ESTUDIO, ANÁLISIS Y APLICACIÓN DE TÉCNICAS DE ETHICAL HACKING EN ENTORNOS CORPORATIVOS.

JAIRO NICOLÁS PIRAJÁN CASTRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

ESTUDIO, ANÁLISIS Y APLICACIÓN DE TÉCNICAS DE ETHICAL HACKING EN ENTORNOS CORPORATIVOS.

JAIRO NICOLÁS PIRAJÁN CASTRO

Monografía elaborada como requisito de grado para optar por el título de Especialista en Seguridad Informática

Tutor
ING. ALEXANDER LARRAHONDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

Nota de Aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 28 de abril de 2022

DEDICATORIA

Deseo dedicar todo este proyecto con mucho fervor y agradecimiento a:

- Mi madre, por alentarme y motivarme cada día, por darme fuerzas, por no esperar nada a cambio, por querer siempre lo mejor para mi vida, por todos los esfuerzos y sacrificios que hizo para criar a un hombre de bien y sobre todo por estar siempre presta a brindarme su apoyo incondicional a pesar de todas las adversidades.

- Mi padre, por siempre tenderme la mano para levantarme y continuar, por ser un ejemplo de buen hombre y de conducta intachable, por aconsejarme y enseñarme el valor de los pequeños detalles y sobre todo por enseñarme el amor por la lectura.

- Mi hermano, para que sepa que con dedicación y empeño se pueden lograr todas las cosas que deseamos y que cuando caemos nos levantamos más fuertes y con la cabeza en alto.

- Mi esposa, por estar a mi lado y motivarme cada día a superarme, por sus valiosas asesorías, su comprensión, su tiempo, su paciencia y su apoyo, sin ti no hubiese sido posible llegar hasta donde estoy, gracias por ser esa persona que me ayudó a crecer como profesional y como persona.

- Mis hijos, por ser mi fuente de inspiración para este y todos mis proyectos, gracias por regalarme esa hermosa sonrisa cada día y enseñarme que con esfuerzo, dedicación, disciplina y compromiso los sueños se cumplen, todo lo que hago es por ustedes mis campeones de vida.

- Mis amigos, su ejemplo de superación y entereza me han inspirado desde siempre, sus consejos nunca sobraron en mi vida, gracias por enseñarme a superarme cada día, gracias por no dejarme desfallecer y gracias por ayudarme a ser una mejor persona cada día.

AGRADECIMIENTOS

Primeramente, a Dios y a la Vida por permitirme estar en este mundo terrenal cumpliendo mis sueños y dándome fuerzas cada día para no desfallecer.

A mi querida madre por siempre estar motivándome y alentándome a continuar con mis estudios y a seguir adelante a pesar de todas las adversidades.

A mi esposa por ser un pilar fundamental en mi vida y porque sin su apoyo y conocimientos no se hubiese podido culminar este trabajo.

Al profesor Luis Fernando Zambrano por tener siempre una buena disposición, tener una excelente pedagogía y aportar toda su experiencia y pericia en la consolidación de esta monografía.

A todos los tutores de las diferentes materias porque siempre estuvieron prestos a resolver todas las inquietudes que les manifesté y aportaron todos sus conocimientos que me sirvieron de insumo para concluir este trabajo de grado.

Al Ing. Nelson P. Albornoz por ser un amigo incondicional y por compartir ampliamente y sin recelo todos sus conocimientos y experiencia para la realización de este trabajo.

Al Ing. Manuel Gutiérrez porque sin sus bastos conocimientos en redes y su valiosa amistad no lo hubiese logrado.

A todos y cada uno de mis compañeros con los que batallamos hombro a hombro y día a día en cada una de las materias por sacar esta especialización adelante.

A todas las demás personas que a pesar de no nombrarlas saben que fueron parte fundamental para la creación de esta monografía, que aportaron un granito de arena y que siempre estuvieron a mi lado motivándome a seguir.

TABLA DE CONTENIDO

INTRODUCCIÓN 10
1. PLANTEAMIENTO DEL PROBLEMA 11
2. JUSTIFICACIÓN 12
3. OBJETIVOS 13
3.1 OBJETIVO GENERAL 13
3.2 OBJETIVOS ESPECÍFICOS 13
4. MARCO REFERENCIAL 14
4.1 MARCO TEÓRICO. 14
4.1.1 OSSTMM (Open Source Security Testing Methodology Manual) 14
4.1.2 PTES (Penetration Testing Execution Standart) 21
4.1.3 CEH (Certified Ethical Hacker) 25
4.2. MARCO CONCEPTUAL 28
4.3. MARCO LEGAL 31
5. DESARROLLO DE LA PROPUESTA 32
5.1. Alistamiento de máquinas 32
5.2 Interacciones previas al compromiso (PTES) 33
5.3 Recolección de información – Exploración - Análisis de vulnerabilidades (PTES-CEH-OSSTMM) 33
5.4 Modelado de amenazas (PTES) 43
5.5 Explotación y Post-explotación – Ganando y Manteniendo el acceso (PTES – CEH- OSSTMM) 44
5.6 Informes (PTES) 60
6. CONCLUSIONES 61
BIBLIOGRAFÍA 65
ANEXOS 67
Anexo 1. Formato Auditoría Inicial 67
Anexo 2. Activos de Información - MAGERIT 79
Anexo 3. Plan de Pruebas según los dominios de ISO/IEC 27001:2013 81
Anexo 4. Formato Informe Ejecutivo de Auditoria 86
Anexo 5. Formato Informe Técnico de Auditoria 87

LISTA DE TABLAS

Tabla 1. Activos de Información - MAGERIT.....79
Tabla 2. Plan de pruebas dominios de ISO/IEC 27001:2013 81

LISTA DE ILUSTRACIONES

Ilustración 1. Fases OSSTMM. 15
Ilustración 2. Fases PTES. 21
Ilustración 3. Fases CEH. 26
Ilustración 4. Portal de empleo con información sensible. 34
Ilustración 5. Búsqueda WhoIs. 35
Ilustración 6. Red Social con información sensible. 35
Ilustración 7. Resolución DNS con nslookup: set type=MX y set type=NS en Windows. 36
Ilustración 8. Maltego – Aplicación de transformaciones DNS y obtención de IP's. 37
Ilustración 9. ip-tracker-Rastreo de IP. 38
Ilustración 10. 192.168.0.1 Enrutador. 39
Ilustración 11. Puertos abiertos enrutador. 40
Ilustración 12. Detalle Enrutador. 40
Ilustración 13. Máquina Ubuntu. 41
Ilustración 14. Puertos abiertos máquina Ubuntu. 41
Ilustración 15. Detalle máquina Ubuntu. 42
Ilustración 16. Máquina Kali Linux. 42
Ilustración 17. Topología de Red desde Nmap. 43
Ilustración 18. ARP Spoofing 44
Ilustración 19. Selección tarjeta de red NAT en Máquina Virtual con Kali Linux. 45
Ilustración 20. Diagrama de Red. 45
Ilustración 21. ifconfig virtual machine. 46
Ilustración 22. netdiscover. 46
Ilustración 23. Clientes conectados a la red – Virtual Machine. 47
Ilustración 24. Lista de clientes conectados a la red - Host Machine. 47
Ilustración 25. Host Machine se convierte en router de Virtual Machine. 48
Ilustración 26. Host Machine reemplaza el verdadero AP. 49
Ilustración 27. MAC de Host Machine reemplazando el verdadero AP. 50
Ilustración 28. Máquina Virtuales en Oracle VM. 51
Ilustración 29. Kali Linux Versión. 51
Ilustración 30. Ubuntu Versión. 52
Ilustración 31. IP Kali Linux. 52
Ilustración 32. IP Ubuntu. 53
Ilustración 33. Instalación Apache. 53
Ilustración 34. Inicio y Status servicio Apache. 54
Ilustración 35. Instalación zenmap Kali Linux. 54
Ilustración 36. Puertos abiertos máquina Ubuntu. 55

Ilustración 37. Escaneo de tráfico de red - Wireshark 55
Ilustración 38. Acceso a Ubuntu desde Kali Linux. 56
Ilustración 39. Archivo en Documentos - Ubuntu. 56
Ilustración 40. Fake mailer. 59
Ilustración 41. e-mail fraudulento. 60

INTRODUCCIÓN

Una de las principales preocupaciones de las organizaciones hoy en día es la ciberseguridad. Dicho tema fue elegido por ser una de las principales actividades que se deben llevar a cabo en los temas relacionados con la seguridad de la información y, la aplicación de diferentes metodologías de intrusiones garantizará que se realice de forma ecuánime y bajo estándares internacionales.

Es importante tener en cuenta que se deben efectuar y llevar a cabo en todas las organizaciones test de penetración con el fin de reforzar los mecanismos y controles de protección de la información teniendo en cuenta el gran número de amenazas a las que están expuestas.

La pérdida de información en las organizaciones en los últimos tiempos es y ha sido el resultado del desconocimiento, descuido y falta de preocupación sobre la seguridad de la información, lo anterior da lugar a que se realicen inversiones y contrataciones de servicios especializados en Hacking Ético y precisamente el objetivo de este ejercicio es brindar un acercamiento a las organizaciones para que actúen preventivamente en contra de intromisiones maliciosas valiéndose de los test de intrusión que evalúan técnicamente la seguridad de la información, aplicaciones web, servidores, redes informáticas, etc.

Es necesario, por tanto, determinar las técnicas basadas en metodologías de Ethical Hacking para cumplir con el objetivo de dar a conocer el impacto sobre los entornos corporativos y saber cuál es la que más se adecúa a las necesidades latentes.

Se toma como referencia para la ejecución de la presente monografía alguna de las metodologías más significativas tales como: OSSTMM, CEH y PTES de las cuales se extraen los puntos más importantes de las fases y etapas que se plantean en cada una de ellas para la realización de una prueba de seguridad o test de penetración.

1. PLANTEAMIENTO DEL PROBLEMA

Dentro de las organizaciones se está cultivando el pensamiento y la cultura de la seguridad informática, sin embargo, se está realizando un uso inadecuado gracias a que en muchas ocasiones se tiene desconocimiento del tema o no se quiere realizar una inversión importante lo cual está generando brechas de seguridad.

Con el pasar del tiempo las personas siguen interesándose mucho más por la seguridad informática ya sea de una forma propositiva o de una forma malintencionada; y es que el valor de la información hoy en día es muy alto, por esto es que cada vez salen a la luz virus informáticos y malware que intentan comprometer la seguridad en una organización y al mismo tiempo se están creando y actualizando las bases de datos de los antivirus para combatir esto, pero no solo es sugerir a las organizaciones que adquieran el antivirus más costoso para estar seguros, existen normatividades y planes creados a nivel público y privado con lineamientos a seguir con el fin de mantener la información lo más privada que se requiera (ISO 27001, COBIT, MAGERIT, entre otras).

Adicional a las normativas, con el pasar del tiempo se han creado organizaciones dedicadas a combatir intrusiones y se han generado metodologías y técnicas que por medio del Ethical Hacking han ayudado a descubrir ciertas vulnerabilidades que anteriormente no se pensaban que existían y que están ayudando a mejorar controles de seguridad.

Por lo anterior, se ha evidenciado que las amenazas de seguridad evolucionan rápidamente y es por esa razón la importancia de realizar pentesting en infraestructuras tecnológicas con el fin de encontrar vulnerabilidades a las que pueden estar expuestas y conocer los motivos que llevan a realizar un ataque.

Con el incremento en el uso de aplicaciones web y todas las funcionalidades que ofrece, es necesario crear aplicaciones con altos niveles de seguridad, confidencialidad e integridad. De igual manera la seguridad de las aplicaciones permite proteger los datos y la pérdida de información que es considerado como uno de los activos más importantes en la actualidad. Teniendo en cuenta lo anterior, se establece el siguiente interrogante:

¿Cómo el uso adecuado de metodologías para realizar Hacking Ético en entorno empresariales proveerá mecanismos y lineamientos adecuados para proteger y garantizar la estabilidad, confiabilidad y seguridad de los datos?

2. JUSTIFICACIÓN

La información es uno de los principales activos de todas las organizaciones y con el trascurrir del tiempo se ha ido buscando la forma de optimizar los procesos de protección de esta lo cual ha generado que se dé mayor atención a la disponibilidad, confidencialidad e integridad de los sistemas informáticos.

Las normativas ISO 27001, COBIT, MAGERIT nos presentan concienzudamente los procesos, políticas y métricas que deben seguirse por parte de los administradores de sistemas, acompañados de los demás altos mandos de la organización, para poder garantizar la integridad de los datos y la seguridad de la Información, sin embargo, aspectos técnicos o metodológicos para la evaluación de vulnerabilidades no se incluyen en estos marcos de referencia, y en no son practicados mayormente, ya sea por temas presupuestarios o por falta de iniciativa los altas esferas dentro de la estructura organizacional mandos en la organización.

Con lo anterior es válido indicar que un proceso de Pentesting o Ethical Hacking se debe realizar como medida de seguridad pertinente que permita encontrar vulnerabilidades y huecos de seguridad que pongan en riesgo la información dentro de la organización. Ésta es una de las razones más importantes para realizar la aplicación de técnicas de intrusión y razón por la cual se eligió el tema para desarrollar la monografía propuesta, de igual forma, se requiere establecer cuál es la mejor metodología que aminore los impactos negativos y ayuden a establecer mejores políticas de seguridad de la información, se pretende que con la generación de un informe final, que enmarque un diagnóstico y unas recomendaciones, se pueda crear un plan de acción que se pueda replicar hacia los demás elementos de la red informática de las organizaciones.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar técnicas y metodologías de Ethical Hacking que puedan ser implementadas en un entorno corporativo, con el fin de generar recomendaciones que permitan mejorar un entorno digital seguro por medio de un documento monográfico.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer las tres metodologías de Ethical Hacking más importantes usadas actualmente que aportan resultados significativos en la realización de pruebas de penetración o auditorias con el fin de destacar cuales pueden ser sus factores de éxito.

- Esquematizar los hallazgos, evidencias y resultados de la ejecución de pruebas de penetración basadas en las metodologías de Ethical Hacking más utilizadas en la actualidad con el fin de reconocer posibles vectores de ataque que más se presentan.

- Plantear recomendaciones basadas en los resultados obtenidos a partir de simulaciones efectuadas, que sirvan como pauta al mejoramiento de la seguridad informática en entornos corporativos.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO.

Con el propósito de realizar un análisis sobre las metodologías de Ethical Hacking más usadas en la actualidad y que se puedan implementar en entorno corporativos, se ha realizado una investigación que permita referenciar las más importantes y las fases que ellas se contemplan, no sin desmeritar las demás metodologías existentes que fueron diseñadas por grandes equipos de trabajo y son igual de aplicables a todos y cada uno de los ambientes informáticos, sin embargo al querer optar por ciertas técnicas más que por otras es basado en la versatilidad y adaptabilidad que tienen estas y sobre todo porque su implementación permite obtener resultados certeros en muy poco tiempo, así pues, a continuación se relacionan las metodologías que aportan resultados muy significativos en la realización de pruebas de penetración y con el que se da cumplimiento al objetivo específico número uno:

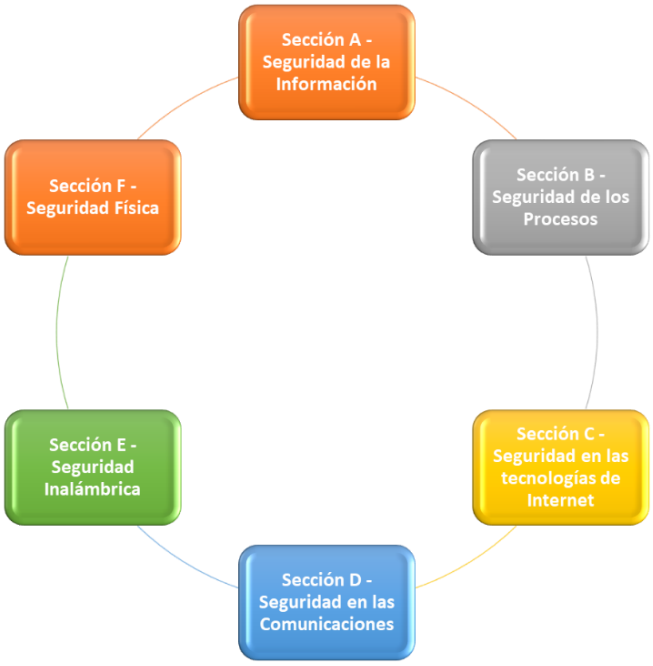
4.1.1 OSSTMM (Open Source Security Testing Methodology Manual)

"La presente metodología está desarrollada por ISECOM (Instituto de Seguridad y Metrologías Abiertas), la cual es una comunidad abierta y una organización sin fines de lucro registrada oficialmente en Cataluña, España, se basa en la investigación en seguridad informática, fue fundada en Enero del 2001 y su objetivo es proporcionar concienciación en seguridad; su principal proyecto es OSSTMM (Open Source Security Testing Methodology Manual), el mencionado documento se ha convertido en un estándar a largo de los años. Este manual ha sido revisado por pares de pruebas y análisis de seguridad que da como resultado hechos verificados, los cuales proporcionan información procesable que puede mejorar apreciablemente la seguridad operativa de cualquier organización a la que se aplique. Una forma de garantizar que un análisis de seguridad tenga valor es saber que se ha realizado de manera exhaustiva, eficiente y precisa."[1]

Según el manual generado por ISECOM, se encuentra que esta metodología se compone de una serie de secciones, módulos y tareas las cuales son lineales y unidireccionales, es decir, cada uno de ellos tiene relación directa con el anterior, así como se ilustra en la ilustración 1:

[1] LÓPEZ Roberto. Propuesta de implementación de una metodología de auditoría de seguridad informática [en línea]. Trabajo de grado. Universidad Autónoma de Madrid, 2015. [Consultado 03 julio 2021]. Disponible en https://repositorio.uam.es/bitstream/handle/10486/668900/Lopez_Santoyo_Roberto_tfg.pdf

Ilustración 1. Fases OSSTMM.



Fuente: El autor.

La sección A comprende la Seguridad de la información y posee los módulos de:

4.1.1.1 Revisión de la Inteligencia Competitiva.

Comprende un reconocimiento pasivo por medio de información publicada a través de internet, las tareas a realizar en este módulo son: Realizar un mapa y medir la estructura de directorio de los servidores web y FTP, examinar la base de datos WHOIS para los servicios de negocio, determinar el costo de soporte de la infraestructura, obtener los productos que se están vendiendo desde las aplicaciones web.[2]

4.1.1.2 Revisión de Privacidad.

Consta del estudio dentro de la ética y responsabilidad legal del almacenamiento, trasmisión y revisión de datos basados en la privacidad del cliente y del empleado, las tareas a realizar en este módulo son: Obtener información del tamaño de la base de datos, su ubicación, los tipos de cookies y verificar los métodos de encriptación de datos.[3]

---

[2] HERZOG, Pete. Revisión de la Inteligencia Competitiva. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 35

[3] HERZOG, Pete. Revisión de Privacidad. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 36

4.1.1.3 Recolección de Documentos.

Aquí se verifica la información testeada y perteneciente a los niveles de seguridad de la información, con el fin de definir perfiles, las tareas a realizar en este módulo son: Examinar las bases de datos, levantar información de personas clave en la organización como direcciones email, datos laborales por niveles tecnológicos.[4]

La sección B comprende la Seguridad de los procesos y posee los módulos de:

4.1.1.4 Testeo de Solicitud.

Es un método para ganar privilegios de acceso preguntando al personal de entrada por medio de teléfono, email, chat, etc.[5]

4.1.1.5 Testeo de las Personas Confiables.

Es un método que se basa en una posición que tiene un individuo de confianza como la de un empleado o un vendedor o un familiar para inducir a una persona interna a revelar información referente a la organización, las tareas a realizar en este módulo son: seleccionar personas y contactarlas e intentar obtener información y, enumerar la cantidad de información privilegiada obtenida.[6]

La sección C comprende la Seguridad en las tecnologías de Internet y posee los módulos de:

4.1.1.6 Exploración de Red.

El sondeo de red sirve para recolectar datos, obtener información y determinar las políticas de control, las tareas a realizar en este módulo son: Examinar la información de registro de dominio en busca de servidores, encontrar propietarios de bloques de IP's, utilizar trazas a la puerta de enlace para identificar routers y segmentos de red e inspeccionar logs de servidores.[7]

---

[4] HERZOG, Pete. Recolección de Documentos. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 37

[5] HERZOG, Pete. Testeo de Solicitud. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 40

[6] HERZOG, Pete. Testeo de las Personas Confiables. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 42

[7] HERZOG, Pete. Exploración de Red. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 47 48

4.1.1.7 Identificación de los Servicios del Sistema.

En este módulo se deben enumerar los servicios de internet activos o accesibles, así como traspasar el firewall con el fin de encontrar más servidores activos, la idea es escanear los puertos y así identificar cuales están abiertos, las tareas a realizar en este módulo son: Recoger respuestas de Broadcast desde la red, intentar traspasar el firewall, emplear ICMP, utilizar intento de conexión al DNS los servidores de red, escanear puertos para enumerar puertos abiertos y cerrados, verificar el tráfico y protocolos de enrutamiento e identificar los servicios relacionados con cada puerto[8].

4.1.1.8 Búsqueda de Información Competitiva.

Se refiere a la búsqueda de información las tareas a realizar en este módulo son: Realizar un mapa y medir la estructura de directorio de los servidores web y FTP, examinar la base de datos WHOIS para los servicios de negocio, determinar el costo de soporte de la infraestructura, registrar los productos que se están vendiendo desde las aplicaciones web, identificar los clientes y socios del negocio.[9]

4.1.1.9 Obtención de Documentos.

Aquí se verifica la información testeada y perteneciente a los niveles de seguridad de la información, con el fin de definir perfiles, las tareas a realizar en este módulo son: Examinar las bases de datos, levantar información de personas clave en la organización como direcciones email, datos laborales por niveles tecnológicos.[10]

4.1.1.10 Búsqueda y Verificación de Vulnerabilidades.

En este módulo se identifica, comprende y verifica las debilidades, y vulnerabilidades en servidores o redes, las tareas a realizar en este módulo son: Integrar las pruebas con herramienta de hacking y exploits, determinar vulnerabilidades de las aplicaciones y sistemas operativos, realizar exploits para descartar falsos positivos y negativos.[11]

---

[8] HERZOG, Pete. Identificación de los Servicios del Sistema. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 49 50

[9] HERZOG, Pete. Búsqueda de Información Competitiva. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 51

[10] HERZOG, Pete. Obtención de Documentos. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 54

[11] HERZOG, Pete. Búsqueda y Verificación de Vulnerabilidades. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 55

4.1.1.11 Testeo de Aplicaciones de Internet.

En este módulo se emplean técnicas de testeo para encontrar fallos de seguridad, las tareas a realizar en este módulo son: explorar combinaciones de contraseñas por fuerza bruta, saltarse sistemas de autenticación, determinar limitaciones de los controles de acceso de las aplicaciones, determinar la información de sesiones en la red, inyectar falsa información con técnicas de hijacking, examinar vulnerabilidades "Cross-Site Scriping" en las aplicaciones web.[12]

4.1.1.12 Enrutamiento.

Este módulo está diseñado para asegurar que las políticas de seguridad ACL dejen pasar los paquetes permitidos por medio del router de la DMZ, las tareas a realizar en este módulo son: Verificar el tipo de router que se maneja, y si está dando servicio de NAT, testear la ACL del router, verificar si el router está filtrando el tráfico de la red y si está detectando direcciones falsas.[13]

4.1.1.13 Testeo de Sistemas Confiados.

El propósito de este módulo es afectar la presencia en internet mostrándose como una entidad de confianza en la red, las tareas a realizar en este módulo son: Verificar que los sistemas y las aplicaciones puedan ser engañadas.[14]

4.1.1.14 Testeo de Control de Acceso.

Este módulo está diseñado para asegurar que solo este permitido lo que debe ser aceptado en la red, las tareas a realizar en este módulo son: Obtener información del firewall y sus características, obtener perfiles de políticas de seguridad en la red, listar los tipos de paquetes que deben entrar a la red, tipos de protocolos con accesos y puertos con accesos.[15]

---

[12] HERZOG, Pete. Testeo de Aplicaciones de Internet. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 56 57

[13] HERZOG, Pete. Enrutamiento. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 58

[14] HERZOG, Pete. Testeo de Sistemas Confiados. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 59

[15] HERZOG, Pete. Testeo de Control de Acceso. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 60 61

4.1.1.15 Testeo de Sistema de Detección de Intrusos.

Está orientado al rendimiento del IDS, las tareas a realizar en este módulo son: Verificar tipo de IDS, testear los estados de alarma y configuraciones, listar falsos positivos y rutas no monitorizadas.[16]

4.1.1.16 Testeo de Medidas de Contingencia.

Las tareas por realizar en este módulo son: Verificar las propiedades del sistema de contingencia, identificar las medidas de contingencia de Escritorio y sus debilidades y listar los recursos de contingencia.[17]

4.1.1.17 Descifrado de Contraseñas.

Radica especialmente en obtener acceso a sistemas y determinar las políticas de generación de contraseñas para poder recomendar su mejora, las tareas a realizar en este módulo son: Obtención de ficheros de contraseñas del servidor, arranque de ataques automatizados de fuerza bruta al fichero de contraseñas, utilizar las contraseñas obtenidas para acceder a las aplicaciones y obtener la edad de las contraseñas.[18]

4.1.1.18 Testeo de Denegación de Servicios.

Las tareas por realizar en este módulo son: Listar puntos débiles a través de internet, comprobar restricciones de los sistemas expuestos en la red y listar cuales sistemas son vulnerables a ataques DoS.[19]

4.1.1.19 Evaluación de Políticas de Seguridad.

Consiste en evaluar las políticas actuales de la organización, las tareas a realizar en este módulo son: Verificar que esté aprobada por la alta gerencia, garantizar que la política está correctamente almacenada y que el personal de la organización la conoce y cotejar que las medidas de seguridad se cumplan.[20]

---

[16] HERZOG, Pete. Testeo de Sistema de Detección de Intrusos. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 62

[17] HERZOG, Pete. Testeo de Medidas de Contingencia. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 63

[18] HERZOG, Pete. Descifrado de Contraseñas. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 64

[19] HERZOG, Pete. Testeo de Denegación de Servicios. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 65

[20] HERZOG, Pete. Evaluación de Políticas de Seguridad. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 66

La sección D comprende Seguridad en las Comunicaciones y posee los módulos de:

4.1.1.20 Testeo de PBX.

Método para lograr acceso a la central telefónica, las tareas a realizar en este módulo son: Revisar detalles de llamadas en busca de sospechas de abuso, asegurarse de que las cuentas administrativas no tengan contraseñas por defecto, verificar que el sistema operativo este actualizado, testear autenticación local y remota de llamadas entrantes.[21]

4.1.1.21 Testeo del Modem.

Este método sirve para enumerar los módems, las tareas a realizar en este módulo son: Escanear central de módems, asegurar que el sistema esté actualizado.[22]

La sección F comprende la Seguridad Física y posee los módulos de:

4.1.1.22 Revisión de Perímetro.

Este método evalúa la seguridad física de la organización verificando el perímetro físico, las tareas a realizar en este módulo son: crear mapa del perímetro físico con sus medidas de protección como puertas y cercas, de igual forma las rutas de acceso y las áreas no monitoreadas. [23]

4.1.1.23 Revisión de monitoreo.

Método para descubrir puntos de acceso monitoreados mediante la realización de mapas y listados de dispositivos de monitoreo. [24]

4.1.1.24 Evaluación de Controles de Acceso.

Método para evaluar privilegios de acceso por medio de puntos físicos, se centra en examinar las áreas de control de acceso, determinar niveles de complejidad y privacidad de los dispositivos de control de acceso.

---

[21] HERZOG, Pete. Testeo de PBX. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 69

[22] HERZOG, Pete. Testeo del Modem. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 72

[23] HERZOG, Pete. Revisión de Perímetro. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 91

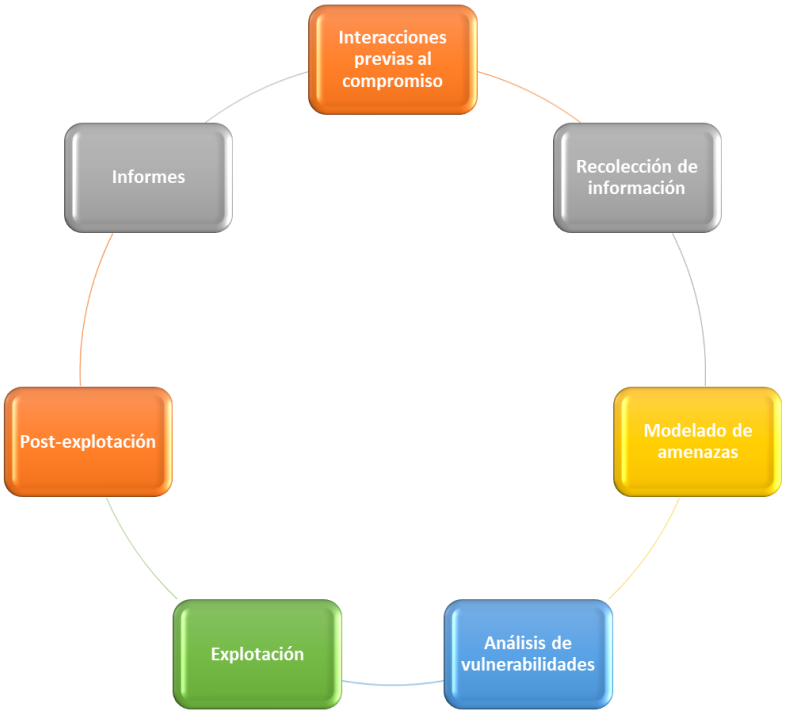
[24] HERZOG, Pete. Revisión de monitoreo. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 92

Es importante resaltar que esta metodología brinda a los auditores ciertos formatos y plantillas de informes acordes para la realización de toda la labor de auditoría." [25]

4.1.2 PTES (Penetration Testing Execution Standart)

"Esta metodología consta de siete secciones, éstas abarcan todo lo relacionado con las pruebas de penetración que se manejan hoy en día, desde la planeación inicial hasta la obtención de un informe concienzudo que sea acorde a las labores realizadas y genere valor a las organizaciones."[26]

Ilustración 2. Fases PTES.



Fuente: El autor.

4.1.2.1 Interacciones previas al compromiso.

"Se definen los alcances de la planeación de la auditoria, en esta fase se realizan las reuniones de apertura, la generación de las contrataciones, firmas de

[25] HERZOG, Pete. Evaluación de Controles de Acceso. En: OSSTMM 2.1. Manual de la Metodología abierta de Testeo de Seguridad. 2003. p. 93

[26] The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Main_Page

documentos de confiabilidad y tiempos de las actividades. Esta fase define formularios con una serie de preguntas relacionadas con el diagnóstico inicial y las categoriza de acuerdo con temas como: Pruebas de penetración de red, de aplicaciones web, de red inalámbrica, penetración física, ingeniería social, enfocadas a la alta gerencia y administradores de sistemas, servicios en la nube, ubicaciones geográficas de los servidores. De igual forma se establecen líneas de comunicación y procedimientos de notificación de incidentes."[27]

4.1.2.2 Recolección de información.

"Esta sección está enfocada en recolectar la mayor cantidad de información para ser utilizada en futuras fases, se usan técnicas de reconocimiento pasivo, semipasivo y activo y se obtiene documentación pertinente de la organización. Es necesario hacer un diagnóstico de la organización objetivo a través de información pública antes de formalizar la contratación, luego del anterior paso se evalúan la información recibida y se emprende investigación por medio de ingeniería social, entre lo que debe estar: ubicación física, relaciones comerciales, razón social, tipos de clientes, competidores, productos ofrecidos, ofertas laborales ofrecidas, estructura organizacional, activos de infraestructura, posición en internet, dominios de correo electrónico.

Es importante resaltar que existe información de la organización que se puede extraer de servidores WHOIS, es necesario ubicar el servidor adecuando que contenga lo que se está buscando, los servidores de búsqueda más adecuados son: ICANN (http://www.icann.org), IANA (http://www.iana.com), NRO (http://www.nro.net), AFRINIC (http://www.afrinic.net), APNIC (http://www.apnic.net), ARIN (http://ws.arin.net), LACNIC (http://www.lacnic.net), RIPE (http://www.ripe.net).

De igual forma se puede obtener un diagnóstico de la infraestructura centrándose en servicios de directorio activo, sitios de intranet, aplicaciones internas empresariales, segmentos de red y mapeo de redes, se puede saber que aplicaciones web están instaladas, detectar y enumerar hosts virtuales, descubrir DNS, identificar umbrales de bloqueo en los servicios de autenticación e identificar mecanismo de protección."[28]

[27] Pre-engagement - The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Pre-engagement

[28] Intelligence Gathering - The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Intelligence_Gathering

4.1.2.3 Modelado de amenazas.

“Con el fin de determinar un modelo de amenazas en la organización es necesario enfocarse en los activos y los procesos empresariales y, en los atacantes y sus privilegios.

Una vez se obtienen los activos de la organización, el pentester o auditor puede identificar cuáles de estos tienen mayor probabilidad de ser atacados, cuál es su valor y cuál sería el impacto de su perdida.

Identificar el proceso empresarial es un punto importante puesto que por medio de este es como gana dinero la organización, en caso de un ataque o vulneración se generaría perdida y por esto es parte importante del modelado de amenazas.

Cuando se desea perfilar un atacante dentro del modelado de amenazas es importante evaluar una serie de clasificaciones de acuerdo a los privilegios y cercanías con la organización, a nivel interno se perfilarán los empleados y sus niveles de habilidad con los sistemas informáticos, personal del área de sistemas y usuarios flotantes como lo son contratistas, proveedores, de igual forma se evalúan las posibles amenazas que puede generar la competencia desleal de los competidores o hacktivistas y/o crimen organizado.

Al final de la evaluación de esta fase se generará un análisis de la capacidad del posible atacante, de su accesibilidad a la organización y los activos más importantes que pueden ser vulnerados.”[29]

4.1.2.4 Análisis de vulnerabilidades.

“En esta fase se realiza el proceso de descubrimiento de fallas en los sistemas y las aplicaciones, las cuales pueden ser aprovechadas por el atacante. Se deben realizar pruebas activas como lo son exploración de puertos, escaneos a los servicios, escaneos a las aplicaciones web, generar listados de directorios, verificar versiones de servidores web, escaneo de la segmentación de redes VoIP; De igual forma se deben realizar pruebas pasivas como el análisis de metadatos, monitoreo de trafico de red, políticas de correo electrónico y políticas de seguridad.”[30]

[29] Threat Modeling - The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Threat_Modeling

[30] Vulnerability Analysis - The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Vulnerability_Analysis

4.1.2.5 Explotación.

“Es la prueba de penetración a los sistemas de acuerdo lo descubierto en la fase de análisis de vulnerabilidades. Existen varios tipos de explotaciones y el auditor definirá bajo su experticia cuales puede o no usar, algunos de ellos son: Desbordamiento de búfer, sobreescritura del SEH (Manejo Estructurado de Excepciones), Análisis de tráfico, ingeniería social, acceder maquinas remotamente, Ataques a la red WiFi.”[31]

4.1.2.6 Post-explotación.

“La intención de esta fase es determinar el valor de las maquina explotadas y el mantenimiento del control de ellas. El valor está determinado por la sensibilidad de la información allí almacenada. Es necesario seguir las reglas de los compromisos acordados con la organización y si estas no se abarcaron en su totalidad es necesario que se tengan en cuenta, por ejemplo:

- Protección del cliente: Garantizar la correcta operación del negocio a menos de que se tenga el aval de bajarlos por un tiempo determinado, los cambios generados sobre las maquinas se deben documentar y después de finalizar el proceso se deben restaurar las configuraciones originales, no incluir contraseñas o datos sensibles en los informes, los datos recopilados se deben destruir una vez se entregue el informe final.

- Autoprotección: Obtener copia de las políticas de seguridad actuales de la organización, verificar regulaciones gubernamentales que rigen la información administrada por el cliente.

Al analizar la infraestructura se debe tener en cuenta las configuraciones e interfaces de red y la identificación de servidores DNS, de igual forma es necesario identificar los servicios que corren a través de la red. Se debe hacer una evaluación del software de las máquinas de la organización con el fin de detectar posibles servicios malintencionados que se suben de manera automática cuando inicia el sistema operativo de la máquina, se debe realizar escaneo de herramientas de bases de datos que apuntan a servidores, listar objetos de los directorios activos y maquinas virtualizadas. Identificar servicios o software de mensajería, sistemas de monitoreo, sistemas de respaldo.”[32]

[31] Exploitation - The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Exploitation

[32] Post Exploitation - The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Post_Exploitation

4.1.2.7 Informes.

“Se debe realizar un informe final que permita un alto nivel de compresión a la alta gerencia. El informe se debe estructurar en dos secciones sintetizando los objetivos, los métodos y los resultados de la labor realizada. Se debe iniciar con un resumen ejecutivo que contenga el objetivo general de la prueba realizada, seguidamente clasificar en una escala los riesgos por medio de puntuaciones, y dar las conclusiones por medio de hallazgos que indiquen cuales son los problemas encontrados, se debe tener en cuenta la generación de graficas estadísticas que permitan al lector dar un mejor entendimiento del informe, se deben dar las respectivas recomendaciones indicando las tareas a realizar para disminuir los riesgos de ataques y bajo un sistema de priorización según las vulnerabilidades encontradas. La segunda sección del informe indicará un reporte técnico que dé los detalles de la prueba realizada y que abarque todos los aspectos acordados, se debe iniciar mostrando un listado de actividades a realizar y sus involucrados, se debe dar de forma detallada lo encontrado en la fase de Obtención de Información y en el análisis de vulnerabilidades, seguidamente se debe demostrar el cumplimiento del cronograma de actividades con evidencias encontradas en la fase de explotación y finalizar con las conclusiones enfocándose en gran medida en el fortalecimiento de la seguridad de la información.” [33]

4.1.3 CEH (Certified Ethical Hacker)

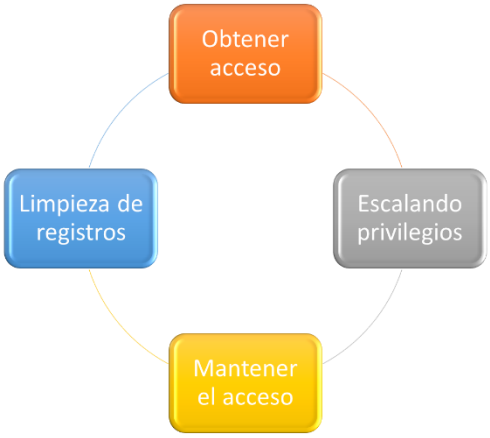
“Permite efectuar pruebas de seguridad abarcando un proceso de auditoria completo, evaluando riesgos y vulnerabilidades, y aplicando variedad de herramientas necesarias para la labor.

Consta de 4 fases o etapas indispensables para su correcto desarrollo”[34]

[33] Reporting - The Penetration Testing Execution Standard. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en http://www.pentest-standard.org/index.php/Reporting

[34] EC-Council, Certified Ethical Hacker. [Sitio web]. Programa de capacitación para Certified Ethical hacker [Consulta: 03 julio 2021]. Disponible en https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Ilustración 3. Fases CEH.



Fuente: El autor.

4.1.3.1 Obtener acceso y Escalar Privilegios.

En esta fase inicial se establece comunicación inicial con la organización y se realiza el inicio de las actividades comenzando el diligenciamiento de documento de confidencialidad, se solicitan permisos por escrito, se definen fechas y cronograma de ejecución de las actividades, se determinan alcances y objetivos de la auditoría, con el fin de obtener accesos se recurre a técnicas de reconocimiento pasivo y activo.

Cuando se habla de un reconocimiento pasivo nos referimos a la recolección de información del cliente sin necesidad de que se entregada por él, es decir, recolectar información que se encuentra al público por medio de su portal web, redes sociales, directorios en internet, realizando ingeniería social o hasta recuperándola de los basureros.

Si no referimos al reconocimiento activo tocamos el punto de la interacción directa con el cliente donde ya se puede sondear la red para describir hosts ocultos o públicos, ip's, servicios que se corren en la red, y hasta la existencia de un firewall, de igual forma la ingeniería social aplica dentro de esta subfase para poder obtener información confidencial a la cual está expuesto el cliente.

Una vez se ha recolectado la información procede a examinar a profundidad la red por medio de: port scanners, network mappers, sweepers y vulnerability scanners, del mismo modo existen herramientas de fácil acceso y comúnmente utilizadas tenemos nmap, Nexpose, Nessus y OpenVAS. No se debe olvidar que la enumeración en esta fase es tan importante como el uso de las demás herramientas y consiste en obtener el listado de cuentas de usuarios, listado de máquinas, listado de recursos compartidos e identificadores de seguridad.

Con esta exploración se pretende identificar o diagnosticar cualquier información que ayude a realizar o perpetrar el ataque analizando las posibles fallas de seguridad, por ejemplo, IP's, nombres de equipos en la red, cuentas de usuario, software instalado puertos abiertos, host's ocultos.[35]

4.1.3.2 Mantener el Acceso.

Durante esta fase se realiza el hackeo a los sistemas, el objetivo es poder explotar las vulnerabilidades descubiertas en las fases anteriores, con lo anterior tendremos un acceso total a las maquinas sin que el usuario pueda detectarlo.

La idea es realizar la ejecución de exploits manuales o automáticos según prefiera el White hacker, entiéndase automáticos como el uso de herramientas desarrolladas por terceros; la herramienta Metasploit Framework viene dentro de la librería del sistema Operativo Kali Linux y es la herramienta idónea para realizar la explotación de las vulnerabilidades permitiendo crear espacios de trabajo diferenciados en caso de que se esté realizando el hacking ético a demás entidades.

De igual forma no solo el Metasploit Framework nos puede ayudar a explotar las vulnerabilidades en un sistema, existen herramientas de ataque basados en diccionarios para descubrir claves, captura de claves usando sniffers de red, ataques de denegación de servicios, death ping's, ataques MITM (Hombre en el Medio), Inyeccion de Malware, etc.

Es importante saber que el objetivo es determinar vulnerabilidades y atacarlas de una forma objetiva y bajo la ética que corresponde, por esto mismo en esta fase se debe realizar el trabajo de la misma forma como si un atacante lo realizara por esto es necesario crear puertas traseras dentro de los sistemas atacados con el fin de poder realizar accesos de manera constante.

Dentro del acuerdo inicial se abordó el tema del tiempo y el alcance del servicio por lo cual se requiere mantener el acceso a las maquinas hackeadas (auditadas) con el fin de saber en qué momentos el usuario atacante y el que está provocando el hueco de información está realizando su labor.

Una vez se realiza el descubrimiento del ataque, los medios y las herramientas utilizadas se indaga historial de comandos utilizados, listado de archivos eliminados, traza de correos electrónicos recibidos y enviados se efectúa una técnica de camuflaje para cubrir huellas dentro de los sistemas hackeados para así poder

[35] The Ultimate Ethical Hacking Methodology Explained. [Sitio web]. Gaining Access, Escalating Privileges [Consulta: 30 noviembre 2021]. Disponible en https://www.linkedin.com/pulse/ultimate-ethical-hacking-methodology-explained-majed-alshodari/

monitorear al intruso. Una vez se descubra la intrusión y las vulnerabilidades se procede a finalizar el Ethical Hacking y a generar los respectivos informes.[36]

4.1.3.3 Limpieza de Registros.

En esta fase se pretende que el hacker se retire sin dejar huellas y para esto intenta ocultar o eliminar todas las pistas que pueda con el fin de nos ser descubierto por el profesional de seguridad TI"[37]

4.2. MARCO CONCEPTUAL

Test de Penetración: "Consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando. Estas pruebas comprenden desde el análisis de dispositivos físicos y digitales, hasta el análisis del factor humano utilizando Ingeniería Social. El objetivo de estas pruebas es verificar bajo situaciones extremas cuál es el comportamiento de los mecanismos de defensa, específicamente, se busca detectar vulnerabilidades en los mismos. Además, se identifican aquellas faltas de controles y las brechas que pueden existir entre la información crítica y los controles existentes."[38]

Hacking Ético: "Es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.[39]

Vulnerabilidad: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible."[40]

---

[36] The Ultimate Ethical Hacking Methodology Explained. [Sitio web]. Maintaining Access [Consulta: 30 noviembre 2021]. Disponible en https://www.linkedin.com/pulse/ultimate-ethical-hacking-methodology-explained-majed-alshodari/

[37] The Ultimate Ethical Hacking Methodology Explained. [Sitio web]. Clearing Logs, Escalating Privileges [Consulta: 30 noviembre 2021]. Disponible en https://www.linkedin.com/pulse/ultimate-ethical-hacking-methodology-explained-majed-alshodari/

[38] WeLiveSecurity. [Sitio web]. Penetration Test, ¿en qué consiste?. [Consulta: 03 julio 2021]. Disponible en https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

[39] Hacking ético. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en https://www.internetglosario.com/1131/Hackingetico.html

[40] Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Sitio web]. [Consulta: 03 julio 2021]. Disponible en https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Confidencialidad, Integridad y Disponibilidad: "Pilares fundamentales para el Sistema de Gestión de Seguridad de la Información según la ISO 27001."[41]

Defense in Depth: El concepto básico de la defensa en profundidad o DiD se basa en el establecimiento de barreras de defensa contra ataques e intrusiones, donde la estrategia indica que si la primera barrera es violada o traspasada la segunda tendrá que parar el ataque, y si la segunda es traspasada, la tercera trabajará en lugar de ella, y así sucesivamente, existen muchos conceptos para generar una buena práctica de establecimiento de defensa de profundidad pero cada una de las estrategias se debe adaptar a las necesidades de la organización, por ejemplo, no es lo mismo establecer una defensa en profundidad en un café internet que en un organización gubernamental.[42]

Black Hackers: Hoy en día se habla del término Crakers o Black Hat Hackers (Hackers de Sombrero Negro) referenciando a los usuarios criminales señalados de hacer intrusión en sistemas sin permiso, realizar ataques, robar información e identidades, son los responsables de todo el spam que recibimos en el correo electrónico, son los que crean los virus malware, etc. buscando un beneficio personal y económico.

El actuar de ellos se basa generalmente en una serie de pasos:

Reconocimiento→ Recolección de Información del posible blanco de ataque, generalmente lo hacen por medio de buscadores en internet y/o acercándose a la empresa blanco a realizar ingeniería social.

Exploración→ Es tomar la información recolectada y empezar a realizar ataques a la red por medio de scanners de puertos, mapeadores de red y algunas otras herramientas que puedan arrojar información sensible del blanco y que ayude a perpetrar un ataque.

Ganando Acceso→ Es la fase del Hackeo e intrusión después de conocer las posibles vulnerabilidades.

Manteniendo el acceso→ Una vez han perpetrado el ataque crean puertas traseras que garanticen el ingreso al sistema en futuras ocasiones.

---

[41] ISO 27001: Pilares fundamentales de un SGSI. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

[42] Defensa en profundidad. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en https://www.ciberseguridadlogitek.com/estrategia-de-defensa-en-profundidad-en-ciberseguridad-industrial/

Cubriendo las huellas→ Una vez se tiene el acceso a los sistemas atacados, el Black Hacker elimina los rastros del ataque (log's del servidor, historial de comandos, alarmas de detección de intrusos, etc.) dejando las puertas traseras abiertas o troyanos que le permitan ingresar de nuevo sin que el personal de seguridad de la red se entere; los rastros se pueden referir.[43]

White Hackers: Conocidos también como Ethical Hackers o White Hat hackers (Hackers de Sombrero Blanco) son aquellos que trabajan de forma profesional como Crackers con la diferencia que su intrusión es avalada por el dueño del sistema y busca evidenciar vulnerabilidades sin afectar los servicios, estudiarlos y corregir las fallas, todo dentro de la legalidad.

Al igual que los Balck Hackers, el actuar de un White Hacker se basa generalmente en una serie de pasos:

Reconocimiento→ Recolección de información activa a través de Sniffer, detección de IP's puertos de salida a internet, servidores y redes ocultas con el fin de verificar vulnerabilidades.

Escaneo→ De acuerdo a los privilegios otorgados por el contratante si realiza un sondeo por medio de herramientas desarrolladas para tal fin: Nmap, Nessus, Snort, NSlookup, Tracert, etc. Es el trabajo de campo previo al hacking ético para empezar a realizar un diagnóstico y detectar cuales son las posibles fallas en la seguridad y por donde podría ingresar un intruso.

Hacking→ Es cuando se han obtenido las vulnerabilidades de los sistemas explorados y se procede a realizar el hacking ético por medio de herramientas avanzadas, la más conocida es Metasploit Framework que corre bajo el sistema operativo Kali Linux.

Informe Final→ Documento descriptivo del trabajo realizado donde de indican las vulnerabilidades, las conclusiones y las recomendaciones correspondientes.[44]

Riesgo informático: Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas.[45]

---

[43] Black Hacker. [Sitio web]. Sombrero negro. [Consulta: 03 julio 2021]. Disponible en https://www.ictea.com/cs/index.php?rp=/knowledgebase/2089/iQue-es-un-andsharp039hackerandsharp039.html

[44] White Hacker. [Sitio web]. Sombrero blanco. [Consulta: 03 julio 2021]. Disponible en https://www.ictea.com/cs/index.php?rp=/knowledgebase/2089/iQue-es-un-andsharp039hackerandsharp039.html

[45] Riesgo Informático. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en https://www.gb-advisors.com/es/riesgos-de-seguridad-que-factores-ponen-en-peligro-tu-entorno-de-ti/

Backdoors: Es una fisura en el sistema que crea un atacante y aprovecha para su beneficio, se podría decir que es un agujero en el sistema de seguridad del ordenador con el fin de poder tomar el control o espiar la maquina atacada.[46]

4.3. MARCO LEGAL

Ley 1273 de 2009

Dentro de la legislación y normatividad vigente se tiene la ley 1273 de 2009 que condena los delitos desde multas monetarias de entre 100 y 1000 salarios mínimos legales vigentes hasta penas de prisión de entre 48 y 96 meses, dependiendo de la gravedad.

El articulado referente a los delitos informáticos se concentra en:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Articulo 269I: hurto por medios informáticos y semejantes.[47]

Ley 527 de 1999

“Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación”[48]

---

[46] Puerta trasera. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en https://www.welivesecurity.com/la-es/2015/04/17/que-es-un-backdoor/

[47] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1273 de 2009. (05, enero, 2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Enero, 2009. Nro. 47223.

[48] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 527 de 1999. (18, agosto, 1999) Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. En: Diario Oficial. Agosto, 1999. Nro. 43673.

Ley 679 de 2001

"Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores."[49]

Ley 1266 de 2008

"Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países."[50]

Ley 1341 de 2009

"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro."[51]

5. DESARROLLO DE LA PROPUESTA

De acuerdo con los objetivos planteados se da inicio con la demostración de cada una de las fases que componen las metodologías de hacking ético escogidas destacando que fue realizado bajo ambientes controlados con la única finalidad de no incurrir en ninguna falta legal ni exposición de datos reales que puedan afectar el buen nombre de alguna empresa u organización, a continuación, se da solución al objetivo específico número dos:

5.1. Alistamiento de máquinas

Se han aprovisionado algunas máquinas virtuales con diferentes sistemas operativos que permitirán realizar las prácticas:

[49] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 679 de 2001. (04, agosto, 1999) Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. En: Diario Oficial. Agosto, 2001. Nro. 44509.

[50] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1266 de 2008. (31, diciembre, 2008) Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. En: Diario Oficial. Agosto, 2008. Nro. 47219.

[51] COLOMBIA, CONGRESO DE LA REPUBLICA, Ley 1341 de 2009. (30, julio, 2009) Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. En: Diario Oficial. Julio, 2009. Nro. 47429.

5.1.1. Kali Linux

Es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información.[52]

5.1.2. Ubuntu

Es una distribución GNU/Linux que ofrece un sistema operativo para equipos de escritorio y servidores. Es una distribución basada en Debian.[53]

5.1.3. Windows

Es un sistema operativo desarrollado por Microsoft con interfaz gráfica basada en ventanas y con licenciamiento pago. Es el sistema operativo más utilizado en el mundo.[54]

5.2 Interacciones previas al compromiso (PTES)

Esta fase arranca justo después de que se ha firmado el compromiso contractual con la organización y es donde se inicia la labor de exposición del plan de trabajo, indicando alcances, tiempos y entregables, y se firman las respectivas cláusulas de confidencialidad.

De igual forma, en esta fase es importante tener en cuenta la ejecución de un diagnóstico inicial de la organización con el fin de poder encontrar hallazgos y encaminar el proyecto de acuerdo con lo evidenciado, para esto se puede utilizar la plantilla de Auditoría Inicial expuesto en el Anexo 1.

5.3 Recolección de información – Exploración - Análisis de vulnerabilidades (PTES-CEH-OSSTMM)

5.3.1 Reconocimiento pasivo

Este reconocimiento permite recolectar información del potencial blanco sin interactuar directamente con sus sistemas de información, servidores y demás elementos.

---

[52] KALI LINUX. [Sitio web]. [Consulta: 03 julio 2021]. Disponible en https://www.kali.org/

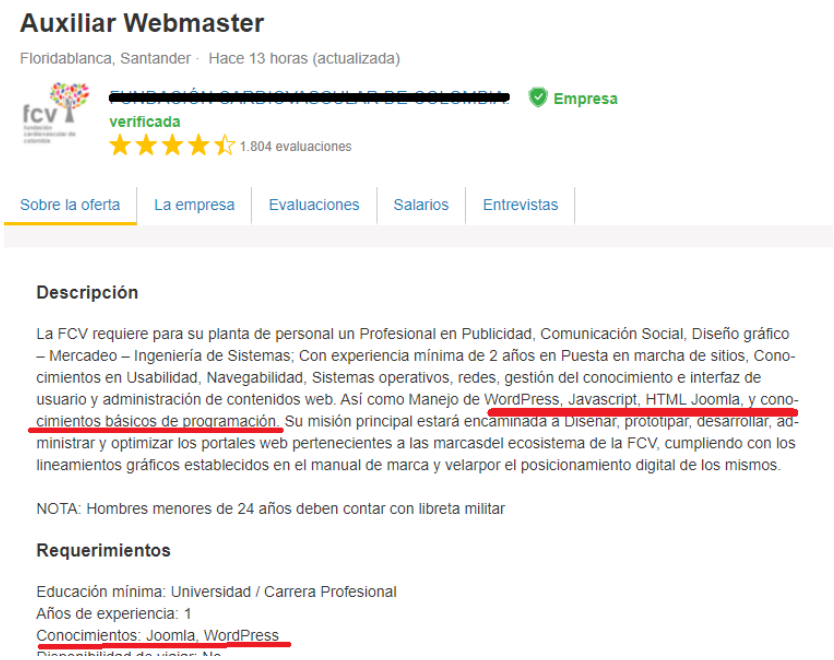
[53] UBUNTU. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/ciudadania-y-seguridad-tic/principios-legales/software-libre/ubuntu-linux/

[54] WINDOWS. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en https://softwarelab.org/es/windows-historia/

Con el fin de demostrar un reconocimiento pasivo se relacionan a continuación ejemplos y casos prácticos:

- Realizar búsqueda en portales de empleo donde se ofrezca algún puesto relacionado con los departamentos de sistemas; en el siguiente ejemplo podemos observar como una empresa del sector salud requiere personal con conocimientos en WordPress y Joomla por lo que podríamos deducir que sus Webserver se basan en un publicador Apache o Nginx y que sus aplicaciones web están soportadas en los motores de base de datos MySQL o MariaDB lo que nos permite indagar sobre sus vulnerabilidades y empezar a idear estrategias de penetración.[55]

Ilustración 4. Portal de empleo con información sensible.



Fuente: https://www.computrabajo.com.co/trabajo-de-webmaster.

- Consultar información de los dominios en internet por medio de portales web especializados como lo son: https://whois.co/ o https://www.robtex.com/, allí podremos saber a qué nombre está registrado el dominio, a qué IP se puede estar conectando el DNS, rangos de IP's publicas asignadas y en algunos casos podremos obtener información personal de la persona que registró el dominio. Es posible pagar para mantener esta información privada, pero muchas organizaciones que adquieren un nombre de dominio no contratan

[55] Requerimientos instalación WordPress. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en https://es-co.wordpress.org/about/requirements/

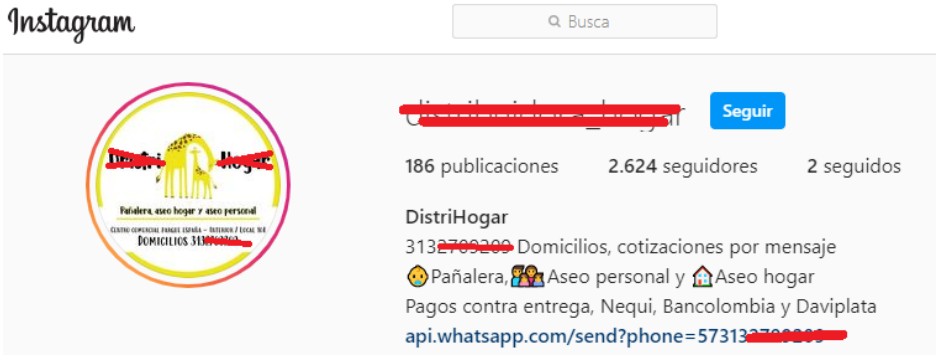
el servicio de privacidad de información por lo que esta técnica de reconocimiento es útil.

Ilustración 5. Búsqueda WhoIs.

Fuente: https://whois.co/whois-gui/

- Las empresas en la actualidad buscan incrementar su cobertura y captar variedad de clientes por lo que han incursionado en el uso de redes sociales, allí es donde se puede recolectar información importante de una forma rápida y gratuita que pueden ser usadas en un ataque de ingeniería social. Con el siguiente ejemplo podemos evidenciar la exposición de números telefónicos amarrados a los medios de pago.

Ilustración 6. Red Social con información sensible.



Fuente: (https://www.instagram.com/distrihogar/?hl=es.

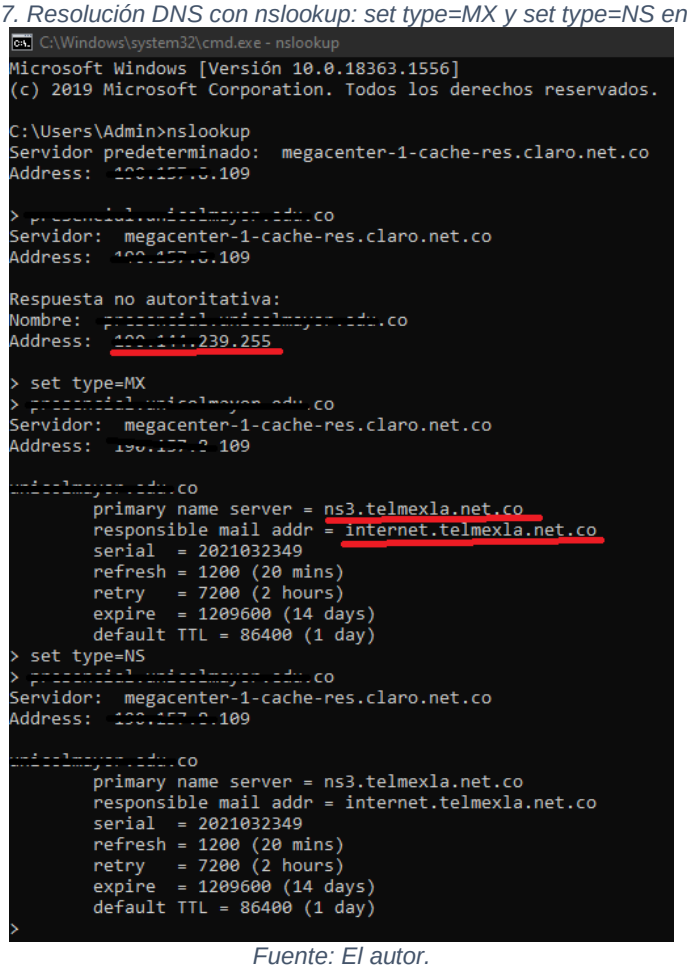
5.3.2 Reconocimiento activo

Este reconocimiento se caracteriza por tener una interacción directa con el objetivo y es altamente confiable puesto que podremos evidenciar sistemas operativos, puertos, servicios, etc.

5.3.2.1 nslookup

Una vez se identifica el portal web de la víctima se procede con la ejecución del comando nslookup para la identificación de la ip del servidor que lo soporta, se puede verificar el servidor de hosting donde se aloja y el servidor de correo:

Ilustración 7. Resolución DNS con nslookup: set type=MX y set type=NS en Windows.

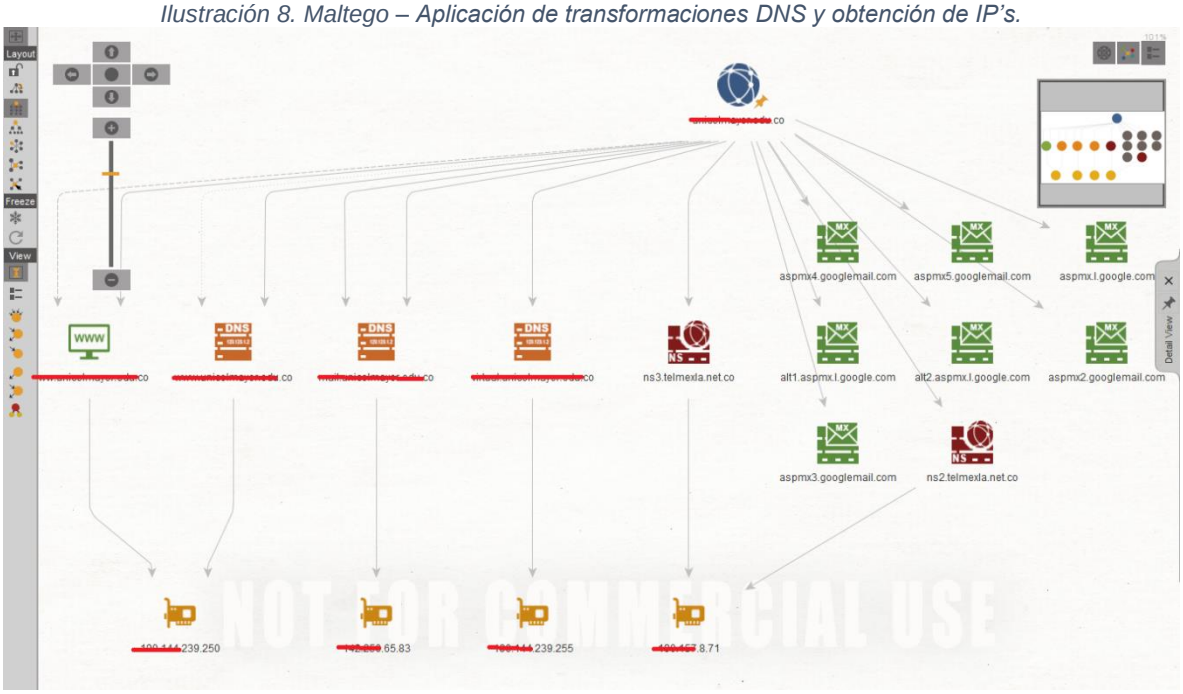


Fuente: El autor.

5.3.2.2 Maltego

Esta herramienta permite mostrar de forma gráfica información sobre organizaciones, personas, portales web, entre otros.[56]

Ilustración 8. Maltego – Aplicación de transformaciones DNS y obtención de IP's.



Fuente: El autor.

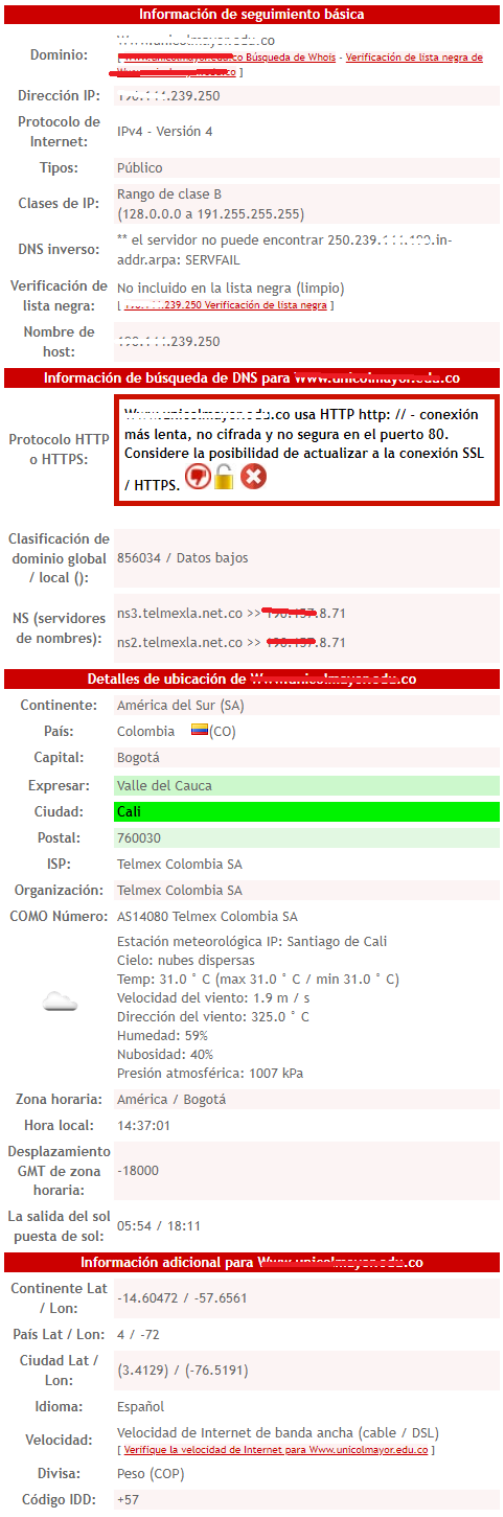
5.3.2.3 Rastreo de IP

Al conocer la(s) IP('s) del potencial blanco es posible obtener la ubicación geográfica de los servidores logrando deducir si estos están almacenados en un datacenter externo o sus propias locaciones.[57]

[56] Maltego. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en http://www.osintux.org/documentacion/maltego

[57] ip tracker. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en https://www.ip-tracker.org/

Ilustración 9. ip-tracker-Rastreo de IP.



Información de seguimiento básica	
Dominio:	[redacted].co [redacted].co Búsqueda de Whois - Verificación de lista negra de [redacted].co]
Dirección IP:	[redacted].239.250
Protocolo de Internet:	IPv4 - Versión 4
Tipos:	Público
Clases de IP:	Rango de clase B (128.0.0.0 a 191.255.255.255)
DNS inverso:	** el servidor no puede encontrar 250.239.[redacted].in-addr.arpa: SERVFAIL
Verificación de lista negra:	No incluido en la lista negra (limpio) [[redacted].239.250 Verificación de lista negra]
Nombre de host:	[redacted].239.250

Información de búsqueda de DNS para [redacted].co	
Protocolo HTTP o HTTPS:	[redacted].co usa HTTP http: // - conexión más lenta, no cifrada y no segura en el puerto 80. Considere la posibilidad de actualizar a la conexión SSL / HTTPS.
Clasificación de dominio global / local ():	856034 / Datos bajos
NS (servidores de nombres):	ns3.telmexla.net.co >> [redacted].8.71 ns2.telmexla.net.co >> [redacted].8.71

Detalles de ubicación de [redacted].co	
Continente:	América del Sur (SA)
País:	Colombia (CO)
Capital:	Bogotá
Expresar:	Valle del Cauca
Ciudad:	Cali
Postal:	760030
ISP:	Telmex Colombia SA
Organización:	Telmex Colombia SA
COMO Número:	AS14080 Telmex Colombia SA
	Estación meteorológica IP: Santiago de Cali Cielo: nubes dispersas Temp: 31.0 ° C (max 31.0 ° C / min 31.0 ° C) Velocidad del viento: 1.9 m / s Dirección del viento: 325.0 ° C Humedad: 59% Nubosidad: 40% Presión atmosférica: 1007 kPa
Zona horaria:	América / Bogotá
Hora local:	14:37:01
Desplazamiento GMT de zona horaria:	-18000
La salida del sol puesta de sol:	05:54 / 18:11

Información adicional para [redacted].co	
Continente Lat / Lon:	-14.60472 / -57.6561
País Lat / Lon:	4 / -72
Ciudad Lat / Lon:	(3.4129) / (-76.5191)
Idioma:	Español
Velocidad:	Velocidad de Internet de banda ancha (cable / DSL) [Verifique la velocidad de Internet para Www.unicolmayor.edu.co]
Divisa:	Peso (COP)
Código IDD:	+57

Fuente: https://www.ip-tracker.org/.

5.3.2.4 nmap

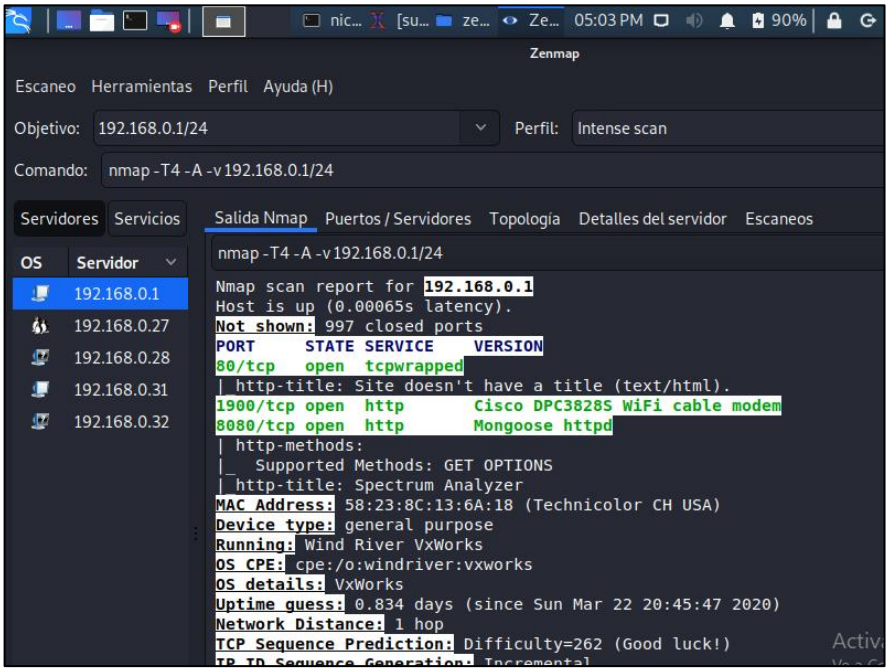
Nmap sirve para descubrir todos los host y puertos que hay en una red y saber qué servicio están corriendo detrás de los puertos con el fin de dejar en evidencia alguna vulnerabilidad de red, de igual forma, este software es capaz de detectar el sistema operativo y su versión dentro de determinado host. Nmap se conecta a una base de datos llamada “nmap-services” que cuenta con más de 2.200 puertos conocidos para poder arrojar un resultado contundente. Este software intenta determinar los protocolos del servicio, el nombre y versión de la aplicación, el tipo de dispositivo y el sistema operativo.[58]

En el siguiente ejemplo se realiza el escaneo de una red local donde se descubren diferentes servidores expuestos:

Se realiza escaneo encontrando 5 máquinas conectadas en la misma red 192.168.0.1, 192.168.0.27, 192.168.0.31 y 192.168.0.32

La máquina 192.168.0.1 corresponde al enrutador:

Ilustración 10. 192.168.0.1 Enrutador.

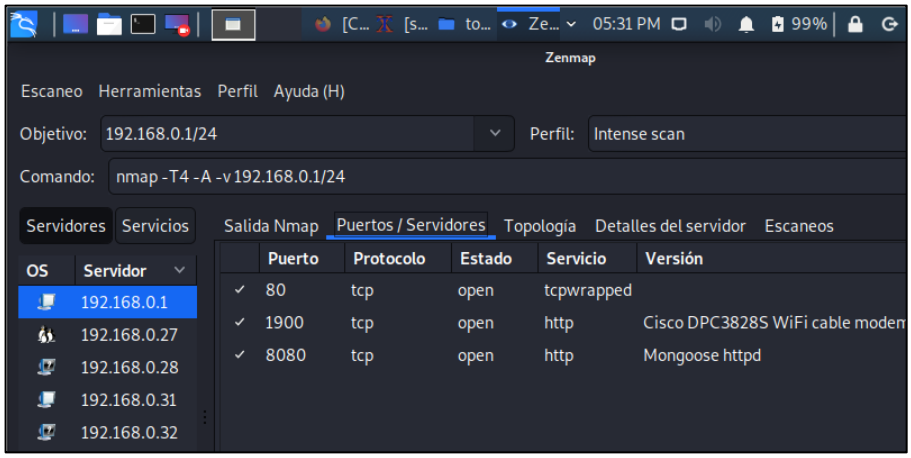


Fuente: El autor.

[58] Escaneo puertos nmap. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/

Sus puertos abiertos se evidencian a continuación:

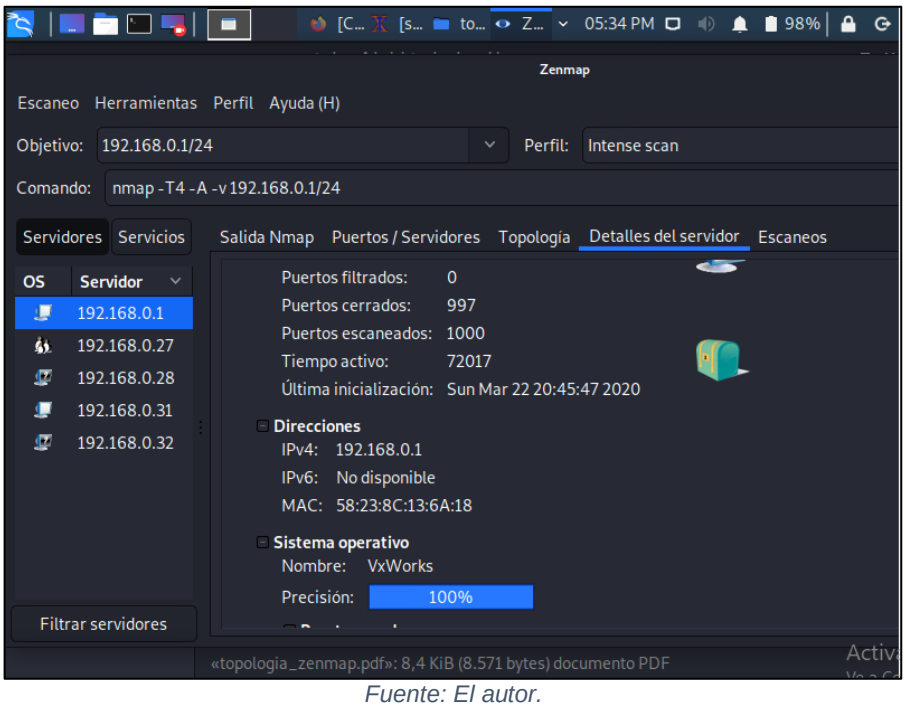
Ilustración 11. Puertos abiertos enrutador.



Fuente: El autor.

Los detalles del enrutador son:

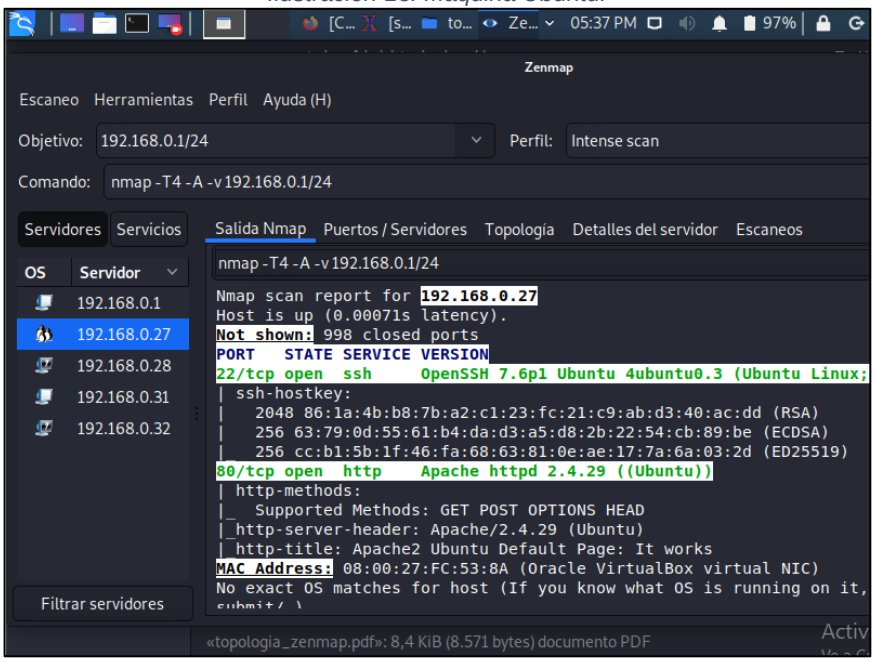
Ilustración 12. Detalle Enrutador.



Fuente: El autor.

La máquina 192.168.0.27 corresponde a un servidor con SO Ubuntu:

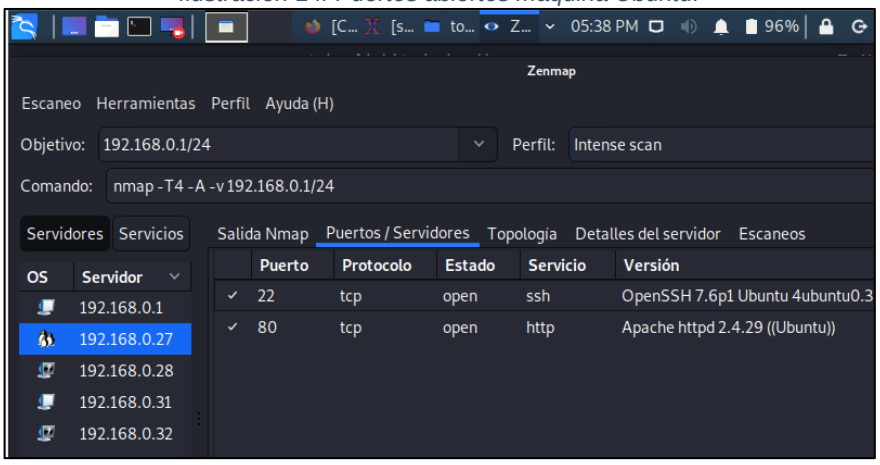
Ilustración 13. Máquina Ubuntu.



Fuente: El autor.

Se encuentran puertos abiertos que corresponden a los servicios de ssh y apache:

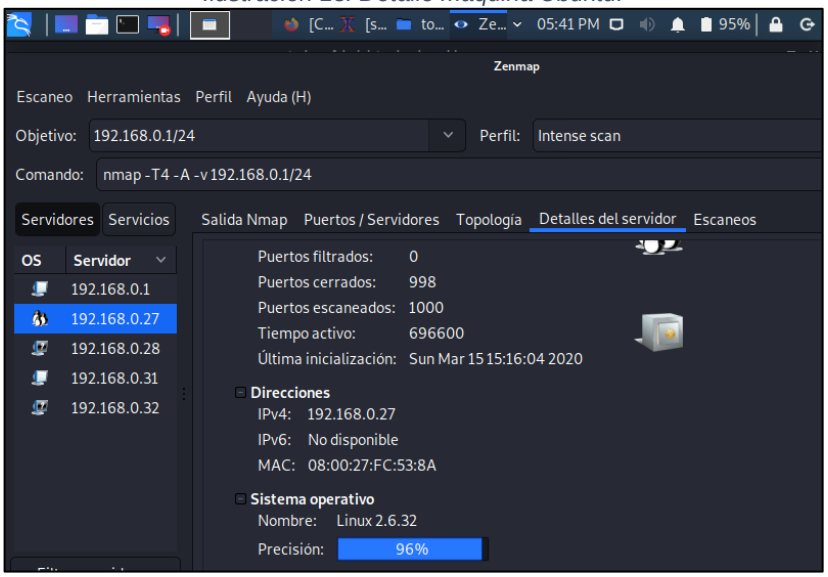
Ilustración 14. Puertos abiertos máquina Ubuntu.



Fuente: El autor.

Los detalles de la máquina Ubuntu son:

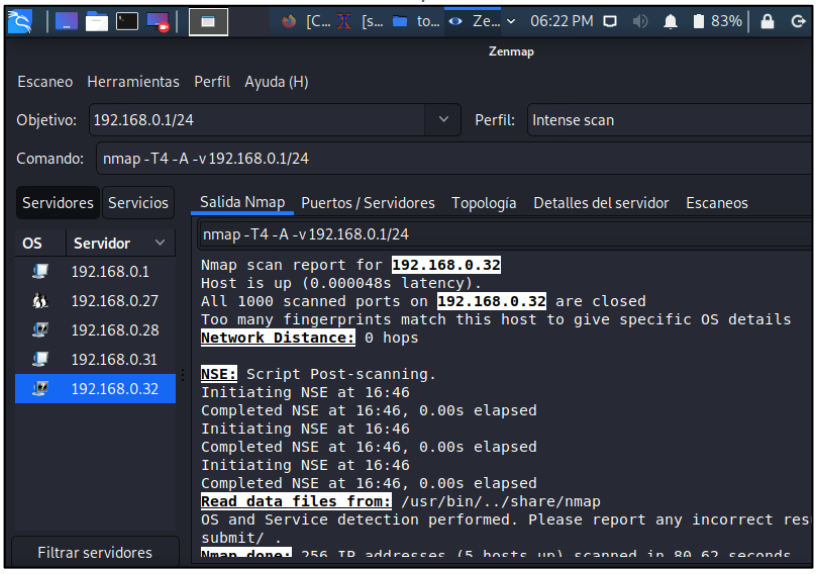
Ilustración 15. Detalle máquina Ubuntu.



Fuente: El autor.

La máquina 192.168.0.32 corresponde a un Kali linux quien es la que está ejecutando el escaneo.

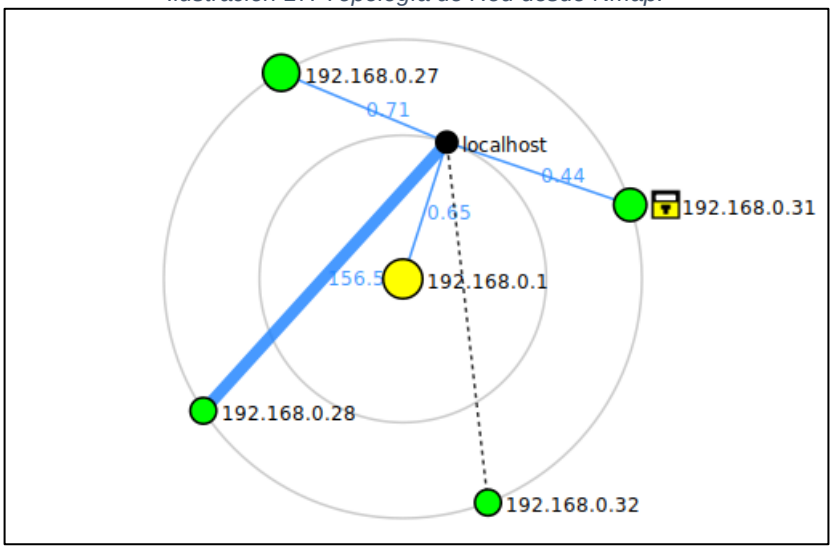
Ilustración 16. Máquina Kali Linux.



Fuente: El autor.

La topología de la red detectada es la siguiente:

Ilustración 17. Topología de Red desde Nmap.



Fuente: El autor.

5.3.2.5 Plan de pruebas según los dominios de ISO/IEC 27001:2013

Al realizar un levantamiento de información basado en los dominios del anexo A de la norma ISO/IEC 27001:2013 se estará efectuando un reconocimiento dentro de la organización y a su vez se estará auditando por lo que efectuar este plan de pruebas siempre será pertinente en un hacking ético. En el Anexo 3 de muestra un ejemplo de la ejecución de un plan de pruebas basado en la norma.

5.4 Modelado de amenazas (PTES)

Esta fase permite, como su nombre lo indica, establecer un modelo de amenazas por medio de un levantamiento y clasificación de los activos de información de la organización y así poder identificar cual tiene mayor probabilidad de ser atacado y que impacto generaría para la organización.

En el Anexo 2 se expone un ejemplo de cómo se debería documentar un inventario de activos de información según sus tipos. Para la clasificación se utilizó la nomenclatura definida en el libro II (catálogo de elementos) de la metodología MAGERIT - Versión 3.[59]

[59] MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos. [en línea]. [Consultado 03 julio 2021]. Disponible en

5.5 Explotación y Post-explotación – Ganando y Manteniendo el acceso (PTES – CEH- OSSTMM)

En esta fase se ejecutan los respectivos hackeos gracias a que en las fases anteriores se ha descubierto los posibles vectores de ataque en el potencial blanco y gracias a esto se ha determinado la estrategia de explotación de vulnerabilidades.

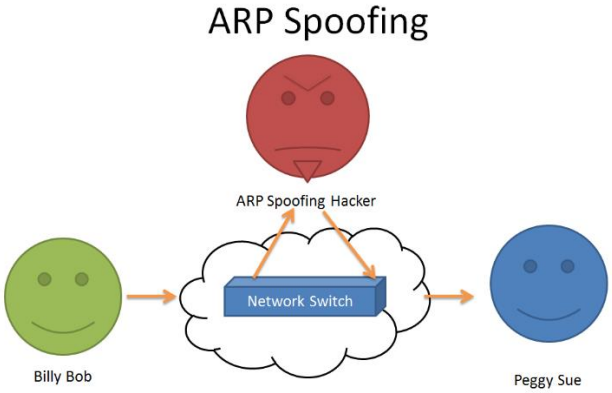
A continuación, se exponen una serie de ataques simulados bajo ambientes controlados que permiten evidenciar algunas de las técnicas que son usadas por los Hackers en la actualidad.

5.5.1 ARP Spoofing

Es un ataque en el que un atacante envía mensajes falsificados de ARP a una red para poder vincular su dirección MAC con la ip de un equipo específico y desde allí poder interceptar el tráfico para así poder manipularlo o retenerlo, dentro de los ataques más comunes que se dan después de haber perpetrado el Spoofing inicial están el de Denegación de Servicio (DoS), Secuestro de sesiones (Session hijacking) y de tipo Man-in-the-middle.

Este tipo de ataques (ARP Spoofing) se dan en las redes de área local que utilizan el protocolo de resolución de direcciones ARP.[60]

Ilustración 18. ARP Spoofing



*Fuente: https://miro.medium.com/max/1400/1*afdP5x0lZ2EeYTWOwiwxtg.png*

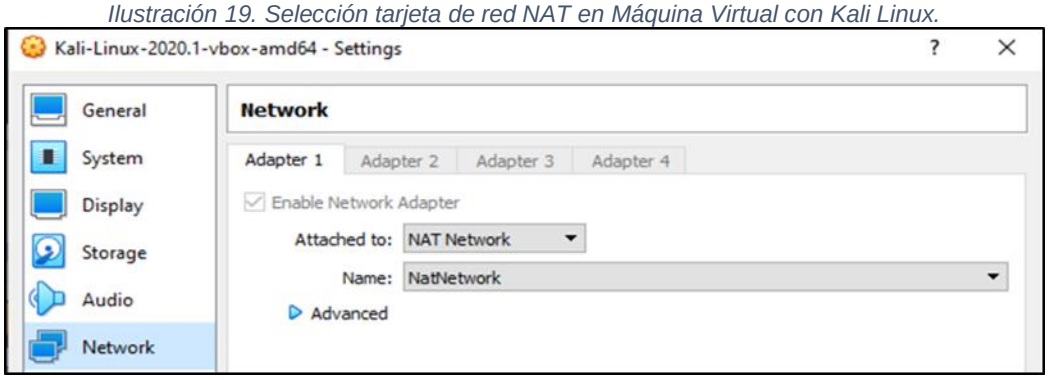
https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

[60] ARP Spoofing. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en https://www.ionos.es/digitalguide/servidores/seguridad/arp-spoofing-ataques-desde-la-red-interna/

En el siguiente ejemplo se ve materializado un ARP Spoofing:

Se realiza instalación de Kali Linux en máquina virtual teniendo en cuenta que la configuración de red será para que trabaje por medio de una red NAT.

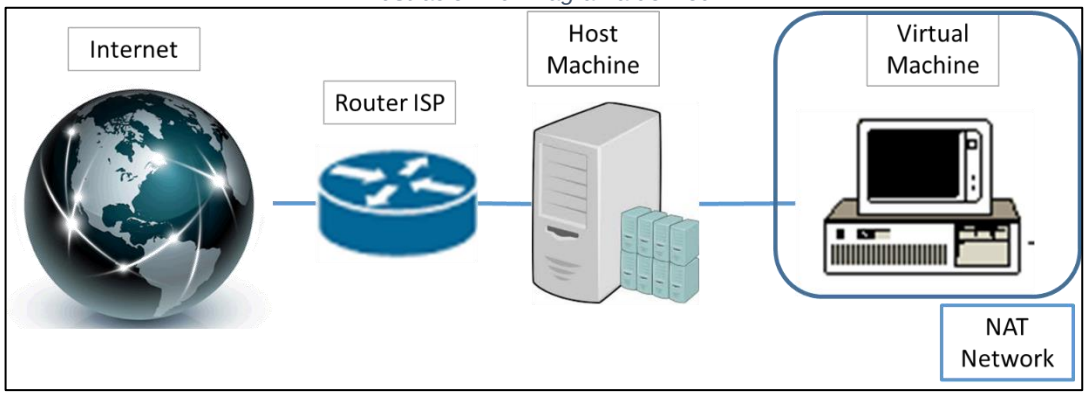
Ilustración 19. Selección tarjeta de red NAT en Máquina Virtual con Kali Linux.



Fuente. El autor.

El motivo de esta configuración es para crear una red virtual en la host machine, es decir, el computador principal que en este caso tiene un SO Windows 10, hará el papel de enrutador y la máquina virtual será un cliente conectado a esta red. Lo anterior genera mayor practicidad al momento de realizar el respectivo ataque.

Ilustración 20. Diagrama de Red.



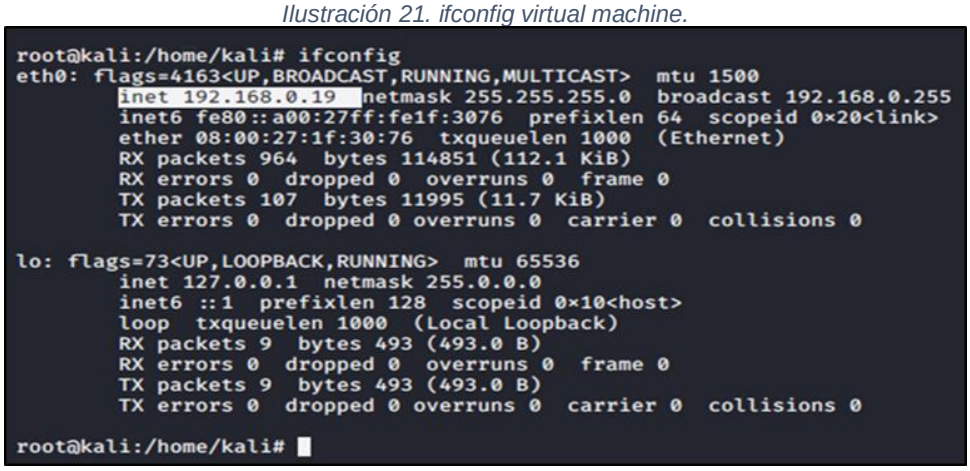
Fuente. El autor.

Para dar inicio con el ataque es necesario la obtención de información necesaria de la “victima” por medio de la herramienta Netdiscover, con este software se pueden descubrir clientes conectados a la red actual, así pues, se obtiene la IP, la MAC y el fabricante del hardware de la tarjeta de red de los clientes.

Con el fin de utilizar la herramienta es necesario conocer como está compuesta la red, ver la IP de la virtual machine y eventualmente usar el rango de dicha IP para encontrar demás clientes conectados a la red.

Para conocer la IP de la virtual machine se ejecuta el comando “ifconfig” que da como resultado 192.168.0.19:

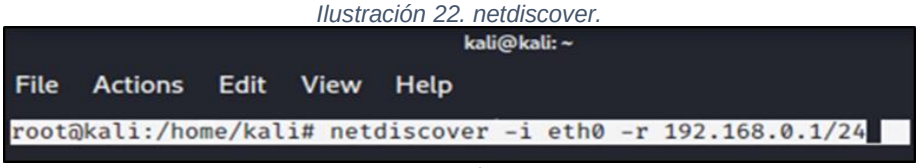
Ilustración 21. ifconfig virtual machine.



Fuente. El autor.

Seguidamente se ejecuta el comando “netdiscover –i eth0 –r 192.168.0.1/24”:

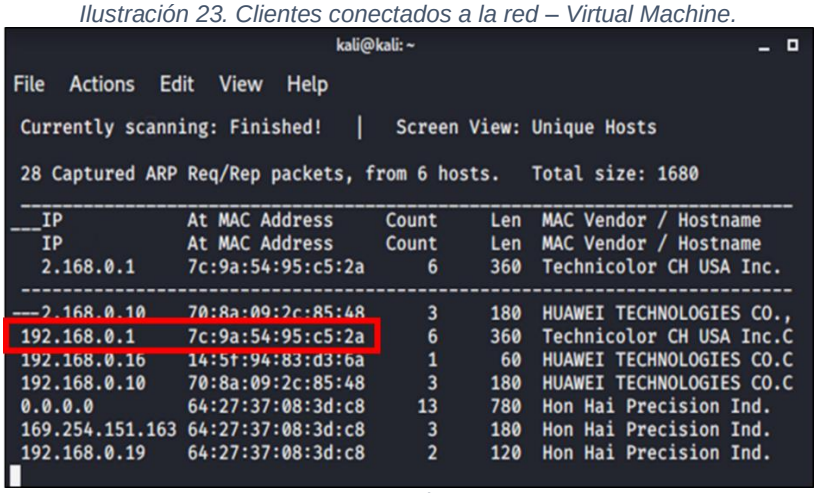
Ilustración 22. netdiscover.



Fuente. El autor.

Se obtiene como resultado los clientes conectados a la red observando que la dirección IP 192.168.0.1 es el AP (Access Point) y su MAC es 7c:9a:54:95:c5:2a

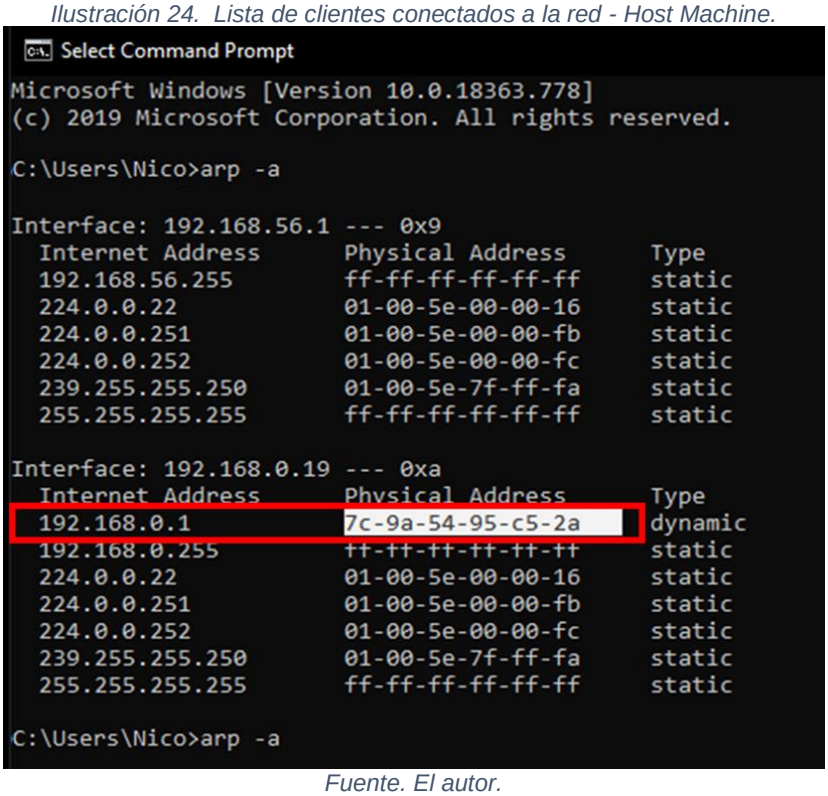
Ilustración 23. Clientes conectados a la red – Virtual Machine.



Fuente. El autor.

Se realiza la misma verificación en la host machine con el comando “arp -a” y se obtiene que la IP 192.168.0.19 (Virtual Machine) está conectada a dirección IP 192.168.0.1, es decir, al AP (Access Point) y su MAC es 7c-9a-54-95-c5-2a

Ilustración 24. Lista de clientes conectados a la red - Host Machine.



Fuente. El autor.

Con la información anterior se procede a realizar el ataque spoofing por medio de la herramienta Arpspoof y que permite hacer ataques Man in The Middle permitiendo redirigir el tráfico que fluye a través de una red.

Los siguientes comandos son los que permiten realizar el ataque:

“arpspoof -i [INTERFACE] –t [TARGET IP] [AP API]” para indicarle a la virtual machine que el host machine es el router.

“arpspoof -i [INTERFACE] –t [AP IP] [TARGET IP]” para indicarle al AP (Access point) que la host machine es el router.

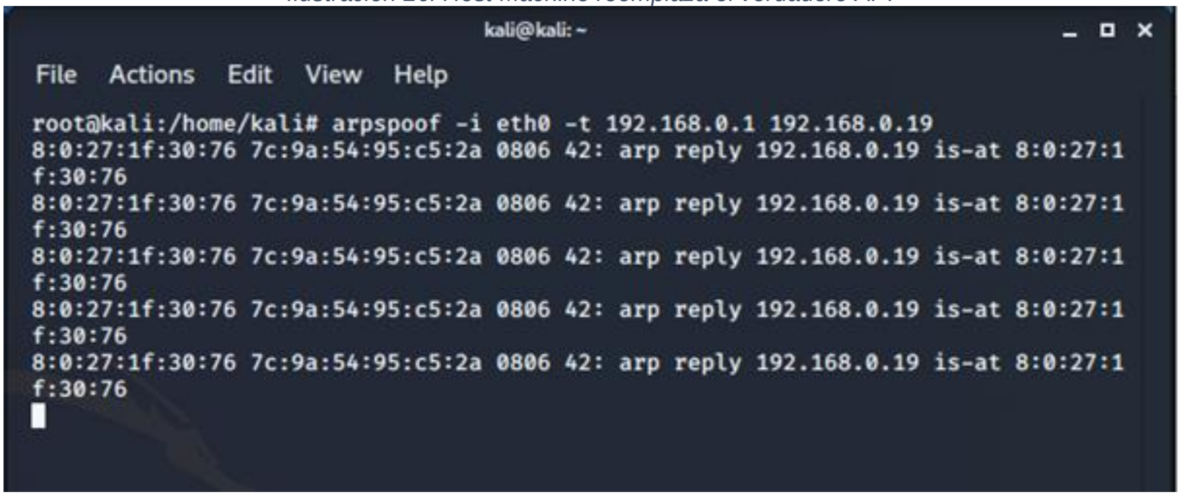
Al ejecutar los siguientes comandos se cambia la MAC del AP por la MAC del host machine a la que la virtual machine se está conectando y completando así el spoofing con lo cual ya se puede acceder a capturar el tráfico de la victima:

“arpspoof –i eth0 –t 192.168.0.19 192.168.0.1”
“arpspoof –i eth0 –t 192.168.0.1 192.168.0.19”

Ilustración 25. Host Machine se convierte en router de Virtual Machine.

Fuente. El autor.

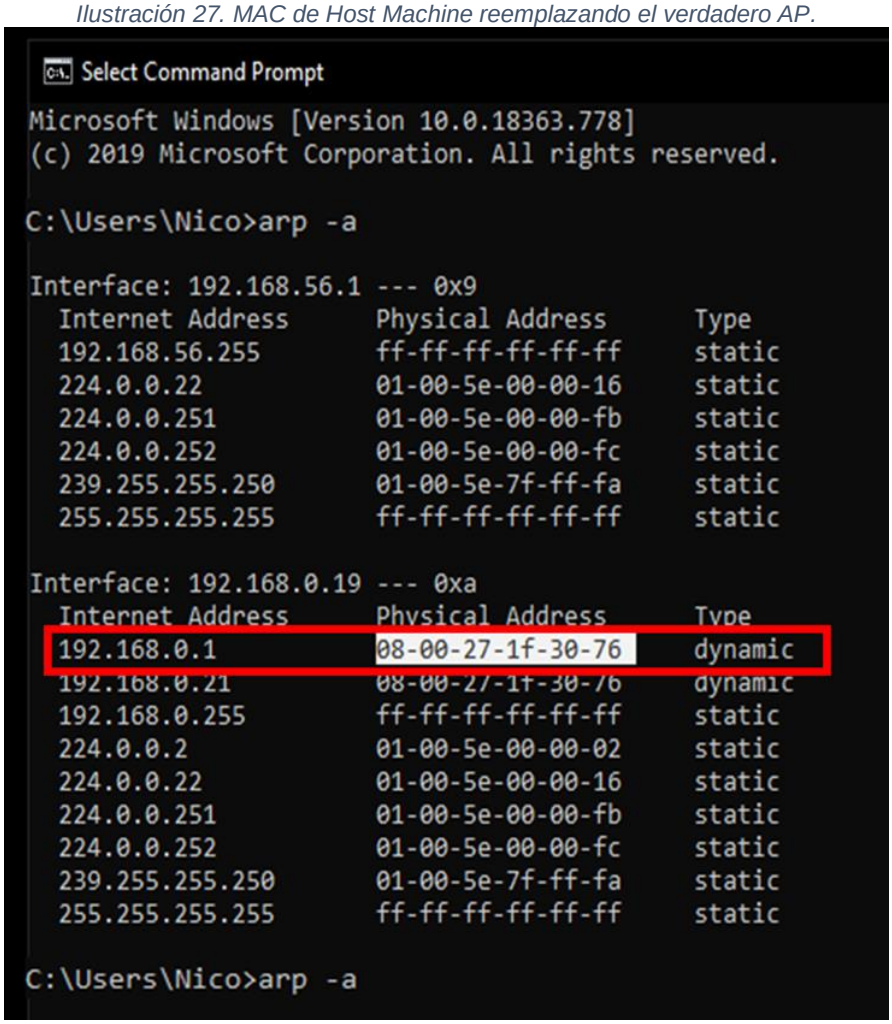
Ilustración 26. Host Machine reemplaza el verdadero AP.



Fuente. El autor.

Se realiza la verificación en la host machine con el comando “arp -a” y se obtiene que la IP 192.168.0.19 (Virtual Machine) está conectada a dirección IP 192.168.0.1, con la diferencia y es que ahora la MAC es 08-00-27-1f-30-76 la cual pertenece a la host machine.

Ilustración 27. MAC de Host Machine reemplazando el verdadero AP.



Fuente. El autor.

Se concluye que la direccion MAC a la que la victima se dirige ya no a la del AP sino a la del host machine por lo que el ataque spoofing es exitoso.

5.5.2 Conexión por ssh a máquina remota

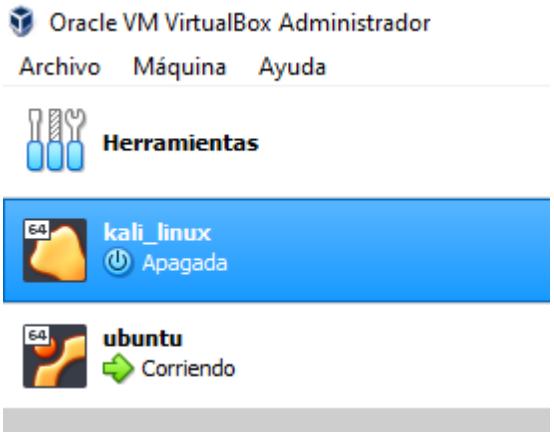
Gracias a la fase de recolección de información se pueden obtener diferentes IP's dentro de una red local y de acuerdo con la pericia y el uso de ingeniería social por parte de un atacante es posible saber una posible distribución de servidores o maquinas dentro de un entorno corporativo lo que permitiría acotar el universo a atacar y enfocarse en las maquinas más valiosas para explotar.

Sin conocer casos de la vida real es muy difícil creer que existan servidores con contraseñas de usuario débiles o sin contraseñas, sin embargo, existen por lo que

en este caso se simulará un acceso a una maquina sin contraseña por medio del protocolo ssh el cual es el más conocido para administrar remotamente servidores. Para los casos donde las maquinas tengan contraseña se puede implementar un ataque por fuerza bruta con herramientas como “THC Hydra” o “John the Ripper” provistos por Kali Linux teniendo en cuenta que en un Hacking ético no se deben afectar los servicios sin previa autorización:

Se realiza descarga e instalación de Oracle VM en entorno Windows 10 con el fin de realizar montaje de máquinas virtuales y allí se instalan dos sistemas operativos basados en Linux: Kali y Ubuntu:

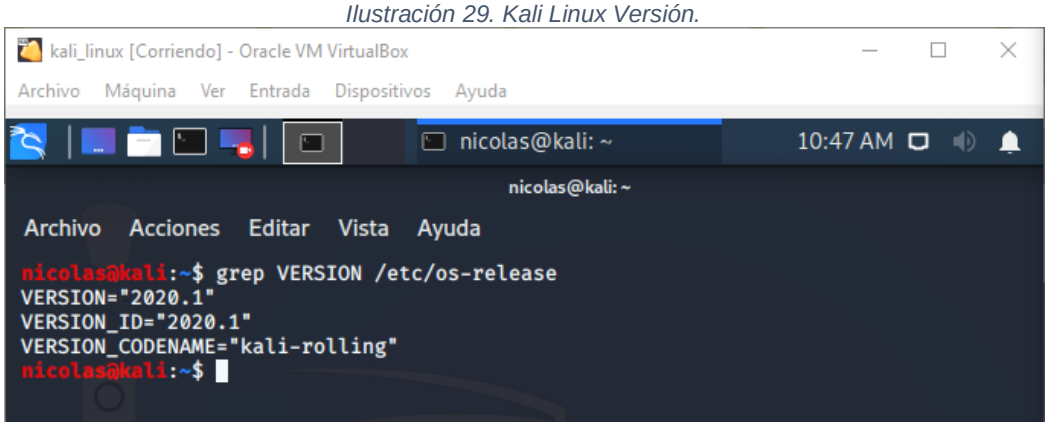
Ilustración 28. Máquina Virtuales en Oracle VM.



Fuente. El autor.

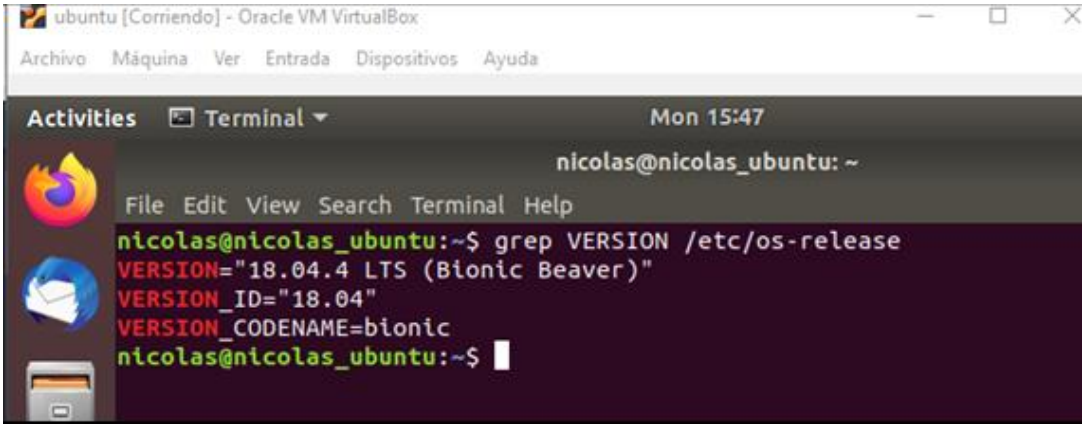
Se da inicio a las 2 máquinas virtuales instaladas y se exponen sus versiones:

Ilustración 29. Kali Linux Versión.



Fuente. El autor.

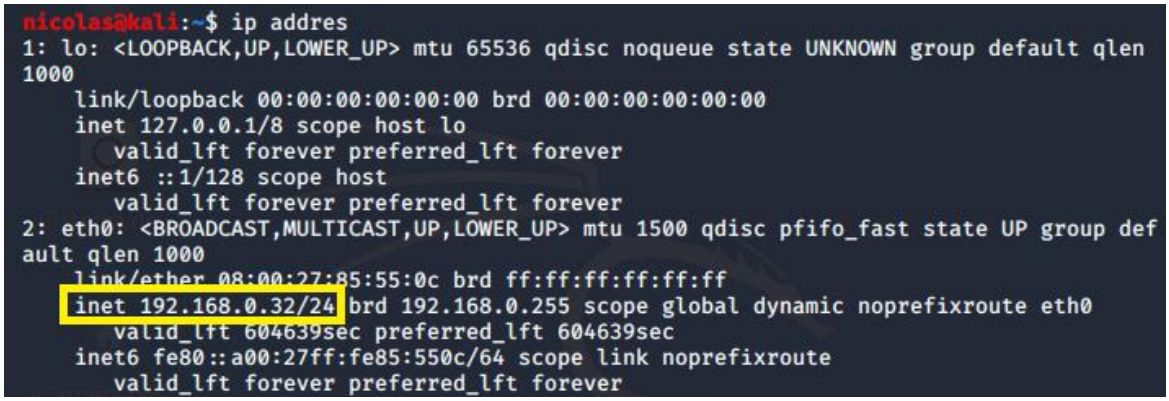
Ilustración 30. Ubuntu Versión.



Fuente. El autor.

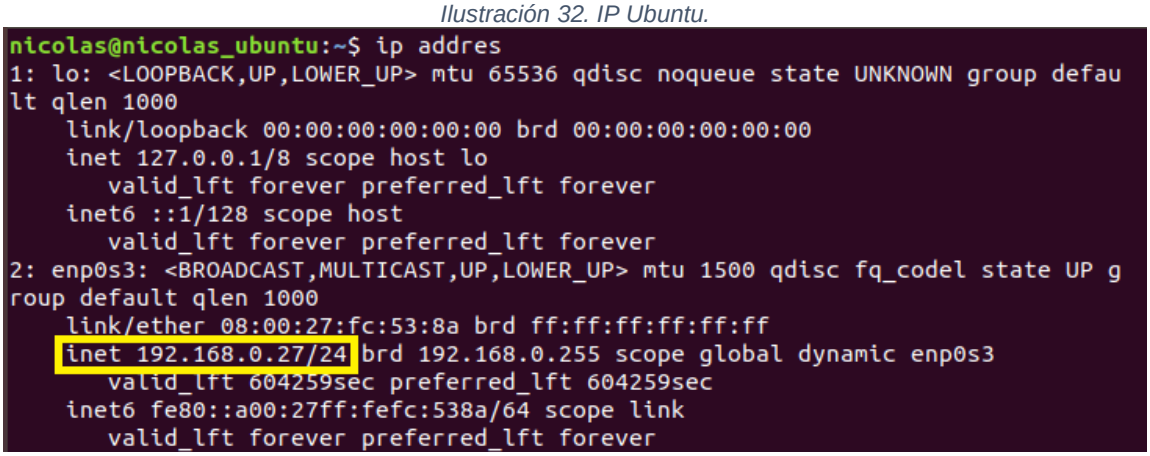
Se verifican las IP's de las 2 máquinas:

Ilustración 31. IP Kali Linux.



Fuente. El autor.

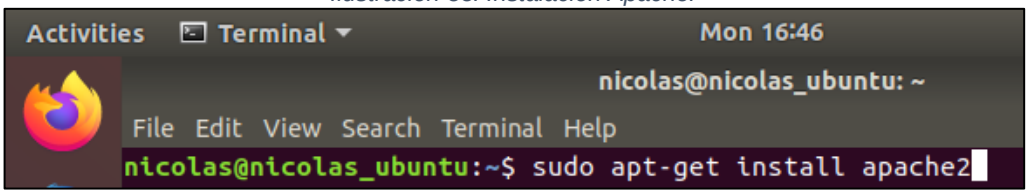
Ilustración 32. IP Ubuntu.



Fuente. El autor.

Se realiza instalación de apache en maquina Ubuntu para simular el servidor:

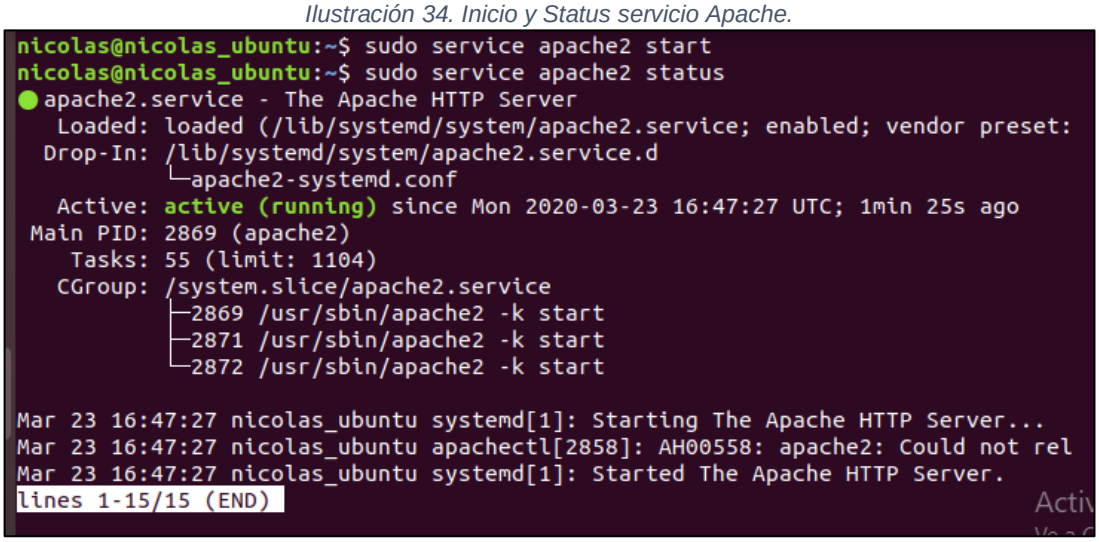
Ilustración 33. Instalación Apache.



Fuente. El autor.

Una vez ha finalizado la instalación se procede con el inicio del servicio y prueba de su status.

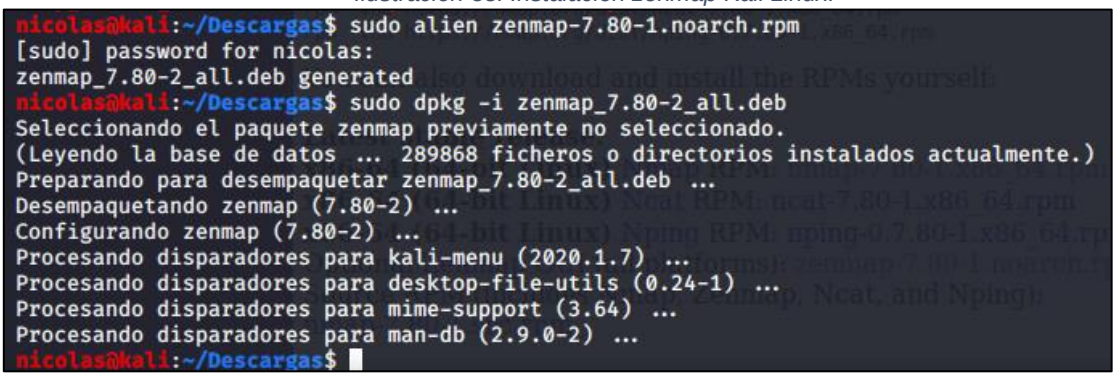
Ilustración 34. Inicio y Status servicio Apache.



Fuente. El autor.

Se procede a realizar la instalación de zenmap en Kali Linux.

Ilustración 35. Instalación zenmap Kali Linux.

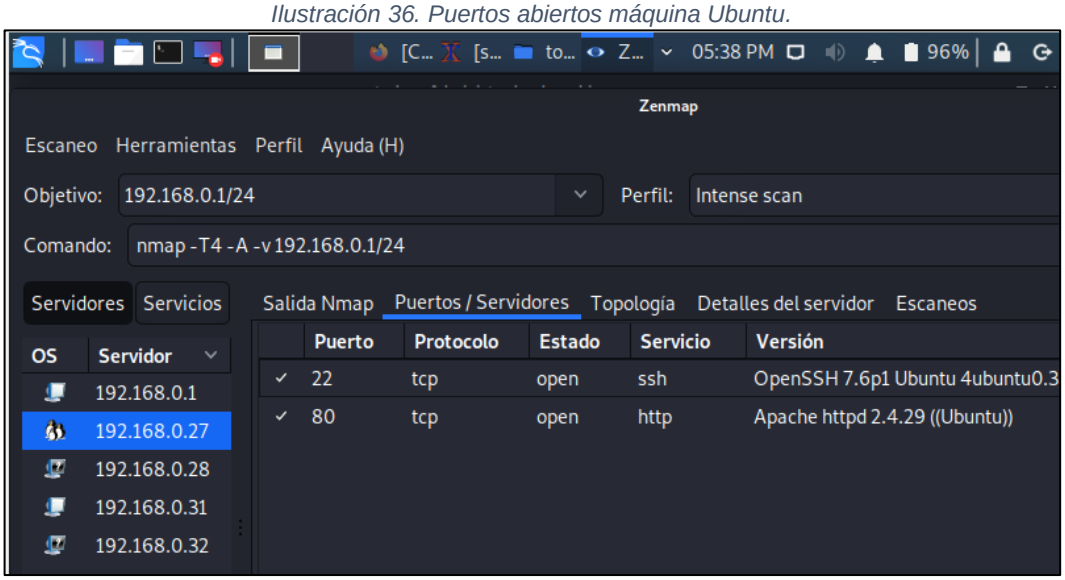


Fuente. El autor.

Se realiza escaneo con el comando "*nmap –T4 –A -v 192.168.0.1/24*" y el sistema arroja los siguientes resultados encontrando 5 máquinas en la red: 192.168.0.1, 192.168.0.27, 192.168.0.31 y 192.168.0.32:

Para la maquina 192.168.0.27 (Máquina Ubuntu) se muestra a continuación los puertos abiertos que corresponden a los servicios de ssh y apache.

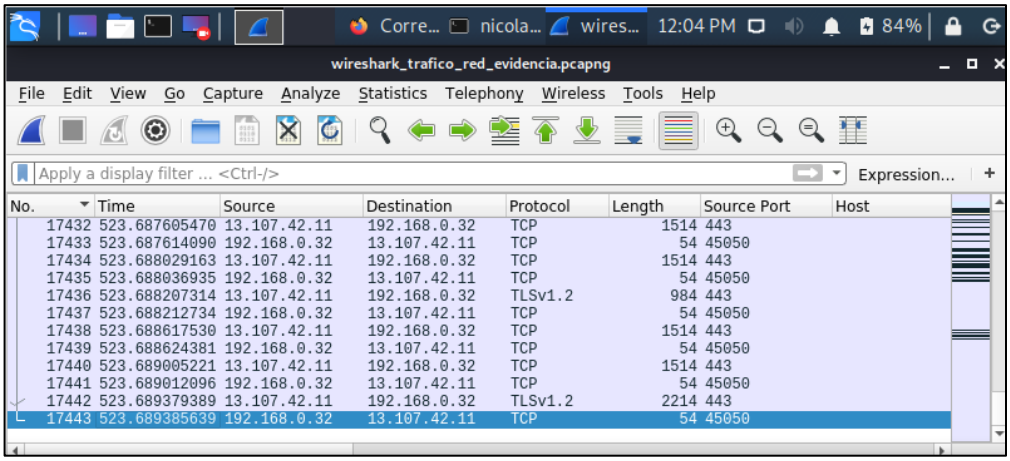
Ilustración 36. Puertos abiertos máquina Ubuntu.



Fuente. El autor.

Se realiza escaneo del tráfico de red desde la máquina de Kali Linux mediante la herramienta The Wireshark donde se detecta la IP de la máquina de Ubuntu 192.168.0.32.

Ilustración 37. Escaneo de tráfico de red - Wireshark

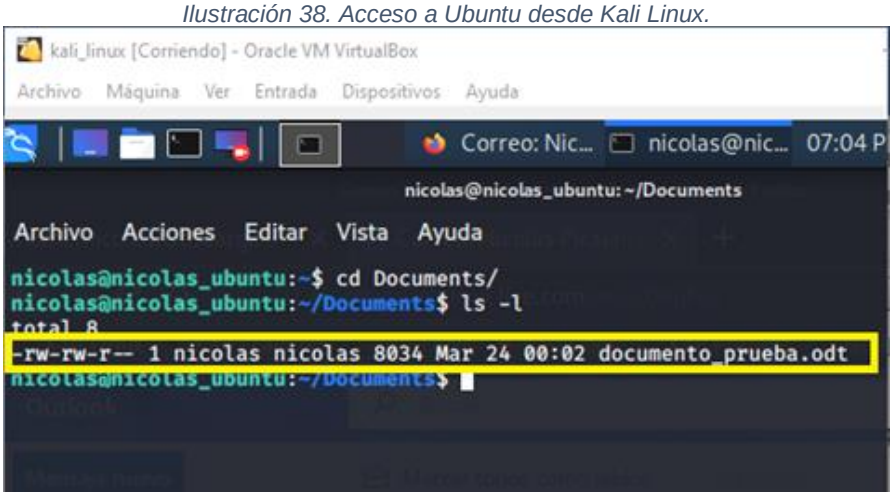


Fuente. El autor.

Una vez se han obtenido los datos de las maquinas se procede a realizar accesos por medio de ssh con el comando "*ssh usuario@ipmaquina*", allí ya se puede verificar el contenido de cualquier carpeta siempre y cuando se tengan los permisos

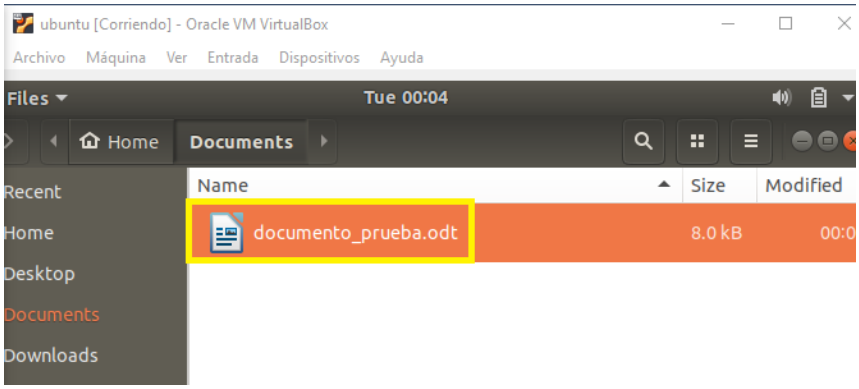
adecuados, por ejemplo, un archivo dejado en el directorio de Documentos y expuesto remotamente.

Ilustración 38. Acceso a Ubuntu desde Kali Linux.



Fuente. El autor.

Ilustración 39. Archivo en Documentos - Ubuntu.



Fuente. El autor.

5.5.3 SQL Injection

Al conocer los sistemas de información de una organización es posible encontrar el en que sitio se encuentran las secciones con las cajas o mecanismos de logueo lo que permite escoger de una baraja de posibilidades como realizar un ataque y poder vulnerar su seguridad, a continuación, se muestra cómo se podría realizar una inyección de SQL no sin antes dar una breve explicación de qué consiste el ataque. El objetivo es insertar un Query como dato de entrada en las cajas de texto del logueo en una aplicación, es decir, enviar peticiones a la base de datos para intentar extraer información sensible y/o vulnerar contraseñas de usuarios.

El SQL Injection permite suplantar la identidad de usuarios, alterar o destruir información y hasta alterar la base de datos para beneficio del atacante.[61]

Ejemplo de ataque:

Sistema de login con cajas de texto que permite teclear los datos de entrada como lo son usuario y contraseña:

User: usuario
Pass: contraseña

Como no se conoce ningún dato de entrada, se deduce que el sistema debería arrojar mensajes de error como lo pueden ser:

"Nombre de usuario incorrecto"
"Contraseña incorrecta"
"Nombre de usuario y contraseña correctos"

Dando inicio a la comprobación se puede colocar una comilla simple en el campo "User" y escribir en un posible usuario:

User: 'usuario
Pass: contraseña

El sistema podría arrojar el siguiente mensaje al querer loguearse:

"Error en la consulta"

Por lo que al usar tautologías en una condición del Query obligamos al sistema a que lea los datos de entrada como verdaderos así no lo sean y así la respuesta de error sería diciente.

User: usuario
Pass: contraseña' OR '1'='1

"Nombre de usuario y contraseña correctos"

Lo anterior permite saber que el usuario si existe dentro de la base de datos y ya se podría proceder con a realizar la misma dinámica para poder obtener los nombres de los campos de la tabla de usuarios.

User: usuario
Pass: contraseña' AND campo is NULL;

[61] SQL Injection. [Sitio web]. [Consulta: 04 julio 2021]. Disponible en http://www.mclibre.org/consultar/php/lecciones/php-db-inyeccion-sql.html

Si el sistema arroja un error como, por ejemplo: "Nombre de usuario incorrecto", significa que el "campo" en la tabla de la base de datos existe y se puede utilizar para extraer el nombre de la tabla.

Seguidamente se inyecta un Query más robusto y que contenga un posible nombre de la tabla para observar la respuesta, si arroja "Nombre de usuario incorrecto" significa que efectivamente se encontró la tabla de usuarios

User: usuario
Pass: contraseña' AND 1=(SELECT COUNT(*) FROM tabla);

Conociendo toda la información extraída, el atacante puede iniciar su hackeo y vulnerar la seguridad del sistema inyectando un Query de inserción de información para crear usuarios o alterando el modelo de datos borrando tablas.

Ejemplo de creación un usuario:

User: usuario
Pass: contraseña'; INSERT INTO tabla ('campo', 'contraseña') VALUES ('usuarioX', 'contraseñaY');

Ejemplo de borrado de tabla:

User: usuario
Pass: contraseña'; DROP TABLE tabla;

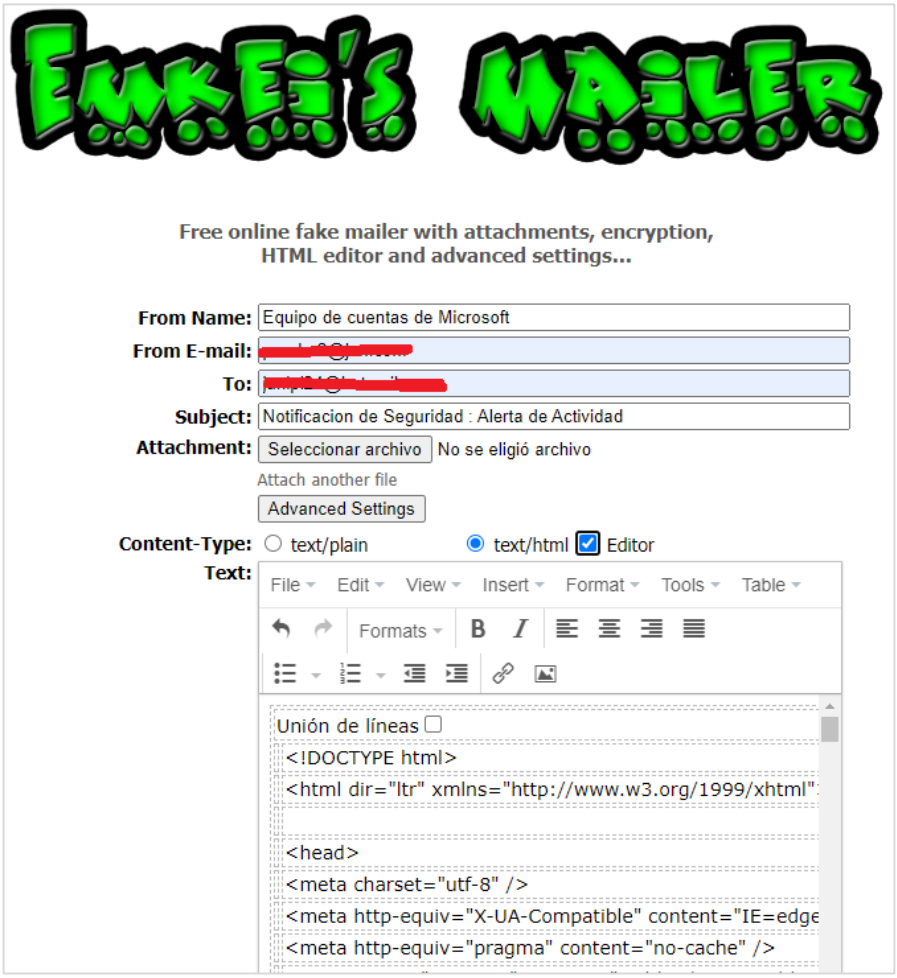
5.5.4 e-mail Spoofing

A esta técnica de ataque se le conoce como suplantación de identidad por medio de correo electrónico puesto que la víctima recibe un e-mail de una dirección remitente que al parecer es confiable sin saber puede ser spam o pishing.[62]

Existen herramientas online que permite ejecutar esta clase de ataques de forma gratuita, lo único que se requiere es remitente y el resto va por cuenta de la creatividad del atacante tal y como se expone a continuación:

[62] E-mail spoofing, [Sitio web]. [Consulta: 04 julio 2021]. Disponible en https://www.welivesecurity.com/la-es/2021/03/23/que-es-email-spoofing-suplantacion-identidad-correos-electronicos

Ilustración 40. Fake mailer.

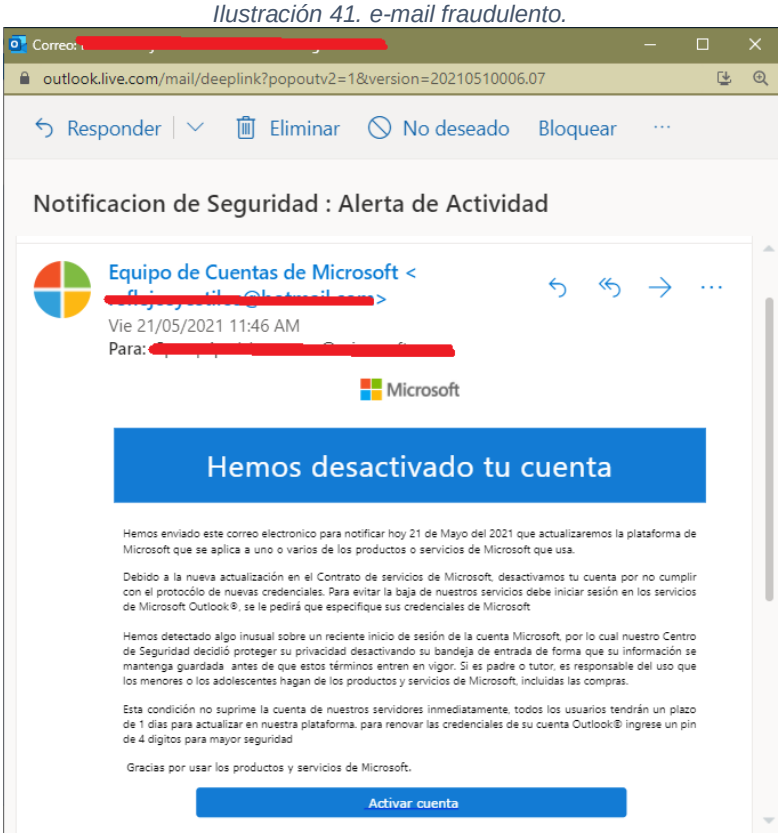


Fuente. https://emkei.cz/

Al utilizar una herramienta que permita suplantar correos electrónicos se puede llegar a construir una verdadera trampa que pase desapercibida por al menos un empleado en una empresa lo que hará que el ataque sea exitoso y se permita dejar abierta la puerta para implantar troyanos, rasomware, etc.

Como resultado de la generación de un correo electrónico fraudulento se muestra el siguiente ejemplo:

Ilustración 41. e-mail fraudulento.



Fuente. El autor.

5.6 Informes (PTES)

En esta fase se generan los respectivos entregables e informes resultantes de la labor realizada, aquí es donde se documentan todos los hallazgos y evidencias y se generan las respectivas recomendaciones con el fin de poder mitigar los riesgos y cerrar las brechas de seguridad.

Se hace necesario la entrega de dos clases de informes, uno para la alta gerencia que dé a conocer el estado general de la situación, y el cómo y en cuanto tiempo se podrán mitigar los inconvenientes encontrados y si es el caso, cuánto dinero se puede ahorrar al implementar las recomendaciones dadas, se puede observar un ejemplo de plantilla de informe ejecutivo en el Anexo 4; el otro informe ya se enfoca en lo técnico donde el detalle es lo importante para dar a conocer cómo se llegó a las conclusiones, este informe se enfoca más en una narración que al diligenciamiento de una plantilla específica, sin embargo, en el Anexo 5 se puede observar un ejemplo de plantilla que puede ayudar a auditor a plasmar lo encontrado después de haber realizado la labor del Hacking Ético.

6. CONCLUSIONES

- Sin desconocer las demás técnicas y metodologías creadas por grandes especialistas en la materia y después de una labor investigativa se optó por resaltar que OSSTMM (Open Source Security Testing Methodology Manual), PTES (Penetration Testing Execution Standart) y CEH (Certified Ethical Hacker) son las metodologías que aportan los resultados concluyentes y significativos al momento de ejecutarlas en entornos corporativos. Los factores de éxito de estas metodologías son:

  - ✓ La ejecución de forma ordenada de cada una de las etapas conlleva a obtener resultados concluyentes que permiten ejecutar acciones de mejora de manera inmediata con el fin de mitigar al máximo los riesgos encontrados.

  - ✓ El generar informes tanto técnicos como ejecutivos permiten el seguimiento y control de las recomendaciones de una forma más detallada y medible tanto del personal de infraestructura como de la alta gerencia para ampliar el horizonte y mejorar la toma de decisiones frente a los riesgos identificados en la ejecución de las metodologías aplicadas.

- Como se pudo evidenciar en la ejecución de pruebas de penetración, uno de los vectores de ataque más críticos es la aplicación de técnicas de reconocimiento pasivo puesto que, sin importar la cantidad de esquemas de seguridad con las que cuenten las empresas, siempre existirá información publicada en internet o documentos físicos desechados en la basura con información sensible lo que permitirá aumentar los riesgos de ataques cibernéticos.

- Basado en las pruebas de pentesting que se pueden ejecutar en las organizaciones y sin importar la metodología de Ethical Hacking escogida se puede concluir que los riesgos y las vulnerabilidades siempre estarán latentes y a la espera de que se manifiesten o que se exploten, sin embargo, existen gran cantidad de buenas prácticas que pueden conllevar a que los impactos sean mínimos. A continuación, se plantean una serie de recomendaciones basadas en los resultados obtenidos a partir de algunas simulaciones efectuadas y que pueden servir como pautas para el mejoramiento continuo de la seguridad informática en cualquier entorno corporativo:

- ✓ El parque informático debe contar siempre con software antivirus licenciado y actualizado al igual que el software utilizado con el fin de evitar que los mismos empleados crackeen licencias.

- ✓ La capacitación constante y la generación de conciencia en los empleados sobre seguridad informática es un factor diferencial para proteger los activos de información.

- ✓ El personal contratado o a contratar en el área de TI debe contar con certificados en seguridad informática.

- ✓ Los equipos de cómputo deben tener los puertos bloqueados con el fin de evitar extracción por medio de medios magnéticos como una USB.

- ✓ Programar el borrado de caché, historial y almacenamiento de contraseñas en los navegadores utilizados por los empleados evitando exponer correos electrónicos o sistemas de información que no cerraron sesión.

- ✓ Cualquier empleado debe ser consciente del correcto uso del correo electrónico corporativo, del riesgo por el mal uso de este, y que solo se deberá utilizar para intercambiar información exclusiva de la organización.

- ✓ Es necesario prohibir actividades diferentes a las laborales de personas no autorizadas en áreas restringidas o circundantes equipos de cómputo con información sensible como lo puede ser el Centro de Datos de la organización, esto evitará accidentes como desconexiones de energía eléctrica, derramamiento de líquidos, etc.

- ✓ Los equipos de cómputo utilizados por los empleados deben tener restricciones de instalación de software y demás privilegios que solo puede tener un administrador.

- ✓ Se debe establecer una política de uso de celulares propios de los empleados para evitar el acceso a los sistemas de información de la empresa desde estos dispositivos.

- ✓ Las claves y privilegios dados a un empleado deben ser retirados inmediatamente una vez se finalice la relación contractual con él.

- ✓ La instalación de seguridad perimetral como Firewall, Sistemas de Detección de intrusos (IDS) y/o Sistemas de Prevención de Intrusos (IPS) aumentaran la seguridad de las redes.

- ✓ Los equipos de cómputo de toda la organización deben tener restricciones en la navegación en internet, es decir, permitir solo las páginas autorizadas dentro de las policitas de seguridad, esto evita descarga de malware accidental.

- ✓ Los equipos de cómputo de toda la organización deben estar configurados para bloqueo automático después de detectar inactividad en un determinado tiempo.

- ✓ Crear políticas de Seguridad de la Información e implementar un Sistema de Gestión que estén enmarcados dentro de la ISO/IEC 27001:2013.

- ✓ Contratar un oficial de Seguridad Informática que este encargado de mantener actualizado el SGSI y al mismo tiempo vele por la seguridad en la organización.

- ✓ Implementar cifrados de contraseñas dentro de los Sistemas de información desarrollados in house y exigir esto a proveedores de software.

- ✓ Generar bloqueos de usuarios en el momento que se detecte una cantidad de ingresos fallidos y generar notificación al administrador del sistema de esta situación.

- ✓ Implementar generación de trazas o logs de auditoria en los sistemas de información que permiten realizar transacciones, por ejemplo, almacenar en un log el Time Stamp de cambios de contraseñas de usuarios.

- ✓ Todos los servicios y Sistemas de Información públicos protegerlos dentro de una DMZ (Zona Desmilitarizada).

- ✓ Los puertos que no estén en uso deberán ser bloqueados.

- ✓ Adquirir certificados SSL para los Sistemas de Información publicados en internet.

- ✓ Separar la red inalámbrica de invitados de la red usada por los empleados.

- ✓ Mantener oculta la información de la organización en los servicios de directorios WhoIs realizando la respectiva petición y pago del proveedor del dominio.

- ✓ El software base de los sistemas operativos debe estar siempre en una partición de disco duro diferente a donde se encuentren los documentos, esto en caso de que falle el sistema se puedan recuperar los documentos.

- ✓ Implementar políticas de copias de seguridad en la nube.

- ✓ Implementar políticas de usuarios, roles y privilegios con el fin de restringir los accesos a información privilegiada.

- ✓ Todas las contraseñas por defecto en los equipos de y en la red deben ser cambiadas periódicamente.

- ✓ Mantener actualizados los planes de contingencia y los controles de cambios.

- ✓ El seguimiento y control de la implementación de un modelo de seguridad informática es lo más importante no solo basta con dejar que las herramientas hagan su trabajo.

- ✓ Es muy importante ejecutar pruebas de vulnerabilidades o test de penetración de forma periódica.

- ✓ Es necesario validar los permisos del usuario del sistema de la aplicación que se conecta a la base de datos (no confundir con usuarios que se autentican en la aplicación) con el fin de que pueda insertar o modificar datos en tablas específicas, es decir permisos de DML (SELECT, UPDATE, INSERT) y no DDL (DROP, ALTER, CREATE) o DCL (REVOKE, GRANT).

- ✓ Implementar el uso de captchas en los formularios con el fin de evitar que robots intenten realizar peticiones masivas sobre los sitios web de la empresa.

- ✓ Implementar tareas de depuración de usuarios en los sistemas de información de manera periódica.

BIBLIOGRAFÍA

[1] ÁLVAREZ MARAÑÓN, Gonzalo y PÉREZ GARCÍA, Pedro Pablo. Seguridad informática para empresas y particulares. Mc Graw Hill, 2004.

[2] BERNABÉ DURÁN, Alejandro. Acceso a datos en aplicaciones web del entorno servidor: desarrollo de aplicaciones con tecnologías web (UF1845). Madrid: IC Editorial, 2015.

[3] CHICANO TEJADA, Ester. MF0487_3: Auditoría de seguridad informática. Madrid: IC Editorial, 2014.

[4] COLOBRAN HUGUET, Miguel; ARQUÉS SOLDEVILA, Josep Maria y GALINDO, Eduard Marco. Administración de sistemas operativos en red. Editorial UOC. 2008.

[5] COSTAS SANTOS, Jesus. Seguridad y alta disponibilidad. RA-MA, 2011.

[6] DERRIEN, Yann. Técnicas de la auditoría informática. Barcelona: Marcombo. 2009.

[7] DÍAZ, Gabriel, et al. Seguridad en las comunicaciones y en la información. Madrid: Librería UNED, 2004.

[8] ESCRIVÁ GASCÓ. Gema, et al. Seguridad informática. Macmillan. 2013.

[9] FERNANDEZ SANCHEZ, Carlos Manuel; PIATTINI VELTHUIS, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. AENOR, 2012.

[10] GÓMEZ FERNANDEZ, Luis; ANDRÉS ALVAREZ, Ana. Guía de aplicación de la norma une-iso/iec 27001 sobre seguridad en sistemas de información para pymes. Madrid: AENOR Ediciones.

[11] GÓMEZ FERNÁNDEZ, Luis Antonio; FERNÁNDEZ RIVERO, Pedro Pablo. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. Madrid: AENOR Ediciones, 2018.

[12] GÓMEZ LOPEZ, Julio; GÓMEZ LOPEZ, Oscar David. Administración de sistema operativos. RA-MA, 2015.

[13] GÓMEZ LÓPEZ, Julio; VILLAR FERNÁNDEZ, Eugenio y ALCAYDE GARCÍA, Alfredo. Seguridad en Sistemas Operativos Windows y GNU/Linux. 2ª Ed. Actualizada. Ra-Ma, 2011.

[14] GÓMEZ VIEITES, Álvaro. Gestión de incidentes de seguridad informática. Madrid: Starbook Editorial, 2011.

[15] GÓMEZ VIEITES, Álvaro. Seguridad en equipos informáticos. Madrid: Starbook Editorial, 2011.

[16] LÓPEZ MATACHANA, Yansenis. (2009). Los virus informáticos: Una amenaza para la sociedad. Cuba: Editorial Universitaria, 2009.

[17] MCCLURE, Stuart; SCAMBRAY, Joel y KURTZ, George. Hackers 6: Secretos y soluciones de seguridad en redes. Mexico: Mc Graw Hill, 2010.

[18] PINTOS FERNANDEZ, Joaquín. Auditorías y continuidad de negocio UF1895. ic editorial, 2014.

[19] RAYA CABRERA, José Luis. Implantación de sistemas operativos. RA-MA, 2010.

[20] RODRÍGUEZ GONZÁLEZ, María Elena. Gestión de datos: bases de datos y sistemas gestores de bases de datos. Barcelona: Editorial UOC, 2010.

[21] SAN MARTIN GONZALEZ, Enrique. Salvaguarda y seguridad de los datos UF1473. Madrid: IC Editorial, 2014.

[22] SANZ MERCADO, Pablo. Seguridad en Linux: Una práctica guiada. Madrid: UAM Ediciones, 2008.

[23] TORRES ESCOBAR, Francisco; PIZARRO GALAN, Ana María. Linux para usuarios. Madrid: Ministerio de Educación de España, 2014.

[24] VALDERREY, Pablo. Administración de sistemas gestores de bases de datos. Madrid: Starbook Editorial, 2013.

ANEXOS

Anexo 1. Formato Auditoría Inicial

LOGO _EMPRESA_ **_Nombre_Empresa_**	**AUDITORIA INICIAL**	**CÓDIGO: XXX-XX-XX** **VERSIÓN: X** **VIGENCIA: XXX de XX** **PÁGINA: X de X**

TIPO DE AUDITORIA APLICADA: AUDITORIA FÍSICA				
	FECHA INICIO	**HORA DE INICIO**	**FECHA TERMINACIÓN**	**HORA TERMINACIÓN**
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

PREGUNTAS	**SI**	**NO**
1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?		
2. ¿Existe una persona responsable de la seguridad?		
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?		
4. ¿Existe personal de vigilancia en la institución?		
5. ¿Existe una clara definición de funciones entre los puestos clave?		
6. ¿Se investiga a los vigilantes cuando son contratados directamente?		
7. ¿Se controla el trabajo fuera de horario?		
8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?		
9. ¿Existe vigilancia en el departamento de cómputo las 24 horas?		
10. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?		
11. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?		
12. ¿El centro de cómputo tiene salida al exterior?		
13. ¿Son controladas las visitas y demostraciones en el centro de cómputo?		
14. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?		

15. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?		
16. ¿Se ha adiestrado el personal en el manejo de los extintores?		
17. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?		
18. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?		
19. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?		
20. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?		
21. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?		
22. ¿Existe salida de emergencia?		
23. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?		
24. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?		
25. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?		
26. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?		
27. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?		
28. ¿Se tienen establecidos procedimientos de actualización a estas copias?		
29. ¿Existe departamento de auditoría interna en la institución?		
30. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?		
31. ¿Se cumplen?		
32. ¿Se auditan los sistemas en operación?		
33. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?		
34. ¿Existe control estricto en las modificaciones?		
35. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?		
36. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?		
37. ¿Se ha establecido que información puede ser acezada y por qué persona? [63]		
ANEXOS		
RESPONSABLE DEL PROCESO	**AUDITOR**	

[63] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

TIPO DE AUDITORIA APLICADA: AUDITORIA DE LA OFIMÁTICA				
	FECHA INICIO	**HORA DE INICIO**	**FECHA TERMINACIÓN**	**HORA TERMINACIÓN**
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

PREGUNTAS	**SI**	**NO**
1. ¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio socioeconómico?		
2. ¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación?		
3. ¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales?		
4. ¿Se cuenta con software de oficina?		
5. ¿Se han efectuado las acciones necesarias para una mayor participación de proveedores?		
6. ¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?		
7. ¿El acceso al centro de cómputo cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado?		
8. ¿Se han implantado claves para garantizar operación de consola y equipo central (mainframe), a personal autorizado?		
9. ¿Se han formulado políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido e intentos de violación?		
10. ¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?		
11. ¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos?		
12. ¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados, preferentemente en bóvedas de bancos?		
13. ¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso?		
14. ¿Todas las actividades del Centro de Computo están normadas mediante manuales, instructivos, normas, reglamentos, etc.?		
15. ¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras?		
16. ¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores, UPS, generadores de energía?		
17. ¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación?		

18. ¿Se han Adquirido equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo?		
19. ¿Si se vence la garantía de mantenimiento del proveedor se contrata mantenimiento preventivo y correctivo?		
20. ¿Se establecen procedimientos para obtención de backups de paquetes y de archivos de datos?		
21. ¿Se hacen revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa?		
22. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos?		
23. ¿Se propende a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y se mantienen actualizadas las versiones y la capacitación sobre modificaciones incluidas?		
24. ¿Existen licencias?[64]		

ANEXOS

_____ **RESPONSABLE DEL PROCESO**	_____ **AUDITOR**

TIPO DE AUDITORIA APLICADA: AUDITORIA DE LA DIRECCIÓN				
	FECHA INICIO	**HORA DE INICIO**	**FECHA TERMINACIÓN**	**HORA TERMINACIÓN**
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

PREGUNTAS	**SI**	**NO**
1. ¿La dirección de los servicios de información desarrollan regularmente planes a corto, medio y largo plazo que apoyen el logro de la misión y las metas generales de la organización?		
2. ¿Dispone su institución de un plan Estratégico de Tecnología de Información?		
3. ¿Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa?		
4. ¿Las tareas y actividades en el plan tienen la correspondiente y adecuada asignación de recursos?		

[64] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

5. ¿Existe un comité de informática?		
6. ¿Existen estándares de funcionamiento y procedimientos que gobiernen la actividad del área de Informática por un lado y sus relaciones con los departamentos usuarios por otro?		
7. ¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados?		
8. ¿Los estándares y procedimientos existentes promueven una filosofía adecuada de control?		
9. ¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica?		
10. ¿La selección de personal se basa en criterios objetivos y tiene en cuenta la formación, experiencia y niveles de responsabilidad?		
11. ¿El rendimiento de cada empleado se evalúa regularmente en base a estándares establecidos?		
12. ¿Existen procesos para determinar las necesidades de formación de los empleados en base a su experiencia?		
13. ¿Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática?		
14. ¿Existe un presupuesto económico? ¿y hay un proceso para elaborarlo?		
15. ¿Existen procedimientos para la adquisición de bienes y servicios?		
16. ¿Existe un plan operativo anual?		
17. ¿Existe un sistema de reparto de costes informáticos y que este sea justo?		
18. ¿Cuentan con pólizas de seguros?		
19. ¿Existen procedimientos para vigilar y determinar permanentemente la legislación aplicable? [65]		

ANEXOS

RESPONSABLE DEL PROCESO	**AUDITOR**

TIPO DE AUDITORIA APLICADA: AUDITORIA DE LA EXPLOTACIÓN

	FECHA INICIO	HORA DE INICIO	FECHA TERMINACIÓN	HORA TERMINACIÓN
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

[65] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

PREGUNTAS	SI	NO
1. ¿Existe personal con conocimiento y experiencia suficiente que organiza el trabajo para que resulte lo más eficaz posible?		
2. ¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		
3. ¿Se aprueban por personal autorizado las solicitudes de nuevas aplicaciones?		
4. ¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		
5. ¿existen procedimientos adecuados para mantener la documentación al día?		
6. ¿tienen manuales todas las aplicaciones?		
7. ¿Existen controles que garanticen el uso adecuado de discos y cintas?		
8. ¿Existen procedimientos adecuados para conectarse y desconectarse de los equipos remotos?		
9. ¿Se aprueban los programas nuevos y los que se revisan antes de ponerlos en funcionamiento?		
10. ¿revisan y evalúan los departamentos de usuario los resultados de las pruebas finales dando su aprobación antes de poner en funcionamiento las aplicaciones?		
11. al poner en funcionamiento nuevas aplicaciones o versiones actualizada ¿funcionan en paralelo las existentes durante un cierto tiempo?		
12. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?		
13. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?		
14. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?		
15. ¿Se lleva control sobre los archivos prestados por la instalación?		
16. ¿Se utiliza la política de conservación de archivos?		
17. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?		
18. ¿Existe un responsable en caso de falla?		
19. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?		
20. Si se queda en el departamento de sistemas, ¿Por cuánto tiempo se guarda?		
21. ¿Existe un registro de anomalías en la información debido a mala codificación?		
22. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?		
23. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?		
24. ¿Se hace una relación de cuándo y a quién fueron distribuidos los listados?		
25. ¿Se controlan separadamente los documentos confidenciales?		
26. ¿Se aprovecha adecuadamente el papel de los listados inservibles?		
27. ¿Existe un registro de los documentos que entran a capturar?		
28. ¿Se lleva un control de la producción por persona?		
29. ¿existe parámetros de control? [66]		

[66] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

ANEXOS	
RESPONSABLE DEL PROCESO	AUDITOR

TIPO DE AUDITORIA APLICADA: AUDITORIA DEL DESARROLLO				
	FECHA INICIO	HORA DE INICIO	FECHA TERMINACIÓN	HORA TERMINACIÓN
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

PREGUNTAS	SI	NO
1. ¿Existe el documento que contiene las funciones que son competencia del área de desarrollo, está aprobado por la dirección de informática y se respeta?		
2. ¿Se comprueban los resultados con datos reales?		
3. ¿Existe un organigrama con la estructura de organización del área?		
4. ¿Existe un manual de organización que regula las relaciones entre puestos?		
5. ¿Existe la relación de personal adscrito al área, incluyendo el puesto ocupado por cada persona?		
6. ¿El plan existe, es claro y realista?		
7. ¿Están establecidos los procedimientos de promoción de personal a puestos superiores, teniendo en cuenta la experiencia y formación?		
8. ¿El área de desarrollo lleva su propio control presupuestario?		
9. ¿Se hace un presupuesto por ejercicio y se cumple?		
10. ¿El presupuesto está en concordancia con los objetivos a cumplir?		
11. ¿El personal de área de desarrollo cuenta con la formación adecuada y son motivados para la realización de su trabajo?		
12. ¿Existen procedimientos de contratación?		
13. ¿Las personas seleccionadas cumplen los requisitos del puesto al que acceden?		
14. ¿Las ofertas de puestos del área se difunden de forma suficiente fuera de la organización y las selecciones se hacen de forma objetiva?		
15. ¿Existe un plan de formación que este en consonancia con los objetivos tecnológicos que se tenga en el área?		

16. ¿El plan de trabajo del área tiene en cuenta los tiempos de formación?		
17. ¿Existe un protocolo de recepción / abandono para las personas que se incorporan o dejan el área?		
18. ¿Existe un protocolo y se respeta para cada incorporación / abandono?		
19. ¿En los abandonos del personal se garantiza la protección del área?		
20. ¿Existe una biblioteca y una hemeroteca accesibles por el personal del área?		
21. ¿Está disponible un número suficiente de libros, publicaciones periódicas, monografías, de reconocido prestigio y el personal tiene acceso a ellos?		
22. ¿El personal está motivado en la realización de su trabajo?		
23. ¿Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área?		
24. ¿Existe rotación de personal y existe un buen ambiente de trabajo?		
25. ¿La realización de nuevos proyectos se basa en el plan de sistemas en cuanto a objetivos?		
26. ¿Las fechas de realización coinciden con los del plan de sistemas?		
27. ¿El plan de sistemas se actualiza con la información que se genera a lo largo de un proceso?		
28. ¿Los cambios en los planes de los proyectos se comunican al responsable de mantenimiento del plan de sistemas?		
29. ¿Existe un procedimiento para la propuesta de realización de nuevos proyectos?		
30. ¿Existe un mecanismo para registrar necesidades de desarrollo de nuevos sistemas?		
31. ¿Se respeta este mecanismo en todas las propuestas?		
32. ¿Existe un procedimiento de aprobación de nuevos proyectos?		
33. ¿Existe un procedimiento para asignar director y equipo de desarrollo a cada nuevo proyecto		
34. ¿Se tiene en cuenta a todas las personas disponibles cuyo perfil sea adecuado a los riesgos de cada proyecto y que tenga disponibilidad para participar?		
35. ¿Existe un protocolo para solicitar al resto de las áreas la participación del personal en el proyecto y se aplica dicho protocolo?		
36. ¿Existe un procedimiento para conseguir los recursos materiales necesarios para cada proyecto?		
37. ¿Se tiene implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda?		
38. ¿La metodología cubre todas las fases del desarrollo y es adaptable a distintos tipos de proyectos?		
39. ¿La metodología y las técnicas asociadas a la misma están adaptadas al entorno tecnológico y a la organización del área de desarrollo?		
40. ¿Existe un catálogo de las aplicaciones disponible en el área?		
41. ¿Existe un registro de problemas que se producen en los proyectos del área?		
42. ¿Existe un catálogo de problemas?		
43. ¿El catálogo es accesible para todos los miembros del área?		
44. ¿Se registran y controlan todos los proyectos fracasados?[67]		

[67] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

ANEXOS	
RESPONSABLE DEL PROCESO	AUDITOR

TIPO DE AUDITORIA APLICADA: AUDITORIA DE BASE DE DATOS				
	FECHA INICIO	HORA DE INICIO	FECHA TERMINACIÓN	HORA TERMINACIÓN
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVOS DE LA AUDITORÍA:				
ALCANCE DE LA AUDITORÍA:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

PREGUNTAS	SI	NO
1. ¿Existe equipos o software de SGBD?		
2. ¿La organización tiene un sistema de gestión de base de datos (SGBD)		
3. ¿Los datos son cargados correctamente en la interfaz gráfica?		
4. Se verifica que los controles y relaciones de datos se realizan de acuerdo a Normalización libre de error		
5. ¿Existe personal restringido que tenga acceso a la BD?		
6. ¿El SGBD es dependiente de los servicios que ofrece el Sistema Operativo?		
7. La interfaz que existe entre el SGBD y el SO es el adecuado		
8. ¿Existen procedimientos formales para la operación del SGBD?		
9. ¿Están actualizados los procedimientos de SGBD?		
10. ¿La periodicidad de la actualización de los procedimientos es Anual?		
11. ¿Son suficientemente claras las operaciones que realiza la BD?		
12. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que están autorizados tengan una razón de ser procesados)		
13. ¿Se procesa las operaciones dentro del departamento de cómputo?		
14. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?		
15. ¿Existe un control estricto de las copias de estos archivos?		
16. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?		
17. ¿Se registran como parte del inventario las nuevas cintas magnéticas que recibe el centro de cómputo?		

18. ¿Se tiene un responsable del SGBD?		
19. ¿Se realizan auditorias periódicas a los medios de almacenamiento?		
20. ¿Se tiene relación del personal autorizado para manipular la BD?		
21. ¿Se lleva control sobre los archivos trasmitidos por el sistema?		
22. ¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD?		
23. ¿Existen integridad de los componentes y de seguridad de datos?		
24. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existen equipos capaces que soportar el trabajo?		
25. ¿El SGBD tiene capacidad de teleproceso?		
26. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?		
27. ¿La capacidad de almacenamiento máximo de la BD es suficiente para atender el proceso por lotes y el proceso remoto? [68]		

ANEXOS

RESPONSABLE DEL PROCESO	**AUDITOR**

TIPO DE AUDITORIA APLICADA: AUDITORIA A LOS SISTEMAS DE REDES

	FECHA INICIO	**HORA DE INICIO**	**FECHA TERMINACIÓN**	**HORA TERMINACIÓN**
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

PREGUNTAS	**SI**	**NO**
1. La gerencia de redes tiene una política definida de planeamiento de tecnología de red?		
2. Esta política es acorde con el plan de calidad de la organización		
3. La gerencia de redes tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes, teniendo en cuenta los posibles cambios tecnológicos o en la organización?		
4. Existe un inventario de equipos y software asociados a las redes de datos?		
5. ¿Existe un plan de infraestructura de redes?		

[68] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

6. El plan de compras de hardware y software para el sector redes está de acuerdo con el plan de infraestructura de redes?		
7. La responsabilidad operativa de las redes está separada de las de operaciones del computador?		
8. Están establecidos controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados		
9. Existen controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas?		
10. Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.?		
11. ¿Existen protocolos de comunicaron establecida?		
12. Existe una topología estandarizada en toda la organización		
13. Existen normas que detallan que estándares que deben cumplir el hardware y el software de tecnología de redes?		
14. ¿La transmisión de la información en las redes es segura?		
15. ¿El acceso a la red tiene password? [69]		
ANEXOS		
RESPONSABLE DEL PROCESO	**AUDITOR**	

TIPO DE AUDITORIA APLICADA: AUDITORIA DE APLICACIONES

	FECHA INICIO	**HORA DE INICIO**	**FECHA TERMINACIÓN**	**HORA TERMINACIÓN**
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				

PREGUNTAS	**SI**	**NO**
1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?		
2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?		
3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?		

[69] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?		
5. Existe la lista de proyectos a corto plazo y largo plazo		
6. Existe una lista de sistemas en proceso periodicidad y usuarios		
7. Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual		
8. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?		
9. ¿Existen fallas de exactitud en los procesos de información?		
10. ¿Se cuenta con un manual de usuario por Sistema?		
11. ¿Es claro y objetivo el manual del usuario?		
12. ¿Qué opinión tiene el manual? _____		
13. ¿Se interviene de su departamento en el diseño de sistemas? [70]		
ANEXOS		
_____ **RESPONSABLE DEL PROCESO**	_____ **AUDITOR**	

[70] Tomado de http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/auditoria_informatica-municipalidad_moquegua.pdf

Anexo 2. Activos de Información - MAGERIT

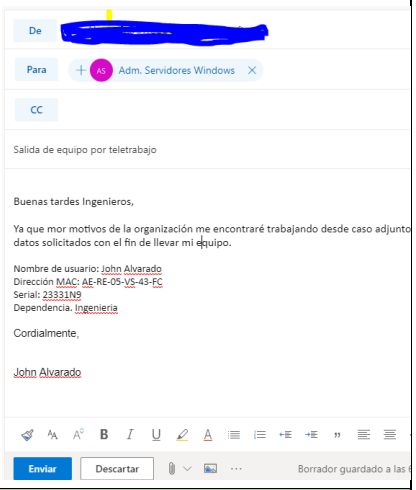
Tabla 1. Activos de Información - MAGERIT

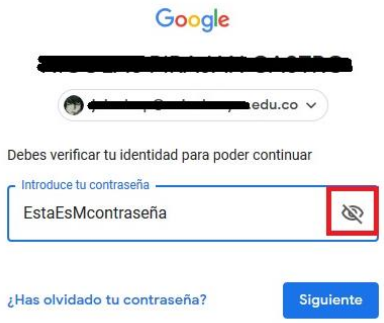
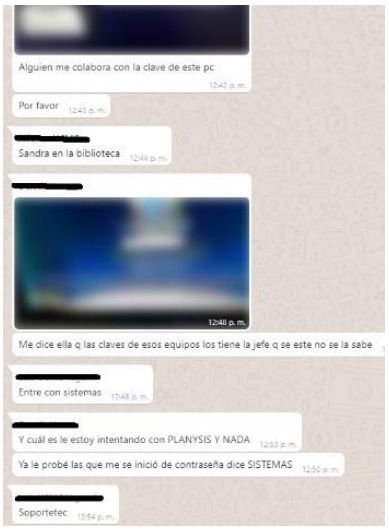
[HW] EQUIPAMIENTO INFORMATICO			
CODIGO	**NOMBRE**	**ACTIVO**	**DESCRIPCION**
[print]	Medios de impresión	Servidor de Impresión	dell en torre PowerEdge T440. Equipo de cómputo que conecta dos impresoras.
[print]	Medios de impresión	Impresora	HP LaserJet Enterprise serie 600
[print]	Medios de impresión	Impresora	SMART MultiXpress M4370LX
[host]	grandes equipos	Servidor de Sistema de Información Core de la organización.	dell en torre PowerEdge T440
[network]	soporte de la red	Servidor DHCP	dell en torre PowerEdge T440. Servidor que asigna y administra de forma dinámica el direccionamiento dentro de la organización
[pc]	Informática personal	Equipo de computo	3 equipos de cómputo para gestión de Sistema de contable en la oficina de Contabilidad.
[pc]	Informática personal	Equipo de computo	3 equipos de cómputo para gestión del Sistema de Información Core de la organización.
[firewall]	cortafuegos	Sistema de protección	Cortafuegos Cisco ASA 5505 Sistema de seguridad que protege la red de datos.
[network]	soporte de la red	Dispositivos de red	6 Switches cisco catalyst 2960 encargados de la interconexión de la red de datos.
[ipphone]	teléfono IP	Teléfonos IP	Sistema de comunicación a través de teléfonos Voz IP
[SW] SOFTWARE - APLICACIONES INFORMÁTICAS			
CODIGO	**NOMBRE**	**ACTIVO**	**DESCRIPCION**
[file]	Servidor de ficheros	Servidor de archivos FTP	dell en torre PowerEdge T130. Equipo de cómputo que almacena y administra los archivos que se están generando en el interior de la organización como son: Digitalización de documento de entrada y de salida, audios y videos generados en reuniones, asambleas y otro tipo de encuentros.
[std]	estándar	Software Apache 2.4.25	Publicador de aplicaciones web.
[std]	estándar	PHP 5.6.30 - 7.1.1	Lenguaje de programación con el que se creó el sistema de información Core de la

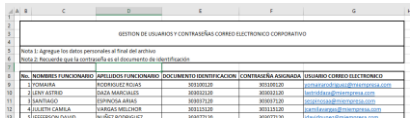
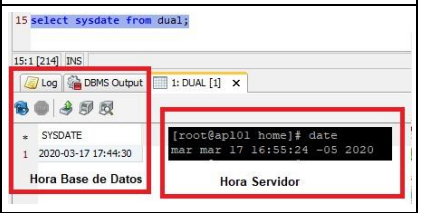
			organización.
[dbms]	sistema de gestión de bases de datos	MySQL 5.7.17	Motor de base de datos donde se sostiene elsistema de información Core de la organización.
[dbms]	sistema de gestión de bases de datos	phpMyAdmin 4.6.6	Herramienta de administración de la base de datos del sistema de información Core de la organización.
[S] SERVICIOS			
CODIGO	**NOMBRE**	**ACTIVO**	**DESCRIPCION**
[file]	almacenamientode ficheros	Servidor de archivos FTP	almacena y administra los archivos que seestán generando en el interior de la organización
[ftp]	transferencia deficheros	Servidor de archivos FTP	almacena y administra los archivos que se están generando en el interior de la organización
[www]	world wide web	Página web	Servicio contratado con la empresa godaddy.com
[P] PERSONAL			
CODIGO	**NOMBRE**	**ACTIVO**	**DESCRIPCION**
[op]	operadores	Técnicos de mantenimiento	Personal técnico encargado de realizar el mantenimiento preventivo a los equipos de cómputo.
[COM] REDES DE COMUNICACIONES			
CODIGO	**NOMBRE**	**ACTIVO**	**DESCRIPCION**
[LAN]	red local	Puntos de acceso alámbricos (hub)	Dispositivos de red encargados de la interconexión de la red de datos
[wifi]	red inalámbrica	Puntos de acceso	Puntos de acceso al servicio de internet en el campus universitario
[PSTN]	red telefónica	Red de telefonía Voz IP	Sistema de comunicación a través de teléfonos Voz IP
[Internet]	Internet	Internet	Internet

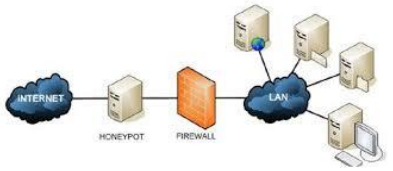
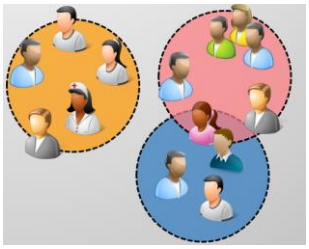
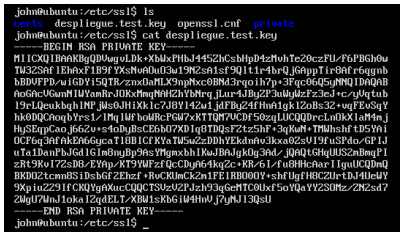
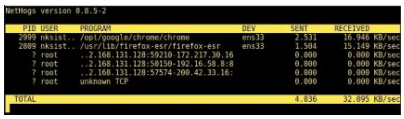
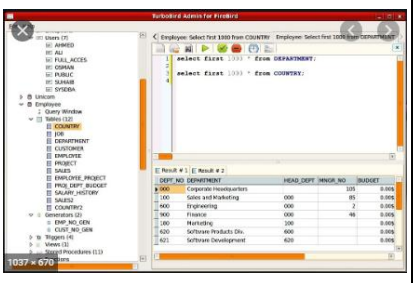
Anexo 3. Plan de Pruebas según los dominios de ISO/IEC 27001:2013

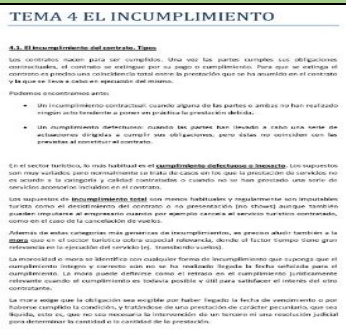
Tabla 2. Plan de pruebas dominios de ISO/IEC 27001:2013

ETAPA	PROCESO	RESULTADO DE LA PRUEBA (vulnerabilidad o amenaza)	EVIDENCIA
5. Políticas de Seguridad de la Información			
5.1. Directrices de la dirección en seguridad de la información	5.1.1. Establecimiento de la política y controles de seguridad de la información con la autorización de la junta directiva.	Existe una política de Seguridad de la información y una guía de con controles de buenas prácticas que fue aprobada en 2015 y no ha sido actualizada ni bien socializada.	
6. Aspectos Organizativos de la Seguridad de la Información			
6.1 Organización interna.	6.1.1 Asignación de responsabilidades para la seguridad de la información.	No se evidencian roles y responsabilidades de la seguridad de la información claros.	
6.2 Dispositivos para movilidad y teletrabajo.	6.2.2 Teletrabajo.	No se cuenta con un procedimiento para la salida de los equipos de la entidad destinados para el teletrabajo. Solo se realiza el envió de un correo.	
7. Seguridad Ligada a los Recursos Humanos			
7.1 Antes de la contratación.	7.1.1 Investigación de antecedentes	No se realiza la verificación de los soportes educativos del personal que se contrata. Se han encontrado diplomas falsos de algunos funcionarios después de su contratación en auditorias.	

8. Gestión de Activos			
8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos	Las políticas de activos no están definidas, no se describen activos. No se evidencia las casillas o sistemas necesarios para inventariar el activo	
8.1 Responsabilidad sobre los activos.	8.1.2 Propiedad de los activos	No se evidencia un sistema que este inventariando los elementos.	
8.1 Responsabilidad sobre los activos.	8.1.3 Uso aceptable de los activos	No se evidencia una política de uso de los activos. El personal no tiene el conocimiento adecuado para la buena manipulación de los activos de información de la compañía.	
9. Control de Accesos			
9.2. Gestión de acceso de usuario.	9.2.4 Gestión de información confidencial de autenticación de usuarios	Las contraseñas de las aplicaciones se encuentran guardadas en los navegadores y sin encriptación.	
9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación	Las contraseñas de los equipos se brindan por medio de un chat.	

9.4 Control de acceso a sistemas y aplicaciones.	9.4.3 Gestión de contraseñas de usuario	La gestión de usuarios de correo electrónico se controla por medio de un Excel guardado en el equipo del administrador de dominio.	
10. Cifrado			
10.1 Controles criptográficos.	10.1.1 Política de uso de los controles criptográficos	Las llaves de criptografía les hace falta una política de eliminación de malware. Se evidencian el uso de llaves criptográficas, pero les hace falta una política para también eliminar malware en los dispositivos extraíbles.	
11. Seguridad física y Ambiental			
11.2 Seguridad de los equipos.	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	Los funcionarios consumen alimentos en los puestos de trabajo.	
12. Seguridad en la Operativa			
12.1 Responsabilidades y procedimientos de operación.	12.1.1 Documentación de procedimientos de operación	La documentación se encuentra desorganizada y sin controles.	
12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso	Los equipos informáticos se encuentran con el antivirus desactualizado y caducado.	
12.4 Registro de actividad y supervisión	12.4.4 Sincronización de relojes	Los relojes de los servidores de base de datos no concuerdan con los relojes de los servidores de aplicaciones.	

12.6 Gestión de la vulnerabilidad técnica	12.6.2 Restricciones en la instalación de software	No existen controles para la instalación de software en las máquinas.	
13. Seguridad en las Telecomunicaciones			
13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red.	No se evidencia una política de acceso a la red para la protección o intrusión de diferentes malware.	
13.1 Gestión de la seguridad en las redes	13.1.3 Segregación de redes	Se determina que no tienen separados a los dos grupos fundamentales en las redes, trabajadores y usuarios visitantes.	
14. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.			
14.1 Requisitos de seguridad de los sistemas de información.	14.1.3 Protección de las transacciones por redes telemáticas.	El SSL de la entidad se encuentra desactualizado.	
14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.2 Procedimientos de control de cambios en los sistemas.	No se cuenta con un procedimiento para el control de cambios en los sistemas en producción.	 SO Obsoleto
14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.6 Seguridad en entornos de desarrollo.	No se evidencian ambientes separados de entornos de pruebas, desarrollo capacitación y producción.	

<table>
<tr><th colspan="4">15. Relaciones con Suministradores</th></tr>
<tr><td rowspan="2">15.1 Seguridad de la información en las relaciones con suministradores.</td><td>15.1.1 Política de seguridad de la información para suministradores</td><td>Existen formatos establecidos para la realización de procesos contractuales y se realizan mediante la plataforma SECOP II.</td><td rowspan="2"> 
TEMA 4 EL INCUMPLIMIENTO</td></tr>
<tr><td>15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores</td><td>En los formatos establecidos no se establece una matriz de riesgo contractual.</td></tr>
<tr><th colspan="4">18. Cumplimiento</th></tr>
<tr><td>18.1 Cumplimiento de los requisitos legales y contractuales.</td><td>18.1.3 Protección de los registros de la organización.</td><td>No se cuenta con un procedimiento contra la perdida, falsificación o destrucción de registros.</td><td> 
VALORES DE LAS DIFERENTES PARTIDAS EN CADA EJERCICIO
Registro de diferentes partidas en cada ejercicio.</td></tr>
<tr><td>18.1 Cumplimiento de los requisitos legales y contractuales.</td><td>18.1.4 Protección de datos y privacidad de la información personal.</td><td>No se cuenta con una política definida frente a la protección de datos personales.</td><td></td></tr>
</table>

Anexo 4. Formato Informe Ejecutivo de Auditoria

LOGO _EMPRESA_ **_Nombre_Empresa_**	**INFORME EJECUTIVO DE AUDITORÍA**			**CÓDIGO: XXX-XX-XX** **VERSIÓN: X** **VIGENCIA: XXX de XX** **PÁGINA: X de X**
	FECHA INICIO	**HORA DE INICIO**	**FECHA TERMINACIÓN**	**HORA TERMINACIÓN**
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				
INTRODUCCIÓN				
OBJETIVOS				
ALCANCE				
DESARROLLO DE LA AUDITORÍA				
HALLAZGOS				
OBSERVACIONES				
RECOMENDACIONES				
CONCLUSIÓN DE AUDITORÍA				
ANEXOS				
_____ **RESPONSABLE DEL PROCESO**			_____ **AUDITOR**	

Anexo 5. Formato Informe Técnico de Auditoria

LOGO _EMPRESA_ **_Nombre_Empresa_**	**INFORME TECNICO DE AUDITORÍA**			**CÓDIGO: XXX-XX-XX** **VERSIÓN: X** **VIGENCIA: XXX de XX** **PÁGINA: X de X**
	FECHA INICIO	**HORA DE INICIO**	**FECHA TERMINACIÓN**	**HORA TERMINACIÓN**
	DD-MM-YYYY	HH:MM	DD-MM-YYYY	HH:MM
OBJETIVO:				
ALCANCE:				
RESPONSABLE PROCESO:				
AUDITOR:				
FUNCIONARIOS ENTREVISTADOS:				
INTRODUCCIÓN				
FASE RECONOCIMIENTO				
FASE DE ANALISIS DE VULNERABILIDADES				
FASE DE EXPLOTACION				
FASE DE POST-EXPLOTACION				
RIESGOS Y AMENAZAS				
CONCLUSIONES Y RECOMENDACIONES				
ANEXOS				
_____ **RESPONSABLE DEL PROCESO**			_____ **AUDITOR**	