L_D + L_P)}{SegOp_{sum}}\right) + \left(L_A \times \frac{(P_T \times CobF + L_V + L_D + L_P)}{SegOp_{sum}}\right) \quad (2.10)$$

La ecuación de las Limitaciones de Seguridad base es dada como:

$$LimSeg_{base} = \log^2 (1 + 100 \times LimSeg_{sum}) \quad (2.11)$$

2.3.7.9 La Fórmula de la Seguridad Actual

Esta es la parte final para el uso de todos los cálculos anteriores en tres aspectos diferentes: Delta de la Seguridad Actual, Protección Real y finalmente obtenemos el valor de la Seguridad Actual.

2.3.7.9.1 Delta de la Seguridad Actual

La Delta de la Seguridad Actual es útil para comparar productos y soluciones previamente estimados el cambio (delta) que el producto o solución hicieron en el ámbito. Podemos determinar la Delta de las Seguridad Actual, *SegAct*Δ, con la siguiente fórmula:

$$SegAct\Delta = CT_{base} - SegOp_{base} - LimSeg_{base} \qquad (2.12)$$

2.3.7.9.2 Protección Real

Se puede utilizar como una expresión simplificada para la cobertura óptima de un determinado ámbito, donde 100 significa una relación óptima entre la Porosidad, los Controles de Verdad y las Limitaciones de Seguridad. La Protección Real está dada por la siguiente ecuación:

$$ProReal = 100 + CV_{base} - SegOp_{base} - LimSeg_{base} \qquad (2.13)$$

2.3.7.9.3 Seguridad Actual

Para medir el estado actual de las operaciones con los controles aplicados y las limitaciones encontradas, un cálculo final es requerido para definir la Seguridad Actual. Como lo indica su nombre este es el valor de la seguridad general que combina los tres valores de la seguridad operacional, controles y limitaciones para mostrar el estado actual de la seguridad.

La Seguridad Actual (total), *SegAct*, es el verdadero estado de la seguridad que ofrece como una especie de hash de las tres secciones.

La última ecuación para obtener el Rav para la Seguridad Actual, se obtiene con la siguiente ecuación:

$$SegAct = \frac{100 + SegAct\Delta - 1}{100} \times \left(SegOp_{base} \times CT_{base} - SegOp_{base} \times LimSeg_{base} + CT_{base} \times LimSeg_{base}\right)$$

(2.14)

2.3.8 Metodología de OSSTMM

El flujo de la metodología de OSSTMM comienza con una revisión de la postura del objetivo. La postura es la cultura, reglas, normas, contratos, leyes y políticas que definen el objetivo. Termina con resultados comparativos de las alarmas, alertas, informes o registros de acceso. Por lo tanto, el primer paso es estar consciente de las necesidades de funcionamiento para interactuar con el objetivo, y el último paso es la revisión de los registros de las pruebas.

Esta metodología separa lo que se necesita hacer en este formato jerárquico:

1. Canal
2. Módulo
3. Tarea

La tarea se muestra en la descripción del módulo para cada canal en particular. La metodología cuenta con 17 módulos y las mismas propiedades se aplican a los cinco canales. Mientras que la metodología en sí puede ser el mismo, en cada canal son diferentes las tareas que se deben realizar. Cada módulo tiene una entrada y una salida. La entrada es la información que se utiliza para la realización de cada tarea. La salida es el resultado de las tareas completadas. Esta salida puede servir de entrada para uno ó más módulos.

2.3.9 Las Fases y los Módulos de la Metodología

La metodología de OSSTMM está conformada por cuatro fases, las cuales son las siguientes:

A. **Fase de Inducción.** El pentester comienza con la comprensión de los requisitos de las pruebas, el alcance y las limitaciones de esta. Con frecuencia, el tipo de prueba se determina mejor después de esta fase.
B. **Fase de Interacción.** Es definido el ámbito de la aplicación.
C. **Fase de Investigación.** En esta fase es posible apreciar el valor o detrimento de la información equivocada y mal administrada como un activo.
D. **Fase de Intervención.** Estas pruebas se enfocan en los recursos que los objetivos requieren en el ámbito.

En la siguiente tabla, es mostrado los módulos que constituyen cada una de las fases de la metodología, así como su descripción:

Tabla 6 Las Fases y los Módulos de la Metodología. (Obtenido del manual de OSSTMM 3.1)

Fases	Módulos	Descripción
A. Fase de Inducción	A.1 Revisión de Postura	La revisión de la cultura, reglas, normas, reglamentos, leyes y políticas aplicables al objetivo. Define el alcance y que pruebas deben hacerse; requerido para realizar de manera correcta la Fase C.
	A.2 Logística	La medición de las limitaciones de

		interacciones tales como la distancia, velocidad, y la falibilidad de determinar los márgenes de exactitud en los resultados.
	A.3 Verificación de la Detección Activa	La verificación de la práctica y la amplitud de detección de interacciones, y la previsibilidad de respuesta. Para conocer las restricciones impuestas a las pruebas interactivas y llevar adecuadamente las Fases B y D.
B. Fase de Interacción	B.4 Auditoría de la Visibilidad	La determinación de los objetivos que van a ser probados dentro del ámbito. La visibilidad es considerada como "presencia" y no se limita a la vista humana.
	B.5 Verificación de Acceso	La medición de la amplitud y profundidad de los puntos de acceso interactivos dentro del objetivo y la autenticación necesaria.
	B.6 Verificación de la Confianza	La determinación de las relaciones de confianza de y entre los objetivos. Una relación de confianza existe en dondequiera que el objetivo acepta la interacción entre los objetivos en el ámbito de aplicación.

	B.7 Verificación de los Controles	La medición de la utilización y eficacia de los controles de pérdida basados en procesos (Clase B): el no repudio, confidencialidad, privacidad e integridad. El control de alarma se verifica al final de la metodología.
C. Fase de Investigación	C.8 Verificación de los Procesos	La determinación de la existencia y eficacia del registro y mantenimiento de los actuales niveles de seguridad se define por la revisión de la postura y los controles de indemnización. La mayoría de los procesos tienen definidos un conjunto de reglas, sin embargo, las operaciones reales no reflejan ninguna eficiencia, por lo tanto, es necesario redefinir las reglas establecidas.
	C.9 Verificación de Configuración/Verificación de la Capacitación	La investigación del estado estable (funcionamiento normal) de los objetivos tal como han sido diseñados para funcionar en condiciones normales para determinar problemas de fondo fuera de la aplicación de pruebas de stress de seguridad.
	C.10 Validación de Propiedad	La medición de la amplitud y profundidad en el uso de la propiedad intelectual ilegales o sin licencia o

		aplicaciones dentro del objetivo.
	C.11 Revisión de la Segregación	La determinación de los niveles de identificación de información personal definido por la revisión de la postura. Sabemos cuáles son los derechos de privacidad se aplican y en qué medida la información detectada como personal puede ser clasificados en base a estos requisitos.
	C.12 Verificación de la Exposición	La búsqueda de información libremente disponible que describe la visibilidad indirecta de los objetivos o los activos en el canal elegido por el alcance.
	C.13 Exploración de Inteligencia Competitiva	La búsqueda de información libremente disponible, directa o indirectamente, que podría perjudicar o afectar negativamente al propietario del objetivo a través de medios externos. Descubrir información que por sí sola o en conjunto puede influir en las decisiones de negocios.
D. Fase de Intervención	D.14 Verificación de la Cuarentena	La determinación y la medición del uso eficaz de la cuarentena para todos los accesos hacia y dentro del objetivo. Determinar la efectividad de los controles

		de autenticación y el sometimiento en términos de cuarentena de listas blancas y negras.
	D.15 Auditoría de Privilegios	El mapeo y la medición del impacto del mal uso de los controles de sometimiento, las credenciales y los privilegios o la escalada no autorizada de privilegios. Determinar la eficacia de la autorización en los controles de autenticación, la indemnización, y el sometimiento en términos de profundidad y roles.
	D.16 Validación de la Supervivencia/Continuidad del Servicio	La determinación y la medición de la resistencia del objetivo a los cambios excesivos o adversos (Denegación de Servicios) en los controles de continuidad y la capacidad de recuperación que se verían afectados.
	D.17 Revisión de Alertas y Registros/Estudio Final	Una revisión de las actividades de auditoría realizadas con la verdadera profundidad de las actividades según lo registrado por el objetivo o por un tercero como control de alarma. Se pretende saber que partes de la auditoría dejó un rastro útil confiable.

2.3.10 Representación en Bloques de la Metodología

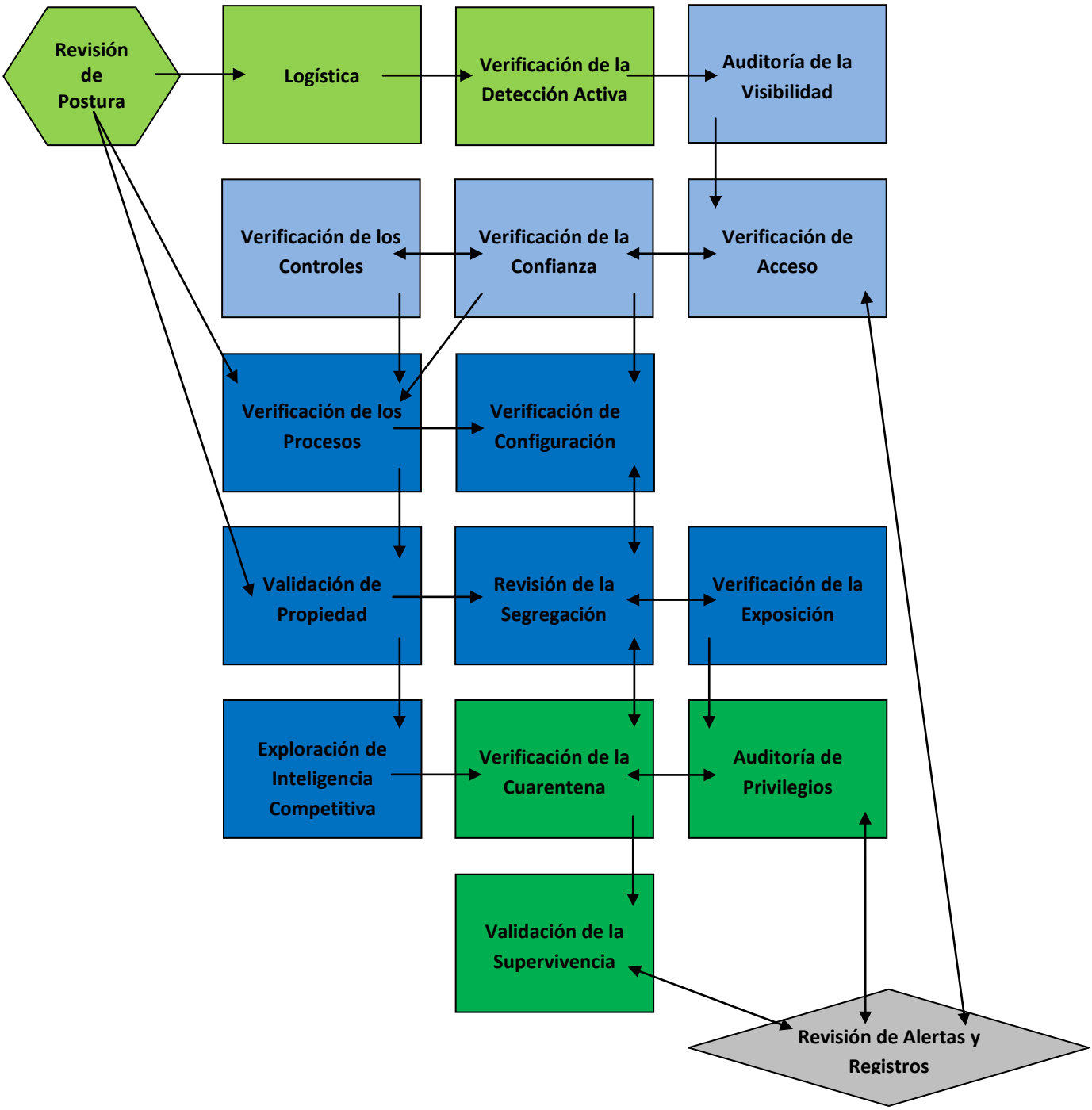

Figura 4 Representación en Bloques de la Metodología. (Obtenido del manual de OSSTMM 3.1)

2.3.11 Resultados de las pruebas

El Reporte de Auditoría de Seguridad de Prueba (Security Test Audit Report – START) requiere la siguiente información:

1. Fecha y hora de la prueba.
2. Duración de la prueba.
3. Los nombres de los analistas responsables.
4. Tipo de Prueba.
5. Ámbito de la prueba.
6. Índice (Método de la enumeración del Objetivo)
7. Canal probado.
8. Vector probado.
9. Métricas de la Superficie de Ataque.
10. Qué pruebas se han completado, cuales no se terminaron, o parcialmente completa, y en qué medida.
11. Cualquier error o problema referente a la prueba y la validez de los resultados.
12. Todos los procesos que influyen en las limitaciones de seguridad.
13. Cualquier incógnita o anomalía.

2.3.12 Síntesis de la Metodología de OSSTMM

La metodología de OSSTMM divide la totalidad de una infraestructura en cinco canales para su estudio. La metodología está constituida de cuatro fases y estás a su vez por diecisiete módulos, estos módulos tienen sus correspondientes tareas y procedimientos, los cuales varían dependiendo del canal que se está evaluando.

A. Fase de inducción. Consiste en determinar los requisitos de las pruebas, el alcance y sus limitaciones. En esta parte se recopilación información pero relacionada las leyes, ética, políticas, regulaciones

industriales y la cultura que influyen en los requisitos de seguridad y privacidad de la organización a la que se aplicará las pruebas.

B. Fase de Interacción. Es definido el ámbito de aplicación, son determinados los objetivos que serán probados. En estas pruebas serán definidos los parámetros de Visibilidad, Acceso, Confianza y la verificación de los controles Clase B (el no repudio, confidencialidad, privacidad e integridad; control de alarma es definido en la fase D).
C. Fase de Investigación. Se determina que tanto en la práctica se están cumpliendo las políticas y reglas de seguridad con la realidad de las operaciones.
D. Fase de Intervención. Son verificados los controles de autenticación, indemnización y sometimiento. También se realizan pruebas para la medición de la resistencia de los controles para mantener la continuidad de las operaciones, así como su capacidad de recuperación. La parte final de toda la metodología consiste en la revisión de los logs, para la búsqueda de la evidencia de las pruebas, lo cual representa verificar el control de alarma.

Al término de la aplicación de la metodología de OSSTMM, tenemos identificados y cuantificados los elementos para determinar los valores que le corresponden a la porosidad y a los controles, con estos resultados hacemos uso de las fórmulas revisadas en este capítulo para determinar el valor de la Seguridad Actual del ámbito que estamos evaluando.

2.4 Conclusiones del capítulo 2

La metodología del NIST indica el proceso general de cómo llevar a cabo una prueba de penetración, hace poca referencia al uso explicito herramientas.

La metodología es extensa y trata de cubrir todos los aspectos informáticos y humanos que tiene contacto con la información de las organizaciones. Es muy detallada en cuanto las técnicas y herramientas a utilizar para realizar las pruebas. Dentro de las herramientas a las que hace referencia incluye tanto propietarias como gratuitas.

La metodología de OSSTMM propone una nueva visión acerca de la seguridad, divide en cinco canales todos los elementos que constituyen el mapa de seguridad de una organización. En base a los elementos antes mencionados son utilizados para obtener la medición de seguridad, siendo así la única metodología en expresar de forma numérica el resultado final de las pruebas.

Capítulo 3

Estudio Comparativo de Metodologías de Pruebas de Penetración

En este capítulo es realizado el estudio comparativo de cada una de las metodologías con respecto a las etapas del Hacking Ético, para determinar sus semejanzas y diferencias.

3.1 Etapas de componen un Hacking Ético

Para realizar el análisis comparativo de las metodologías tomamos como referencia las siguientes etapas para aplicar un Hacking Ético.

1. Planificación
2. Recopilación de Información.
3. Escaneo.
4. Explotación.
5. Manteniendo el Acceso.
6. Cubrir Huellas.
7. Reporte.

Estas etapas son definidas en base a la literatura revisada, varía en la forma de nombrar cada una de las etapas pero en esencia convergen a las 7 etapas propuestas. (Ali, 2011), (Faircloth, 2011), (Engebretson, 2011), (Kennedy,2011) (Sallis, 2011).

3.2. Similitudes entre las Metodologías del NIST SP800-115, EC-Council LPT y OSSTMM

A continuación son enlistadas las similitudes de las metodologías de nuestro estudio:

- Lista de requisitos y necesidades de la organización que la prueba de penetración debe cumplir.
- De acuerdo a las necesidades de la organización, determinar los tipos de pruebas a realizar y los servicios que serán revisados.
- Obtener el permiso de la Alta Gerencia de la organización para realizar la prueba de penetración.
- Definir el alcance de las pruebas. Establecer los límites de la prueba en términos de acciones y de los resultados esperados.

- Preparar el documento legal de la prueba de penetración, en la cual se indique las reglas, las condiciones y aspectos legales de las pruebas que se pretenden realizar.
- Definir los criterios y procedimientos a realizar en caso de que una de las pruebas tenga un impacto negativo en la red o que un ataque se presente durante la prueba en marcha.
- Especificar las obligaciones y limitaciones del pentester.
- Preparar el contrato de Confidencialidad.
- Obtener un seguro de responsabilidad de una empresa de seguros. Para protegerse en caso de provocar un daño no intencionado a cualquiera de los activos informáticos de la organización durante la prueba de penetración.
- Realizar una relación de los administradores de los principales activos de la organización, con sus respectivos datos, para contactarlos en caso de ser necesario.
- Identificar los requisitos de cumplimiento de seguridad del cliente.
- Determinar los sistemas y/o redes que se probará durante todo el proceso de pruebas y establecer una lista de exclusión.
- Determinar la frecuencia y los métodos de comunicación con respecto a los avances e incidentes ocurridos durante el proceso de la prueba de penetración.
- En dado caso que se pretenda realizar algún tipo de entrevista (ingeniería social), se debe proporcionar las preguntas y deben de ser aprobadas por la alta gerencia antes de ser aplicadas.
- Establecer la forma en que será la recolección, almacenamiento y transmisión de los datos generados como resultado de las pruebas.
- Establecer los requisitos de la presentación y el informe de los resultados que se esperan durante y finalización de las pruebas. Especificar la información mínima que debe contener cada reporte

(por ejemplo, las vulnerabilidades y las técnicas recomendadas de mitigación).

- Determinar el nivel de acceso (usuario o administrador) a los sistemas y/o red.
- Especificar el hardware y software, que el equipo de pentesters utilizará para realizar las pruebas.
- Los contratos deben explicar con claridad los límites y peligros de la prueba de seguridad como parte del contrato de trabajo.
- En el caso de las pruebas a distancia, el contrato debe incluir el origen de los analistas por su dirección, número de teléfono o la dirección IP.
- Los contratos deben contener los nombres de contacto de emergencia y sus números telefónicos.
- El alcance debe estar claramente definido contractualmente antes de verificar los servicios vulnerables.
- El pentester siempre debe operar dentro de la ley de la ubicación física de los objetivos además de las normas y leyes que regulan la ubicación de las pruebas.
- Cuando la prueba incluye con privilegios conocidos, el pentester debe probar primero sin privilegios antes de realizar la prueba con privilegios.
- El pentester deben de conocer sus herramientas, como trabajan y haberlas probado en área de pruebas restringido antes de usarlas en la organización del cliente.
- En las pruebas en donde se involucran personas sólo puede llevarse a cabo sobre las prácticas identificadas en el ámbito de aplicación y no puede incluir personas privadas, clientes, socios, asociados, o de otras entidades externas sin el permiso escrito de estas entidades.
- Sí durante las pruebas son encontradas vulnerabilidades con una alta tasa de explotación o que podría poner en peligro vidas deben ser reportadas a la organización de inmediato.

- Las notificaciones al cliente son necesarias cada vez que el pentester cambia el plan de las pruebas, cambia el lugar de origen de las pruebas, tiene resultados bajos en confianza, o cualquier problema que se ha producido en las pruebas. Las notificaciones deben ser siempre antes de que las pruebas se vuelvan a ejecutar, son peligrosas o de mucho tráfico, y las actualizaciones del progreso de las pruebas deben de ser de forma periódica.
- Especificar las reglas de la forma a realizar la prueba de penetración así como indicar las limitaciones y líneas de tiempo. Es necesario indicar los tipos de ataques a realizar, a que servidores y los horarios y tiempos de duración para ejecutarlos.
- Lista de las pruebas que no se realizarán en la red de la organización.
- En caso que se requiera realizar una prueba desde Internet que sea considerada como prohibida o como un delito informático, solicitar un permiso especial para el cumplimiento de la ley.
- Establecer los requisitos de la presentación y el reporte de los resultados que se esperan durante y finalización de las pruebas. Especificar la información mínima que debe contener cada reporte (por ejemplo, las vulnerabilidades y las técnicas recomendadas de mitigación).
- El pentester no puede firmar los resultados de las pruebas ni los informes en los que no estuvo directamente involucrado.

3.2.1 Similitudes entre las metodologías de EC-Council LPT y NIST SP800-115

A continuación son enlistadas las similitudes entre las metodologías de EC-Council LPT y el NIST SP800-115:

- El escaneo de vulnerabilidades es mediante el uso de herramientas que contienen una base de datos de vulnerabilidades conocidas.
- En el reporte final presentan: las vulnerabilidades encontradas, indican el proceso utilizado para su explotación, finalmente recomendaciones y observaciones para mitigar las debilidades encontradas.

3.3 Diferencias entre las Metodologías NIST SP800-115, EC-Council LPT y OSSTMM

De acuerdo al estudio realizado, mostrados a continuación las diferencias que tiene entre sí las metodologías:

3.3.1 NIST SP800-115

- Establece destruir los datos generados como resultado de las pruebas.

3.3.2 EC-Council LPT

- Recopilar información sobre la organización, incluyendo su historia.
- Visitar las instalaciones de la organización en cuestión para familiarizarse con el entorno e instalaciones.
- Identificar el espacio asignado de oficina para que el equipo de pentesters trabaje durante la duración del proyecto.

- Preparar el equipo humano para realizar la prueba de penetración.
    - Jefe del equipo de las Pruebas de Penetración.
    - Experto en Base de Datos
    - Experto en Aplicaciones Web.
    - Experto en Redes.
    - Analista de Datos.
    - Encargado de documentar las pruebas realizadas.

3.3.3 OSSTMM

- En OSSTMM están explícitamente prohibidas las siguientes actividades:
    - El uso del miedo, la incertidumbre, la duda y el engaño en las presentaciones de ventas o marketing, con el propósito de vender o proporcionar pruebas de seguridad.
    - Ofrecer servicios gratuitos para fallar en la prueba de penetración al objetivo.
    - Organizar concursos para realizar cracking, hacking y violaciones a sistemas para promover las garantías de seguridad para la venta y la comercialización de pruebas de seguridad o de productos de seguridad.
    - Nombrar a clientes pasados o presentes en la comercialización o la venta para los clientes potenciales, solo sí cliente nombrado ha proporcionado la autorización por escrito por escrito para hacerlo.
    - El uso de la Denegación de Servicio Distribuido durante las pruebas.
- Es requerido que a los clientes se les aconseja con la verdad y a los hechos en lo que respecta a las medidas de seguridad.

- Las pruebas de seguridad a sistemas, obviamente muy inseguros e inestables, están prohibidas hasta que la adecuada infraestructura de seguridad se ha puesto en marcha.
- Con o sin un contrato de acuerdo de Confidencialidad, el pentester debe garantizar la confidencialidad y no divulgación de información de clientes y resultados de las pruebas.
- El plan de pruebas no puede contener los planes, procesos, técnicas o procedimientos que están fuera del área de experiencia o nivel de competencia del pentester.
- El analista debe respetar y mantener la seguridad, la salud, el bienestar y la privacidad de los ciudadanos tanto dentro como fuera del ámbito de aplicación.
- El pentester debe respetar y mantener la privacidad de todos los individuos en los resultados obtenidos.
- En los resultados que involucran a personas sin entrenamiento en seguridad o que no pertenezcan al personal de seguridad, sólo serán reportados a través de la no identificación o por medios estadísticos.
- Los reportes deben ser objetivos y sin mentiras.
- Las soluciones y recomendaciones incluidas en el reporte, deben ser válidos y prácticos.
- Los reportes deben marcar claramente todas las incógnitas y las anomalías.
- Los reportes deben establecer claramente los descubrimientos exitosos de fallas en las medidas de seguridad así como de limitaciones en los controles.
- Los reportes deben de utilizar sólo métricas cuantitativas para medir la seguridad. Estas métricas deben basarse en hechos y evitar las interpretaciones subjetivas.

- El cliente debe recibir una notificación cuando el reporte le es enviado y a su vez el cliente debe confirmar la recepción de la entrega.
- Todos los canales de comunicación para la entrega del informe deben ser confidenciales, de extremo a extremo.
- Los resultados y los informes no pueden ser utilizados para fines comerciales.
- Realiza una revisión de las reglas y políticas de seguridad de la organización, OSSTMM las toma como parámetro para determinar sí los controles de seguridad que las políticas establecidas, por el contrario, establecer nuevas políticas de seguridad y/o corregir las ya existentes.
- Una vulnerabilidad es aquellas fallas en los activos o en los controles que permite en la seguridad operacional un acceso o relación de confianza en los activos que vayan en contra de las políticas de seguridad de la organización.
- La etapa de cubrir huella no es una actividad considerada en OSSTMM, sino por el contrario, tiene como objetivo validar el correcto funcionamiento de los controles de alarma, que todas las actividades realizadas en la metodología queden registradas, es decir, que ninguna actividad quede sin registro o en su defecto activen algún control de alarma todo aquello vaya en contra de las políticas de seguridad.
- Además de entregar reporte como lo hacen EC-Council LPT y el NIST SP800-115, incluye adicionalmente su plantilla llamada START (Security Test Audit Report). Es un resumen ejecutivo en el cual se muestra los canales evaluados, el tipo de pruebas y los valores obtenidos derivados de la aplicación de sus fórmulas propuestas, en el que destaca el valor de la Seguridad Actual, además de otros datos.

3.4 Conclusiones del capítulo 3

Las fases que constituyen al NIST SP800-115 se asemejan a las etapas de un Hacking Ético, su principal diferencia consiste en establecer como obligatorio la eliminación de los datos derivados de las pruebas, ya que EC-Council y OSSTMM lo dejan al criterio al pentester y a la organización.

Por otro lado, EC-Council LPT es un compendio de técnicas de hacking, la cual tiene como objetivo proporcionar las bases para entender estás técnicas y ser una guía para llevar a cabo pruebas de seguridad. Esta metodología está enfocada a pentester con poca experiencia, ya que para su aplicación marca paso a paso como realizar las pruebas. La desventaja de esta metodología esta en las pruebas relacionadas a sitios Web, son realizadas de manera general, siendo mejor en esta área la metodología de OWASP, que se especializa en pruebas de penetración en sitios web. Otra desventaja es que en muchos de sus módulos se traslapan las pruebas a realizar, por ejemplo, las actividades del módulo Análisis de Vulnerabilidades son realizadas también en los módulos de Pruebas Externas e Internas o en cualquier módulo que haga referencias a un dispositivo de red de la organización (como lo son Routers, Switches, Firewal, etc.).

Las metodologías que tienen más similitudes entre sí son las de EC-Council LPT y la del NIST SP800-115.

OSSTMM tiene un enfoque diferente de realizar las pruebas de penetración, toma como base las políticas de seguridad y contempla la existencia entre los controles de seguridad la indemnización de los activos, el tenerlos asegurados, característica que no cubren las otras metodologías. La principal ventaja que tiene OSSTMM, es la capacidad de expresar con un valor numérico el nivel de seguridad de una organización. OSSTMM hace énfasis el carácter ético del pentester para la realización de las pruebas.

Para OSSTMM, la falta de reglas y políticas de seguridad en una organización, es la falta de una postura de cómo debe ser tratada la información de dicha información en sus procesos operativos.

Capítulo 4

Conclusiones y Trabajo a Futuro

En este capítulo son presentadas las conclusiones del estudio comparativo de las metodologías del NIST SP800-115, EC-Council LPT y OSSTMM.

CONCLUSIONES

Las metodologías de pruebas de penetración constan de tres partes:

- Antes de la fase de ataque: Consiste en recopilar la mayor información posible del objetivo.
- Fase de ataque: Es la ejecución de la estrategia de ataque hacia el objetivo.
- Después del ataque: El pentester debe restablecer a las aplicaciones y a la red en general a su estado original. Esto implica la eliminación de las vulnerabilidades creadas y la limpieza de los procesos y exploits utilizados durante la prueba.

La autorización escrita por parte de la organización, para la realización y los alcances de la prueba de penetración, es la diferencia entre un pentester y un atacante.

Una metodología de prueba de penetración ayuda a planificar y establecer una estrategia para la ejecución de las pruebas de acuerdo con la información previamente recolectada.

Una metodología garantiza que el proceso de una prueba de penetración sea de manera estándar con resultados repetibles.

Las fases que constituyen al NIST SP800-115 se asemejan a las etapas de un Hacking Ético. Su principal diferencia consiste en establecer como obligatorio la eliminación de los datos derivados de las pruebas, ya que EC-Council y OSSTMM lo dejan al criterio al pentester y a la organización.

EC-Council LPT es un compendio de técnicas de hacking, la cual tiene como objetivo proporcionar las bases para entender estás técnicas y ser una guía para llevar a cabo pruebas de seguridad.

La metodología de OSSTMM, contempla la revisión de las políticas de seguridad y la indemnización de los sistemas informáticos. Esta metodología es la que tiende a tener características de una auditoría informática. La principal ventaja que tiene OSSTMM sobre las otras metodologías, es su capacidad de expresar con un valor numérico el nivel de seguridad de una organización.

TRABAJO A FUTURO

Realizar el análisis comparativo entre otras metodologías de prueba de penetración distintas a las analizadas en este trabajo.

Diseñar una metodología para realizar pruebas de penetración a partir del resultado de los análisis realizados.

BIBLIOGRAFÍA

ALI, S., Heriyanto, T. (2011). *BackTrack 4: Assuring Security by Penetration Testing.* Packt Publishing. The United States of America

EC-COUNCIL (2008). *EC-Council Certified Security Analyst/ Lincesed Penetration Tester V.4*

ENGEBRETSON, P. (2011). *The Basics of Hacking and Penetration Testing.* Syngress. The United States of America

FAIRCLOTH, J. (2011). *Penetration Tester's Open Source Toolkit.* Syngress. The United States of America

HERZOG, P. (2010). *OSSTMM 3.1 (The Open Source Security Testing Methodology Manual)*.

KENNEDY, D., O'Gorman, J., et. al. (2011). *Metasploit. The Penetration Tester's Guide.* No starch press. The United States of America

OWASP Fundation (2008). *OWASP TESTING GUIDE V3.0*

SALLIS, E., Caracciolo, C., et. al. (2010). *ETHICAL HACKING. Un enfoque metodológico para profesionales.* Alfaomega. Argentina

SCARFONE, K., Souppaya, M., et. al. (2008). *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115 Technical Guide to Information Security Testing and Assessment.* The United States of America

HEMEROGRAFÍA

Caballero, A. (2009, Julio-Agosto). Barcelona: Ethical Hacking utilizando BackTrack. *Linux*+, 56, 18-27.

García, L. (2009, Julio-Agosto). Barcelona: El Arte de la Seguridad. *Linux*+, 56, 52-57.

Kilpatrick, I. (2010, Mayo). Estados Unidos de América: Don't let the zombies take you down, *Haking9*, 5-30, 46-48.

Lozano, R. (2008, Diciembre). Barcelona: Hardening en Linux. *Linux*+, 49, 42-46.

Lozano, A. (2009, Septiembre). Barcelona: Seguridad básica en servidores Linux, *Linux*+, 57, 68-71.

Puente, D. (2009a, Abril). Barcelona: Ataques Man In The Middle. *Linux*+, 53, 46-53.

Puente, D. (2009b, Abril). Barcelona: Proyecto Metaspolit. *Linux*+, 53, 54-59.

Puente, D. (2009a, Julio-Agosto). Barcelona: Xprobe2: técnicas de fingerprinting. *Linux*+, 56, 28-31.

Puente, D. (2009b, Julio-Agosto). Barcelona: Hacking: Análisis de Seguridad. *Linux*+, 56, 32-38.

Puente, D. (2009, Septiembre). Barcelona: Buffer Overflows: un mal interminable, *Linux*+, 57, 82-87.

Puente, D. (2009, Octubre). Barcelona: Buffer Overflows: un mal interminable, parte 2, *Linux*+, 58, 50-57.

Puente, D. (2009, Noviembre). Barcelona: Shellcodes en Linux, *Linux*+, 59, 74-81.

CIBERGRAFÍA

CERT UNAM: www.cert.org.mx/estadisticas.dsc (Consultado en Agosto, 2011)

CHECK: www.cesg.gov.uk/products_services/iacs/check/index.shtml (Consultado en Agosto, 2011)

COFETEL: http://www.cft.gob.mx/es/Cofetel_2008/Cofe_servicios_de_internet (Consultado en Agosto, 2010)

EC-COUNCIL: www.eccouncil.org (Consultado en Agosto, 2010)

IBM http://www-935.ibm.com/services/in/gts/iss/pdf/i10707562-pen-tes-tds.pdf (Consultado en Agosto, 2011

McAfee: http://www.mcafee.com/us/services/technology-consulting/infrastructure-assessments/external-assessment.aspx (Consultado en Agosto, 2011)

OISSG: www.oissg.org/issaf (Consultado en Agosto, 2010)