UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

TEMA

"HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A."

Proyecto de Trabajo de Graduación. Modalidad: Proyecto de investigación, Presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLÍNEA DE INVESTIGACIÓN: Seguridad Informática

AUTOR: Alexander Israel Rojas Buenaño

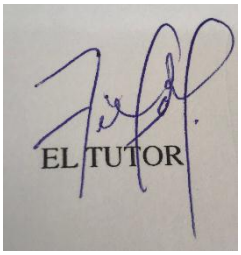
TUTOR: PhD. Félix Oscar Fernández Peña

AMBATO – ECUADOR
2018

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: "Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa Plasticaucho Industrial S.A.", del señor Alexander Israel Rojas Buenaño, estudiante de la Carrera de Ingeniería en Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

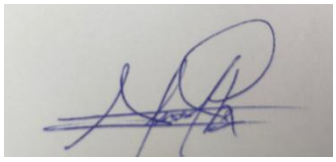
Ambato junio, 2018



AUTORÍA

El presente Proyecto de Investigación titulado: "Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa Plasticaucho Industrial S.A.", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato junio, 2018



Alexander Israel Rojas Buenaño

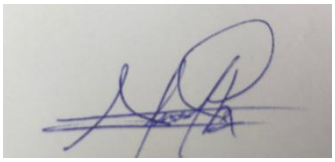
CC: 160046869-6

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato junio, 2018

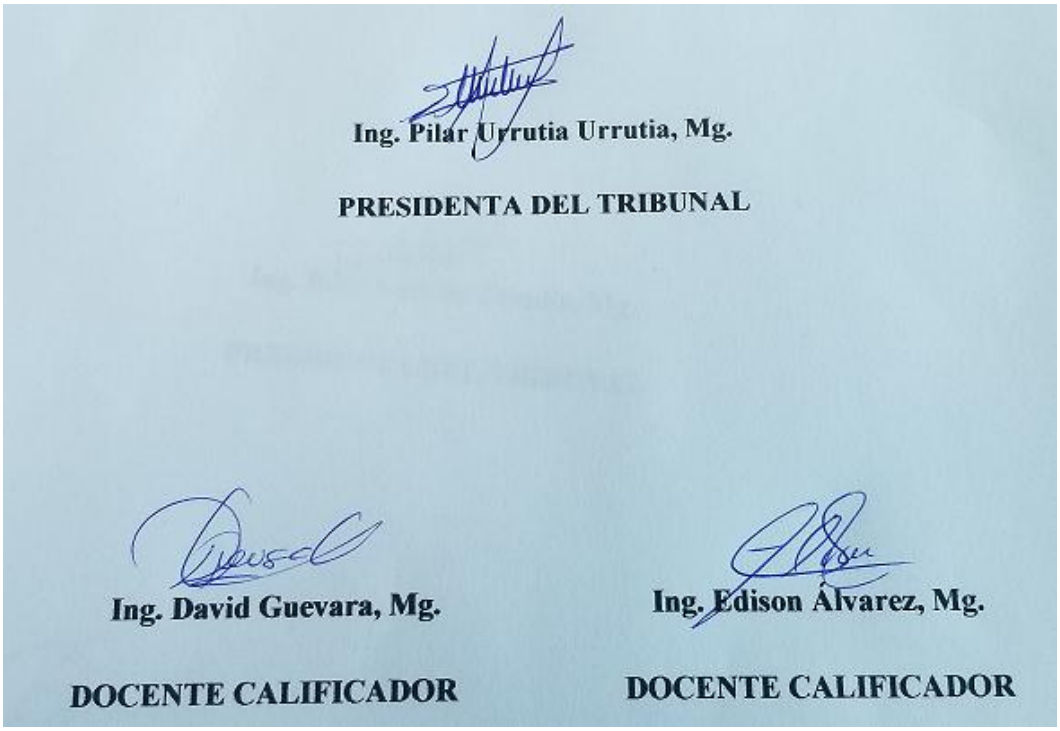


Alexander Israel Rojas Buenaño

CC: 160046869-6

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. David Guevara e Ing. Edison Álvarez, revisó y aprobó el Informe Final del Proyecto de Investigación titulado "HACKING ÉTICO PARA ANALIZAR Y EVALUAR LA SEGURIDAD INFORMÁTICA EN LA INFRAESTRUCTURA DE LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.", presentado por el señor Rojas Buenaño Alexander Israel de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.



AGRADECIMIENTO:

Agradezco a mi familia por su apoyo incondicional en cada etapa de vida. Agradezco a mi tutor por la guía dada en la elaboración del proyecto. De igual manera agradezco a la empresa que me dio la apertura para realizar el proyecto y finalmente a mis amigos y compañeros de trabajo por su incansable motivación.

Alexander Israel Rojas Buenaño

ÍNDICE GENERAL

CAPÍTULO I 16
EL PROBLEMA 16
1.1. Tema 16
1.2. Planteamiento del problema 16
1.3. Delimitación 18
1.3.1. Delimitación de Contenidos 18
1.3.2. Delimitación Espacial 18
1.3.3. Delimitación Temporal 18
1.4. Justificación 18
1.5. Objetivos 19
1.5.1. General 19
1.5.2. Específicos 19
CAPÍTULO II 20
MARCO TEÓRICO 20
2.1 Antecedentes investigativos 20
2.2 Fundamentación Teórica 21
2.2.1 El Origen 21
2.2.2 Hechos importantes en la historia del hacking 21
2.2.3 Hackers 22
2.2.4 Tipos de Hackers 22
2.2.5 Por qué el Hacking Ético 23
2.2.6 Hacking ético vs Auditoría Informática 23
2.2.7 Tipos de Pentest 23
2.2.8 Metodología 24
2.2.9 Etapas del hacking 25
2.3 Propuesta de solución 26
CAPÍTULO III 27
METODOLOGÍA 27
3.1 Modalidad de la investigación 27
3.2 Recolección de información 28
3.3 Procesamiento y análisis de datos 28

3.4 Desarrollo del proyecto 28
CAPÍTULO IV 29
DESARROLLO DE LA PROPUESTA 29
4.1 Planificación 29
4.2 Recolección de Información 36
4.3 Enumeración 46
4.4 Análisis 47
4.5 Explotación 63
4.6 Documentación 73
CAPÍTULO V 83
CONCLUSIONES Y RECOMENDACIONES 83
ANEXOS 2

ÍNDICE DE GRÁFICOS

Gráfico 1 - Enfoque basado en DragonJar [13] 30
Gráfico 2- Google 31
Gráfico 3 - TheHarvester 32
Gráfico 4 - Whois 32
Gráfico 5 - Nslookup 32
Gráfico 6 - Fierce 33
Gráfico 7 - ejemplo de FOCA pentest 33
Gráfico 8 - Consola nmap 34
Gráfico 9 - Logo Nessus 34
Gráfico 10 - Logo OpenVAS 35
Gráfico 11 - Logo Metasploit 36
Gráfico 12 - Tecnología sitio web plasticaucho.com 37
Gráfico 13 - Tecnología del sitio web Plasticaucho.com.ec 38
Gráfico 14 - Búsqueda para listar directorios 39
Gráfico 15 - Búsqueda de páginas de administración 39
Gráfico 16 - Búsqueda de páginas vulnerables a la redirección arbitraria 40
Gráfico 17 – Búsqueda de vulnerabilidades de inyección de SQL 40
Gráfico 18 - Búsqueda con TheHarvester 41
Gráfico 19 - Resultado TheHarvester correos 42
Gráfico 20 - Búsqueda TheHarvester dominios 42
Gráfico 21 – Resultado parcial Whois plasticaucho.com.ec 43
Gráfico 22 –Resultado parcial Whois plasticaucho.com 43
Gráfico 23 - Resultado Whois.net 44
Gráfico 24 - Resultado nslookup 44
Gráfico 25 - Resultados Fierce 45
Gráfico 26 – Análisis de metadatos con FOCA 45
Gráfico 27 - Red corporativa 46
Gráfico 28 - Descubrimiento de la red interna 47
Gráfico 29 - Número de hosts activos en la red 47
Gráfico 30 - Resumen de SO escaneo nmap 49
Gráfico 32 - Dashboard OpenVAS 50
Gráfico 33 - Targets OpenVAS 51
Gráfico 34 - Tasks OpenVAS 51

Gráfico 35 - Dashboard Nessus 52
Gráfico 36 - Tipos de escaneos en Nessus 53
Gráfico 37 - Vulnerabilidades críticas host 10.192.168.1 OpenVAS 55
Gráfico 38 - Vulnerabilidades críticas host 10.192.168.1 Nessus 55
Gráfico 39 - Vulnerabilidades medias host 10.192.168.3OpenVAS 56
Gráfico 40 -Vulnerabilidades críticas host 10.192.168.3 Nessus 57
Gráfico 41 - Vulnerabilidades críticas host 10.192.168.6 OpenVAS 57
Gráfico 42 - Vulnerabilidades medias host 10.192.168.6 58
Gráfico 31 - Gráfico SO clientes proporcionados por la empresa 59
Gráfico 43 - Vulnerabilidades críticas OpenVAS equipo W- XP 61
Gráfico 44 - Vulnerabilidades críticas Nessus equipo W- XP 61
Gráfico 45 - Vulnerabilidades críticas OpenVAS equipoW- 7 62
Gráfico 46 - Vulnerabilidades críticas Nessus equipoW-7 62
Gráfico 47 - Vulnerabilidades críticas OpenVAS equipo W-8 62
Gráfico 48 - Vulnerabilidades críticas Nessus equipo W- 8 63
Gráfico 43 - Consola de Metasploit 63
Gráfico 44 – Comunicado interno de Telefónica Movistar tras Wannacry [27] 65
Gráfico 45 - Módulo Auxiliar ms17_010_command 66
Gráfico 46 - Resultado ejecución ms17_010_command 67
Gráfico 47 - Módulo de explotación ms17_010_psexec 67
Gráfico 48 - Resultado ejecución ms17_010_psexec 67
Gráfico 49 - Ejecución getsystem 67
Gráfico 50 - PID proceso local 68
Gráfico 51 - Migración de proceso meterpreter 68
Gráfico 52 – Consola Mimikatzs 68
Gráfico 53 - Credenciales obtenidas Mimikatz 69
Gráfico 54 - Vulnerabilidad MS15-034 metasploitable 70
Gráfico 55 - Ejecución exploit ms15_034_ ulonglongadd 70
Gráfico 56 - Event Viewer error en el sistema 71
Gráfico 63 - Resultado acceso telnet sin credenciales 71
Gráfico 64 - Vulnerabilidad protocolo SMB equipo W-XP 72
Gráfico 65 - Vulnerabilidad al protocolo RDP 73
Gráfico 66 - Vulnerabilidad SMB equipo W-8 73

ÍNDICE DE TABLAS

Tabla 1 - Resumen google hacking 41
Tabla 2 - Resumen de SO escaneo nmap 48
Tabla 3 - Equipos Windows Server 49
Tabla 4 - Equipos GNU/Linux 50
Tabla 5 - Escaneo OpenVAS hosts Windows Server 51
Tabla 6 - Escaneo OpenVAS hosts GNU/Linux 52
Tabla 7 - Escaneo Nessus hosts Windows Server 53
Tabla 8 - Escaneo Nessus hosts GNU/Linux 54
Tabla 9 - Resumen SO clientes proporcionados por la empresa 58
Tabla 10 - Resumen de Vulnerabilidades OpenVAS equipos W-XP 59
Tabla 11 - Resumen de Vulnerabilidades OpenVAS equipos W-7 60
Tabla 12 -Resumen de Vulnerabilidades OpenVAS equipos W-8 60
Tabla 13 - Resumen de Vulnerabilidades Nessus equipos W-XP 60
Tabla 14 - Resumen de Vulnerabilidades Nessus equipos W-7 60
Tabla 15 - Resumen de Vulnerabilidades Nessus equipos W-8 60

RESUMEN EJECUTIVO

El impulso tecnológico que ha tenido el mundo se ha visto frustrado por hechos lamentables efectuados por ciberdelincuentes. El 2017 fue un año marcado por ataques de tipo ransomware que infectaron un sin número de ordenadores cifrando la información de usuarios comunes pasando por departamentos de gobierno, hospitales, y llegando a empresas multinacionales que se vieron obligados a parar sus operaciones para detener la propagación del malware en sus infraestructuras.

Es por ello que a nivel de infraestructura tecnológica un factor decisivo a la hora de sufrir un ataque informático implica una adecuada gestión de configuración en los servicios implementados y una correcta administración y despliegue de actualizaciones en sistemas operativos y aplicaciones. Si un atacante logra penetrar la seguridad perimetral y obtener acceso a la red interna puede aprovechar deficientes configuraciones en los servicios internos y buscar vulnerabilidades que no han sido parchadas, esto conllevaría a que en algunos casos comprometa toda la infraestructura tecnológica.

La presente investigación tuvo como objeto simular las acciones de un atacante a través de un ejercicio de Hacking Ético. Esto permitió analizar la infraestructura de la empresa teniendo como principio la ética y la confidencialidad. Además del análisis se demostró cómo explotar y aprovechar vulnerabilidades de la misma forma en la que un ciberdelincuente lo haría. Se mostró la criticidad de la materialización de un ataque buscando comprometer equipos y extrayendo información delicada de la organización.

Adicionalmente se propusieron acciones correctivas que permiten disminuir el riesgo de un ataque y robustecer la infraestructura interna de la empresa. Se recomienda garantizar una actualización continua de la estrategia de seguridad informática de la entidad para la que se realizó el trabajo.

ABSTRACT

The technological impulse that has had the world has been frustrated by lamentable facts effected by cybercriminals. 2017 was a year marked by ransomware-type attacks that infected countless computers by encrypting the information of ordinary users passing through government departments, hospitals, and reaching multinational companies that were forced to stop their operations to stop the spread of the virus. malware in its infrastructures.

That is why, at the level of technological infrastructure, a decisive factor when suffering a computer attack involves an adequate configuration management in the services implemented and a correct administration and deployment of updates in operating systems and applications. If an attacker manages to penetrate the perimeter security and gain access to the internal network, it can take advantage of deficient configurations in the internal services and look for vulnerabilities that have not been patched, this would entail that in some cases it compromises the entire technological infrastructure.

The purpose of the present investigation was to simulate the actions of an attacker through an Ethical Hacking exercise. This allowed us to analyze the company's infrastructure based on ethics and confidentiality. In addition to the analysis, it was demonstrated how to exploit and exploit vulnerabilities in the same way that a cybercriminal would. The criticality of the materialization of an attack was shown, seeking to commit teams and extract sensitive information from the organization.

In addition, corrective actions were proposed to reduce the risk of an attack and strengthen the company's internal infrastructure. It is recommended to guarantee a continuous update of the IT security strategy of the entity for which the work was carried out.

INTRODUCCIÓN

El presente trabajo de investigación se enfocó en ejecutar un análisis del estado de la seguridad en la infraestructura de la empresa Plasticaucho Industrial a través de un ejercicio de Hacking Ético.

La necesidad que enfrenta la empresa nace de una observación de auditoría interna que busca proteger la disponibilidad de los servicios tecnológicos y la confidencialidad de la información que puede verse comprometida si un ciberdelincuente perpetra un ataque a su infraestructura.

Se consideró los tipos de pentest que existen y la factibilidad de su implementación. Con el apoyo de la empresa fue posible llevar a cabo un análisis de caja gris que contempló la entrega de cierta información inicial como parte de la estructura de la red interna.

Para la ejecución del proyecto fue importante considerar las fases que implica un Hacking Ético, indistintamente de las metodologías actuales. Se siguió una secuencia de etapas que permitió cumplir el objetivo; estas son: recolección de la información, enumeración, análisis, explotación y documentación. A este conjunto de etapas se agregó la planificación, fase inicial en la cual se detalla que herramientas o técnicas nos facultaron llevar a cabo el Hacking Ético.

En el desarrollo del proyecto se analizó información pública de la empresa que se encontraba en internet lo cual permitió conocer que varios servicios como el sitio web que se encuentra hospedado con un proveedor. Siguiendo las etapas indicadas, se descubrió información considerable como los sistemas operativos que maneja Plasticaucho Industrial S.A.; posteriormente se ejecutó un análisis de vulnerabilidades de los equipos identificados. Esto derivó en información que permitió identificar debilidades que podrían ser aprovechadas para comprometer los equipos analizados.

CAPÍTULO I

EL PROBLEMA

1.1. Tema

"Hacking Ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa Plasticaucho Industrial S.A."

1.2. Planteamiento del problema

La seguridad informática ha tomado mucho impulso en los últimos años y se ha convertido en un campo de gran interés para las empresas y usuarios en general [1], quienes empiezan a tomar consciencia de la importancia de salvaguardar sus activos tangibles e intangibles [2]. Sin embargo, hay que considerar que años atrás, al implementar alguna herramienta o algo tan escueto como un servidor, el fin principal que se buscaba era la funcionalidad, llegando a utilizar configuraciones por defecto o la incorrecta gestión de actualizaciones, creando brechas de seguridad que pueden ser aprovechadas hoy por hoy por piratas informáticos. Desde el año anterior, el mundo se ha hecho eco de noticias en las que grandes empresas se han visto comprometidas al ser víctimas de ataques y quedando expuestas. Entre algunos de los casos que causaron mayor revuelo podemos destacar el robo de datos de millones de cuentas de usuarios de Yahoo y el caso de filtración de información correspondiente a empleados del Departamento de Justicia de Estados Unidos [3].

En el ámbito nacional ya se ha venido hablando del tema. En este sentido, vale mencionar que el Estado tuvo contacto con el colectivo Hacking Team que fue

expuesto en su momento y en su lista de clientes constaba Ecuador como uno de los países involucrados en sus servicios [4]. En el sector privado encontramos el caso del Banco del Austro que sufrió un ciberataque que le costó cerca de 9 millones de dólares. Según su versión, indican que "un usuario no identificado estaba usando el sistema de ordenadores de su banco" [4]; este es solo uno de los varios casos que se han presentado en el país. Por ello, es de vital importancia ser proactivos a la hora de identificar brechas de seguridad que permitan anticiparse a los atacantes y llevar una adecuada gestión de la seguridad informática.

Plasticaucho Industrial S.A. es una empresa Tungurahuense con más de 85 años de experiencia en el mercado. Con el pasar de los años y gracias al trabajo realizado han conseguido tener representación a nivel nacional e incluso en los países de Colombia y Perú. Debido a la envergadura de los procesos y la cantidad de información que empezó a manejar la empresa, tuvieron la necesidad de recurrir a un sistema ERP (del inglés Enterprise Resource Planning) siendo SAP R/3 el elegido a convertirse en el sistema CORE del negocio. A través del mismo gestionan gran parte de procesos como: gestión financiera, gestión de activos, gestión de materiales entre otros. La empresa también dispone de sistemas que trabajan por fuera del ERP. Estos dan soporte a procesos como: nómina, gestión médica, contact center, telefonía, etc. Estos sistemas son administrados y gestionados en los centros de datos ubicados en la ciudad de Ambato, sector Parque Industrial y Catiglata.

En el año 2016, resultado de una auditoría interna realizada a los procesos del departamento de Tecnología de la Información, se levanta como observación que no existe una actividad de control que permita realizar auditorías de hacking ético y verificar vulnerabilidades para evitar que ingresen en los sistemas de la empresa, esto se puede evidenciar en el anexo A. Como consecuencia, se aprobó llevar a cabo un ejercicio de hacking ético que permitiera analizar y evaluar las vulnerabilidades que pueden ser explotadas en los sistemas de la empresa, generando como resultado un conjunto de remediaciones a implementar con el fin de prevenir ataques de cibercriminales.

1.3. Delimitación

1.3.1. Delimitación de Contenidos

El campo de la investigación está basado en la Tecnología Informática:

Área Académica: Hardware y Redes.

Línea de Investigación: Sistemas Administradores de Recursos.

Sub línea: Seguridad Informática.

1.3.2. Delimitación Espacial

La presente investigación se llevó a cabo en las instalaciones de la empresa PLASTICAUCHO INDUSTRIAL S.A.

1.3.3. Delimitación Temporal

La presente investigación se desarrolló en los 5 meses posteriores a la aprobación del proyecto por parte del H. Consejo Directivo.

1.4. Justificación

Plasticaucho Industrial S.A., al darse cuenta de la necesidad de cuidar del robo y la confidencialidad de su información, precisa una estimación del estado de la seguridad informática en su infraestructura tecnológica. El presente trabajo busca ser útil y beneficiar a la empresa, quien muestra gran interés al contemplar el hacking ético como una actividad de control obligatoria resultado de una observación de auditoría interna (Véase anexo A).

El presente trabajo concibe ser sugestivo para Plasticaucho Industrial S.A. al representar el primer análisis de seguridad a realizarse en su infraestructura tecnológica. De esta manera se conseguirá tener un panorama detallado y claro de las vulnerabilidades y amenazas a las cuales pueden estar expuestos sus sistemas.

La importancia teórico-práctica de este trabajo contempla el uso de una metodología que permita llevar a cabo todo el proceso desde el reconocimiento y

recolección de información hasta proponer medidas para contrarrestar los fallos de seguridad identificados y aportar conocimientos técnicos y mejoras en los procesos de gestión para el departamento de Tecnología de la Información, así como al investigador.

El impacto de este trabajo ha de ser determinante para las actividades que lleva a cabo el personal del departamento de Tecnología de la Información y Proyectos. Los resultados permiten identificar las fortalezas y debilidades encontradas de manera que se corrijan brechas de seguridad. De esta manera, la empresa busca una adecuada gestión de control para reducir el riesgo de un ataque y robo de información confidencial a la empresa.

1.5. Objetivos

1.5.1. General

Aplicar Hacking Ético para analizar y evaluar la seguridad informática en la infraestructura tecnológica de la empresa Plasticaucho Industrial S.A.

1.5.2. Específicos

- Examinar y descubrir la infraestructura tecnológica de la empresa Plasticaucho S.A. desde una perspectiva de hacking ético para determinar la metodología a emplear.
- Medir y evaluar el grado de exposición ante vulnerabilidades conocidas en la infraestructura identificada.
- Proponer medidas de protección en base a los resultados obtenidos para fortalecer la seguridad informática en la empresa.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes investigativos

El crecimiento exponencial de las redes en internet ha derivado en grandes beneficios, como por ejemplo: comercio electrónico (e-commerce), trabajo colaborativo, publicidad y distribución de información, por nombrar algunos casos. La interconexión resultante es inmensurable. Lamentablemente estos avances tecnológicos también traen consigo un lado oscuro: los cibercriminales. Estos atacantes buscan beneficiarse y sacar provecho de información personal o corporativa y venderla al mejor postor. En otros escenarios, incluso buscan generar la indisponibilidad de los servicios tecnológicos [5].

La naturaleza propia de internet no permite que exista un gobierno de control, aunque en algunos países existan leyes o agencias que traten de intervenir la libertad que existe en el mundo cibernético; este principio es violentado por los atacantes. “Los altos mandos y gerencias de empresas necesitan ver y entender claramente estas amenazas para protegerse” [6].

“El riesgo de irrupción en los sistemas es alto considerando que los cibercriminales diariamente crean nuevos, mejores y sofisticados ataques que buscan dañar y sobrepasar los sistemas de seguridad” [7]; una posibilidad de mejorar la seguridad y robustecerla es a través de un hacking ético que permita conocer y evaluar las debilidades existentes en la infraestructura antes de sufrir un ataque que conlleve a los problemas mencionados anteriormente.

2.2 Fundamentación Teórica

2.2.1 El Origen

En sus inicios el desarrollo y avances tecnológicos se realizaban con la concepción de ofrecer funcionalidad y operatividad, de hecho podemos tomar como ejemplo varios protocolos en los que se sustentan servicios de tecnología y comunicaciones que se siguen usando hasta la actualidad (http, ftp, etc.), estos no fueron pensados para cuidar de la seguridad de los usuarios o sistemas, simplemente buscaban cumplir su función.

En ese entonces, la mayoría de técnicos y usuarios no tenían una noción madura acerca de la seguridad de la información o de intrusiones realizadas por terceros no autorizados en sus sistemas. Sin embargo la curiosidad y la incentiva fueron más allá y permitieron contestar algunas preguntas, el: ¿cómo? y ¿porque? del funcionamiento de protocolos y servicios, además de sus debilidades y vulnerabilidades. Como consecuencia se empezaron a conocer casos de intrusión a través de los medios de prensa y se hizo notoria la falta de personal capacitado y consciente de la seguridad de la información [8].

2.2.2 Hechos importantes en la historia del hacking

A continuación se exponen algunos de los hechos relevantes[8] :

1982: John Shoch (uno de los creadores de Ethernet) junto a un colega, escribieron el primer reporte sobre un gusano (worm), tomando ese nombre de una novela de ciencia ficción de 1975 en la que, bajo el nombre de Taperworms, describían a programas autómatas que viajaban por las redes transportando información.

1983: Ese año se estrenó la película War Games, en la que el protagonista ingresaba en una base militar a través de su computadora y casi desata una guerra nuclear.

1984: Se crearon la publicación 2600, el CCC chaos computer club, Legion of doom y la división de fraude con tarjetas y computadoras del Servicio Secreto.

1988: Robert Tappan Morris soltó un gusano en Arpanet (como se llamaba internet antes) y logró infectar miles de servidores Unix. Fue enjuiciado y condenado a cumplir 400 horas de trabajo social.

1992: Kevin Mitnik, luego de estar prófugo y ser atrapado por el FBI, fue sentenciado por robo de software e intrusiones en organizaciones.

1994: Vladimir Levin robó, desde San Petersburgo, a través de los sistemas de Citi bank, más de 10 millones de dólares por medio de transferencias a sus cuentas.

2.2.3 Hackers

Se han llevado a cabo varias discusiones un poco acaloradas en cuanto a las connotaciones positivas o negativas que implica la palabra, podemos asumir que un hacker es alguien capaz de llegar más allá de los límites, consiguiendo hacer cosas que van desde lo curioso hasta la asombroso. En otras palabras son gente con capacidades especiales en la informática adquiridas tras largas horas de estudio y práctica [9].

2.2.4 Tipos de Hackers

La sola palabra hacker no define si una persona usa su conocimiento para el bien o el mal, es por ello que el término se ha dividido en tres tipos:

- **Hackers de sombrero blanco:** también llamados hackers éticos, son considerados profesionales de la seguridad informática quienes realizan test de intrusión en corporaciones o instituciones para buscar fallas de seguridad siempre bajo el consentimiento de los involucrados [5].
- **Hackers de sombrero negro:** son lo opuesto a los hackers de sombrero blanco, también denominados crackers pues no trabajan en conjunto con

un ente, buscan causar daño y robar información, dañar y sabotear sistemas para su fin personal o de un tercero [5].

- **Hackers de sombrero gris:** aunque el término es un poco ambiguo, se puede decir que es una combinación híbrida entre los hackers de sombrero blanco y sombrero negro [5].

2.2.5 Por qué el Hacking Ético

El Hacking Ético o test de penetración es visto como un procedimiento de ciberseguridad pues se trata de emular un ataque real para filtrarse en un sistema informático o una red bajo el consentimiento del propietario con la intención de descubrir debilidades y vulnerabilidades que un cibercriminal podría utilizar. Esto permite a la compañía entender las necesidades en seguridad que afronta y mejorar sus sistemas según lo requirieran [6].

2.2.6 Hacking ético vs Auditoría Informática

Cuando se empieza en el tema de la seguridad se presenta algo de confusión entre un hacking ético y una auditoría informática. De hecho mucha gente lo confunde en el medio, sin embargo existen grandes diferencias.

La auditoría informática trata las políticas de seguridad de la compañía y el cumplimiento de estas o cómo se están llevando en los procesos. Se busca validar que existan controles de la seguridad y en muchos casos puede no ser técnica.

Por otro lado un hacking ético se enfoca en vulnerabilidades que pueden ser explotadas por terceros y que puedan ser explotadas, para de esta manera comprobar la resistencia que ofrece el sistema ante este tipo de ataques [10].

2.2.7 Tipos de Pentest

Existen tres tipos de hacking ético o pentest que son utilizados [11]:

- **Pentest de caja negra:** En este tipo de test no se tiene mayor información, no se conoce nada acerca de los sistemas o arquitectura a atacar. Se tiene que recopilar toda la información sobre el objetivo.

- **Pentest de caja blanca:** Al contrario del anterior, en este tipo de pentest se proporciona la mayor información posible acerca del objetivo, aplicaciones, sistemas operativos, arquitectura, entre otros datos.
- **Pentest de caja gris:** En este test se tiene parte o limitada información acerca de los detalles internos.

2.2.8 Metodología

En cada pentest, la metodología es un punto importante a definir pues permite conocer el cómo debe realizarse, dependiendo de las valoraciones que se consideren al momento de planificar la ejecución. A continuación se listan las principales metodologías que han sido encontradas en la literatura consultada:

- **OSSTMM (Open Source Security Testing Methodology Manual)**
  El principal propósito está centrado en proporcionar un manual científico para la caracterización precisa de seguridad operacional (OpSec) mediante el análisis y la correlación de los resultados de prueba en una forma confiable y consistente [12].
  Sugiere un ámbito bastante amplio para realizar validaciones en diferentes módulos y canales que buscan ir más allá de la parte técnica, llegando incluso a auditar procesos en la parte operativa. Actualmente, se dispone del borrador de la versión 4.0 únicamente para miembros de ISECOM (Instituto para la Seguridad y Metodologías Abiertas). La versión 3.0 se encuentra disponible para descarga desde su sitio oficial y en internet se puede encontrar la versión 2.1 de la que se toman algunas plantillas para documentación de ciertas fases del hacking ético.
- **ISSAF (Information Systems Security Assessment Framework)**
  Su objetivo es proporcionar procedimientos muy minuciosos para la comprobación de sistemas de información que reflejen situaciones reales.
  Constituye un marco de trabajo que detalla cómo evaluar la seguridad de los sistemas. Sugiere estándares de pruebas para diferentes ámbitos de dominio. Una de las características de este marco de trabajo es que sugiere las herramientas a utilizar en cada fase.

ISSAF se utiliza principalmente evaluar los requisitos de organizaciones y puede ser utilizado como referencia para nuevas implementaciones relacionadas con la seguridad de la información [11]. Sin embargo, en los últimos años no ha tenido mucha connotación pues su última actualización fue en la versión 0.2.1, liberada en el 2006.

- **OWASP Testing Guide (Open Web Application Security Project Testing Guide)**

  Esta guía se encuentra actualmente en su versión 4.0 y contempla tres secciones primarias: OWASP Testing Framework, Web Application Security Testing y Reportería. La primera de estas secciones está orientada al desarrollo seguro de aplicaciones web, la segunda a pruebas de seguridad de aplicaciones web, como tal, y la tercera constituye todo un capítulo dedicado a cómo documentos los resultados obtenidos. La sección correspondiente a las Pruebas de Seguridad de Aplicaciones contempla un listado de las 10 vulnerabilidades que están siendo más explotadas por los atacantes (Top 10 OWASP) y provee una guía a seguir para llevar a cabo la validación de estas.

  Busca motivar y fomentar a los desarrolladores a elaborar su trabajo brindando confiabilidad en las aplicaciones creadas para el desempeño de los negocios [12].

2.2.9 Etapas del hacking

La ejecución de un hacking ético conlleva una serie de etapas; estas difieren en algunos pasos dependiendo de la metodología a utilizar. Sin embargo, se puede disponer de las etapas que fueron tomadas del curso: "¿Cómo realizar un Pentest?" [13] de DragonJAR Soluciones y Seguridad, que incluyen:

- **Recolección de Información:** Es la fase de preparación en la cual se busca recolectar toda la información esencial del objetivo; esta fase normalmente toma más tiempo pues de esta dependerá la estrategia a seguir para los siguientes pasos [14].

- **Enumeración:** Es la recolección y compilación de toda la información obtenida en el paso anterior: detección de equipos activos, rangos IP, Sistemas operativos, etc.
- **Análisis:** Modelado de la infraestructura, servicios, aplicaciones; identificación de fallos conocidos basados en los pasos anteriores.
- **Explotación:** Búsqueda de exploits y herramientas para atacar las vulnerabilidades y fallos encontrados, en esta etapa se busca demostrar la criticidad de materializarse alguna amenaza.
- **Documentación:** Generación y envío de informe técnico, informe ejecutivo.

Cabe mencionar que para la ejecución de cada una de las fases mencionadas se pueden utilizar herramientas de software libre así como software comercial.

2.3 Propuesta de solución

La ejecución de un hacking ético en la infraestructura de Plasticaucho Industrial S.A. implica simular ataques informáticos de un ciberdelincuente sin afectar la disponibilidad de servicios ni tampoco comprometer información confidencial de la empresa, con el fin de obtener una visión del nivel de seguridad informática que tiene la organización.

CAPÍTULO III

METODOLOGÍA

3.1 Modalidad de la investigación

En base a la cualidad de este proyecto se aplicó una investigación aplicada (I); la misma permitió conocer el estado actual de la infraestructura tecnológica previa ejecución del ejercicio de hacking ético. A su vez también facultó al investigador adquirir competencias en seguridad informática.

Investigación de campo

Se hizo uso de la modalidad de investigación de campo para cotejar el entorno de gestión de la seguridad en la infraestructura informática de Plasticaucho Industrial S.A. consiguiendo la información necesaria para el análisis de la problemática.

Investigación documental - bibliográfica

Se trabajó en el uso de la modalidad de investigación bibliográfica buscando apalancar el conocimiento del investigador para el desarrollo del proyecto a través de: tesis, artículos, libros y documentación en línea que brinden información relevante.

3.2 Recolección de información

Se usaron métodos correspondientes a la fase de reconocimiento de un hacking ético para el levantamiento de información técnica. Esta información permitió adquirir un escenario claro de los recursos informáticos que dispone la empresa.

3.3 Procesamiento y análisis de datos

Se siguieron los pasos mencionados en la etapa de análisis de un hacking ético. Se recopiló toda la información obtenida en las fases anteriores depurando y resumiendo los datos alcanzados; teniendo como finalidad modelar los servicios de la infraestructura tecnológica.

3.4 Desarrollo del proyecto

Para el desarrollo del proyecto se tomó como base las etapas para la ejecución del ejercicio de hacking ético mencionadas en el capítulo II - recolección de información, enumeración, análisis, explotación y documentación - , a lo que se agregó la fase de planificación, tal y como se explican a continuación:

- **Planificación:** esta etapa incluyó la identificación de las herramientas y/o técnicas a utilizar para obtener los objetivos propuestos. Se persigue dejar claro el alcance del trabajo en el contexto en que se lleva a cabo.
- **Recolección de Información:** también denominada fase de reconocimiento o preparación, permitió recoger la información pública del objetivo sin interactuar directamente con él, llámese también reconocimiento pasivo.
- **Enumeración:** consistió en realizar un mapeo de la red interna con el fin de conocer los equipos activos, sistemas operativos y servicios que se están ejecutando.
- **Análisis:** modelado de la infraestructura en base a la información obtenida anteriormente; posteriormente se buscó identificar vulnerabilidades conocidas y plantear una ruta de los posibles caminos a seguir en la siguiente fase.

- **Explotación:** búsqueda de exploits y herramientas para atacar y explotar las vulnerabilidades encontradas.
- **Documentación:** generación de informe de explotación y remediación.

CAPÍTULO IV

DESARROLLO DE LA PROPUESTA

4.1 Planificación

Se siguieron las etapas mencionadas en el capítulo III, página 27 referenciando las bases del curso "¿Cómo realizar un pentest?". Es primordial destacar que el objetivo incuestionable del hacking ético será siempre verificar el estado de la seguridad de los sistemas informáticos y buscar ser proactivos para mitigar los riesgos que un atacante pueda aprovechar [14].

Gráfico 1 - Enfoque basado en DragonJar [13]

La secuencia de pasos que se muestan en el diagrama, detallan de forma clara el conjunto de etapas tomadas a consideración, teniendo en cuenta que el proyecto no busca obtener una certificación de las metodologías existentes, sino que pretende identificar un conjunto de vulnerabilidades y debilidades a las cuales poder plantear posibles soluciones en un ejercicio de hacking ético.

Cabe destacar que para el desarrollo del presente proyecto se propuso como plataformas base los sistemas operativos: Kali Linux y Windows 10. El criterio fue dado por la factibilidad para poder ejecutar herramientas de pentest en los mismos.

Por cuestiones referentes al acuerdo a la confidencialidad (Véase Anexo B) el presente proyecto de Hacking Ético no expone información sensible de la empresa, se oculta o modifican parte de los resultados que incluyan direcciones IP, nombres de equipos, usuarios o cualquier información que exponga datos de Plasticaucho Industrial S.A.. Por tanto se usa el rango de direcciones IP 10.192.168.1 - 10.192.168.10 para referenciar a los equipos

Windows Servers y GNU/Linux, para los equipos Windows XP se usa el rango 10.192.168.50 – 190.192.168.53, para equipos Windows 7 se usa el rango 10.192.168.60 – 10.192.168.63 y para equipos Windows 8 se usa el rango 10.192.168.70 – 10.192.168.73. Se recalca que estas direcciones no son reales.

Como parte del trabajo de planificación, a continuación se plantearon posibles herramientas a usar en cada una de las fases del proceso de hacking ético llevado a cabo:

- **Fase de Recolección de Información**

  Cuanta más información se consiga recabar del objetivo, mayor es la probabilidad de lograr una explotación exitosa. La perspectiva de esta fase contempla un reconocimiento pasivo (sin interactuar directamente con un equipo informático) y una búsqueda de toda la información de conocimiento público (OSINT) de la empresa incluyendo: sitio web, dominios, dns, sistemas operativos, mecanismos de control, correos electrónicos, etc.

  Dentro de esta etapa se propusieron varias herramientas en dependencia de la información que se quiso obtener.

  Google Hacking: el motor de búsqueda de google y sus operadores avanzados permiten realizar búsquedas más específicas [15]**.**

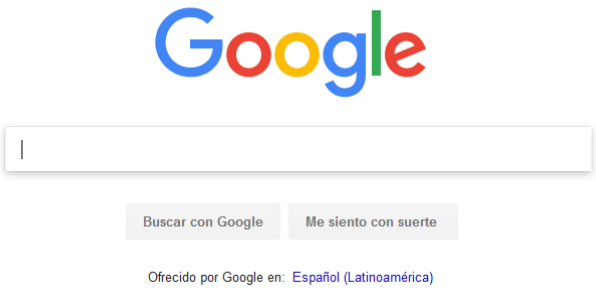


Gráfico 2- Google

TheHarvester: Esta herramienta permite realizar una búsqueda en internet de direcciones de correos electrónicos a partir de un dominio.

Gráfico 3 - TheHarvester

Whois: es un servicio de consulta para obtener información pública del propietario de un nombre de dominio o dirección IP.

Gráfico 4 - Whois

Nslookup: esta es una utilidad propia del sistema Windows o GNU/Linux que permite hacer un descubrimiento de las entradas DNS a partir de nombre de dominio.

Gráfico 5 - Nslookup

Fierce: es una utilidad de reconocimiento de DNS [16].

```
root@tesis:~# fierce --h
fierce.pl (C) Copywrite 2006,2007 - By RSnake at http://ha.ckers.org/fierce/

        Usage: perl fierce.pl [-dns example.com] [OPTIONS]

Overview:
        Fierce is a semi-lightweight scanner that helps locate non-contiguous
        IP space and hostnames against specified domains.  It's really meant
        as a pre-cursor to nmap, unicornscan, nessus, nikto, etc, since all
        of those require that you already know what IP space you are looking
        for.  This does not perform exploitation and does not scan the whole
        internet indiscriminately.  It is meant specifically to locate likely
        targets both inside and outside a corporate network.  Because it uses
        DNS primarily you will often find mis-configured networks that leak
        internal address space. That's especially useful in targeted malware.
```

Gráfico 6 - Fierce

FOCA: es una herramienta que permite analizar los metadatos de documentos publicados en un determinado sitio web.

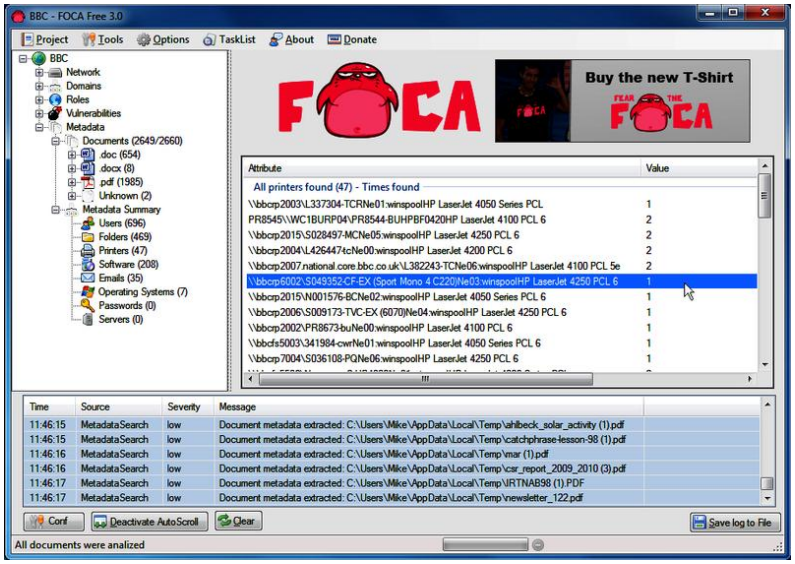


Gráfico 7 - ejemplo de FOCA pentest

- **Fase de Enumeración**

  Esta etapa tiene como fin mapear la red interna de la empresa ejecutando un reconocimiento activo (interactuando con los equipos). Se busca identificar y conocer direcciones y rangos IPs, equipos activos, sistemas operativos, servicios que se ejecutan, firewalls, etc.

  Nmap: existen varias herramientas de reconocimiento de red; sin embargo, siguiendo la propuesta de Engebretson [17], se propuso Nmap. A parte de ser un escáner de red permite identificar puertos que se

encuentran ejecutándose en cada host y detallar las versiones y servicios tras estos.

```
root@projectx:~# nmap --help
Nmap 7.60 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Gráfico 8 - Consola nmap

- **Fase de Análisis**

  En esta etapa se recolecta toda la información levantada en las fases de recolección y enumeración para posteriormente llevar a cabo un análisis de vulnerabilidades. Esto permite identificar vulnerabilidades conocidas y descartar falsos positivos que pudiesen llegar a presentarse en la infraestructura. A continuación se proponen algunas herramientas a usar en esta fase:

  Nessus: es un escáner de vulnerabilidades administrado bajo una consola web y dispone de una gran base de datos de vulnerabilidades conocidas.

Gráfico 9 - Logo Nessus

OpenVAS: es otra herramienta para ejecutar análisis de vulnerabilidades similar a Nessus en cuanto al enfoque y administración a través de una consola web.

Gráfico 10 - Logo OpenVAS

- **Fase de Explotación**

  Tras la fase de análisis, se procede a realizar pruebas de penetración lo cual involucra un proceso en donde se realizan distintos tipos de ataques que buscan explotar las vulnerabilidades identificadas. También, como parte de la planificación del hacking ético llevado a cabo, se acordó con el cliente ejecutar las pruebas en un ambiente seguro y controlado para evitar la indisponibilidad de los servicios informáticos contemplando los siguientes puntos:

  - Las pruebas se ejecutaran en horarios fuera de oficina.
  - Ninguna prueba debe puede la indisponibilidad de los servicios tecnológicos, salvo el consentimiento del administrador de redes e infraestructura.
  - Todas las pruebas a realizarse tendrán la aprobación del administrador de redes e infraestructura.

  La principal herramienta que se propone para esta fase es:

  Metasploit: un framework de explotación perteneciente a la Empresa Rapid7. Dispone de una versión community que viene preinstalada en Kali Linux o se puede descargar desde el sitio oficial para otras plataformas. Está compuesto de diferentes módulos como: payloads, auxiliares, explotación, post explotación, etc [18]. La colaboración de la comunidad en seguridad informática ha permitido que metasploit vaya creciendo y mejorando con el desarrollo de nuevos scripts y módulos para aprovechar vulnerabilidades y comprometer el equipo llegando incluso a obtener credenciales de usuarios.

Gráfico 11 - Logo Metasploit

- **Documentación**

  Para la etapa final se debe elaborar un informe donde se detalle el conjunto de vulnerabilidades encontradas y su criticidad además de información sobre los equipos analizados, recalcando los planes de remediación que se deberán aplicar para minimizar o mitigar el riesgo. Se realizará un informe ejecutivo y un informe técnico.

4.2 Recolección de Información

Se buscó información del sitio web de la empresa y se evidenció lo siguiente:

De acuerdo al nombre de la empresa se encontraron cuatro sitios web que tienen relación; se consultó al administrador de redes e infraestructura quien manifestó que el dominio plasticaucho.com.ec corresponde al sitio web de Ecuador. Sin embargo, se manejan con el dominio plasticaucho.com para información a nivel corporativo y para el correo electrónico. Los dos sitios adicionales corresponden a las filiales de Colombia y Perú.

Las siguientes pruebas de reconocimiento se realizaron obviando los sitios correspondientes a las sucursales pues no se tuvo acceso a las mismas y el proyecto se enfoca en la matriz ubicada en Ambato, Ecuador.

Cabe destacar que en esta fase o las siguientes no se interactuó con ningún equipo de un proveedor o tercero al que no se tuviera consentimiento para realizar pruebas; por ejemplo, servicios hosteados.

- **Google Hacking**

Primero es importante navegar e investigar los sitios web. Esto brinda una idea del funcionamiento de cada página. Adicionalmente es significativo identificar la tecnología con la que está hecho el sitio web, para ello se disponen de varios servicios en línea que con tan solo el nombre del dominio pueden interpretar en que lenguaje de programación fueron realizados, si usan o no algún sistema gestor de contenidos, etc. Para el proyecto se usó la web www.w3techs.com, en el apartado *Sites* se colocó el dominio y se obtuvo la siguiente información:

Site Info - plasticaucho.com

Server-side Programming Language	
PHP	PHP is a popular scripting language for creating web pages.
Client-side Programming Language	
JavaScript	JavaScript is a lightweight, object-oriented, cross-platform scripting language, mainly used within web pages.
JavaScript Libraries	
jQuery 1.11.1 (55% of sites use a newer version)	jQuery is a JavaScript library that simplifies HTML document traversing, event handling, animating and Ajax interaction. Originally developed by John Resig.
Bootstrap	Bootstrap is an open source HTML, CSS, and JavaScript framework.
Markup Language	
HTML5	HTML5 is the fifth revision of the HTML standard.

Gráfico 12 - Tecnología sitio web plasticaucho.com

Site Info - plasticaucho.com.ec

Server-side Programming Language	
PHP	PHP is a popular scripting language for creating web pages.
Client-side Programming Language	
JavaScript	JavaScript is a lightweight, object-oriented, cross-platform scripting language, mainly used within web pages.
JavaScript Libraries	
jQuery 1.11.1 (54% of sites use a newer version)	jQuery is a JavaScript library that simplifies HTML document traversing, event handling, animating and Ajax interaction. Originally developed by John Resig.
Bootstrap	Bootstrap is an open source HTML, CSS, and JavaScript framework.
Markup Language	
HTML5	HTML5 is the fifth revision of the HTML standard.

Gráfico 13 - Tecnología del sitio web Plasticaucho.com.ec

Haciendo una breve revisión del contenido se identificó que el sitio plasticaucho.com es solo una página informativa que enlaza los otros sitios de las sucursales. Por su parte, la página web plasticaucho.com.ec muestra mayor información de catálogos de los productos que fabrica y comercializa. Adicionalmente en los gráficos 12 y 13 se evidencia que ninguno de los sitios fue elaborado a través de un sistema gestor de contenidos lo cual reduce en parte que se presenten vulnerabilidades. Esta información fue de utilidad para continuar con la disciplina de Google Hacking.

Google dispone de un algoritmo interno que permite interpretar "*keywords*" o "*dorks*" para optimizar las búsquedas e incluso potenciarlas para analizar un objetivo a detalle. Tras conocer los sitios web de la empresa, se buscó información especificando el nombre de dominio a través del dork site:plasticaucho.com.ec; esto indicó que todos los dorks siguientes realicen las búsquedas únicamente en el sitio.

Búsqueda de directorios sensibles

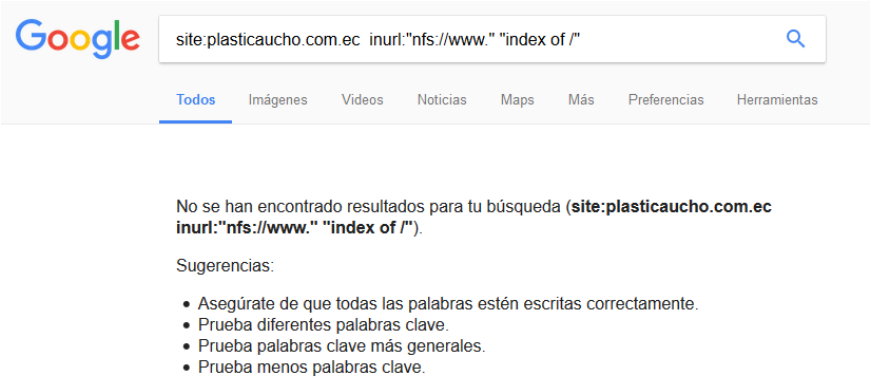


Gráfico 14 - Búsqueda para listar directorios

Este dork permite identificar archivos o directorios compartidos si se tuviera un sistema de archivos de red (NFS) a través del *path* por defecto [19]. Al aplicarlo al dominio plasticaucho.com.ec no se encontró información.

Búsqueda de páginas que contengan portal de login

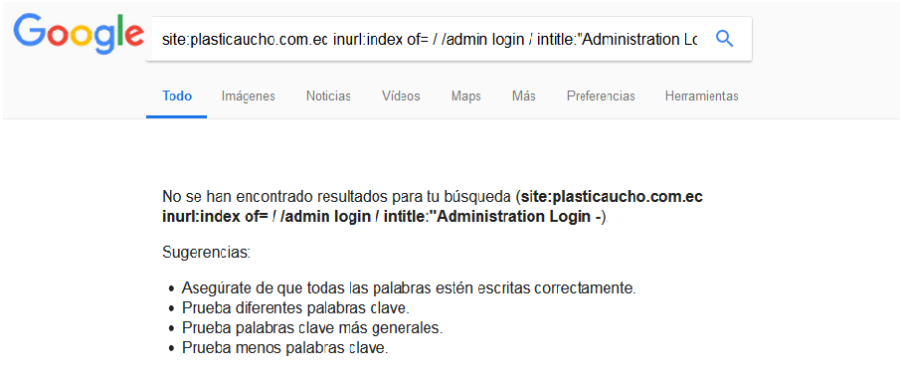


Gráfico 15 - Búsqueda de páginas de administración

Este dork busca páginas de administración dentro del sitio; en las direcciones (inurl) usando palabras claves o a través del título (intittle) de

las páginas [20]. Al aplicarlo al dominio plasticaucho.com.ec no se encontró información.

Búsqueda de redirección arbitraria

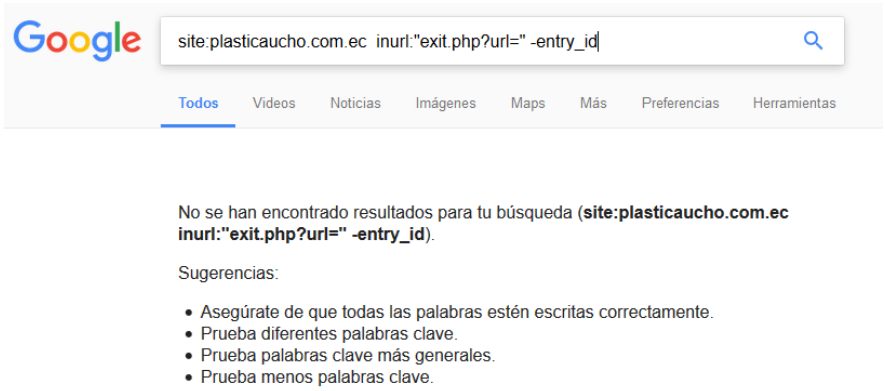


Gráfico 16 - Búsqueda de páginas vulnerables a la redirección arbitraria

Este dork busca páginas dentro del sitio que permitan la ejecución de redirección arbitraria buscando en las direcciones (inurl) [21]. Al aplicarlo al dominio plasticaucho.com.ec no se encontró información.

Búsqueda de avisos y vulnerabilidades

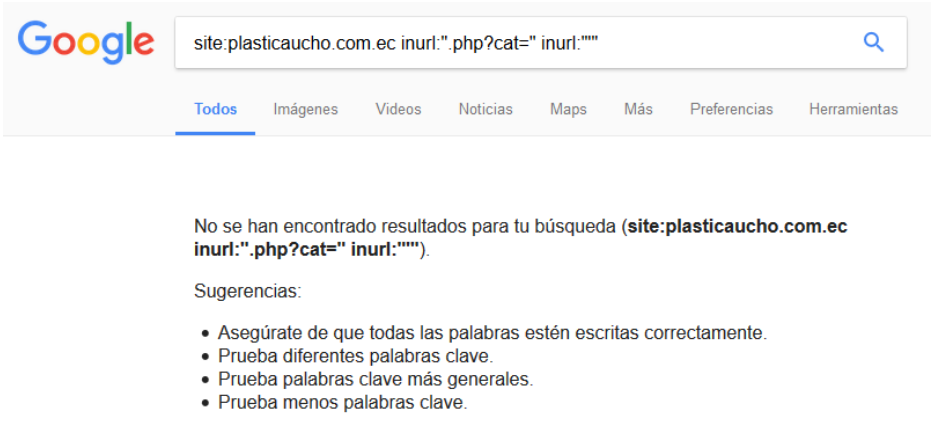


Gráfico 17 – Búsqueda de vulnerabilidades de inyección de SQL

Este dork permite analizar si el sitio es vulnerable a un ataque de inyección SQL buscando en las direcciones (inurl) [22]. Al aplicarlo al dominio plasticaucho.com.ec no se encontró información.

A continuación se muestra una tabla resumen de los dorks aplicados:

Dork ejecutado	Sintaxis	Resultado
Búsqueda de directorios sensibles	inurl:"nfs://www." "index of /"	Al aplicarlo al dominio plasticaucho.com .ec no se encontró información.
Búsqueda de páginas que contengan portal de login	inurl:index of= %2F /admin login %2F intitle:"Administration Login -	
Búsqueda de redirección arbitraria	inurl:"exit.php?url=" -entry_id	
Búsqueda de avisos y vulnerabilidades	inurl:".php?cat=" inurl:"'"	

Tabla 1 - Resumen google hacking

Las consultas ejecutadas fueron tomadas del sitio www.exploit-db.com que dispone de una base de datos con dorks de Google [23].

- **TheHarvester**

  Se procedió a hacer un análisis del dominio principal la empresa que es usado para la gestión de correo electrónico (plasticaucho.com). Para ello se ejecutó una búsqueda con el siguiente comando:

```
root@tesis:~# theharvester -d plasticaucho.com -l 10 -b all
```

Gráfico 18 - Búsqueda con TheHarvester

Se llama a la herramienta con el parámetro theharvester a continuación se especificó el dominio con el parámetro –d, el resultado de la búsqueda a 10 registros con –l y finalmente que busque en todas las fuentes de datos con el parámetro –b. Los resultados fueron los siguientes:

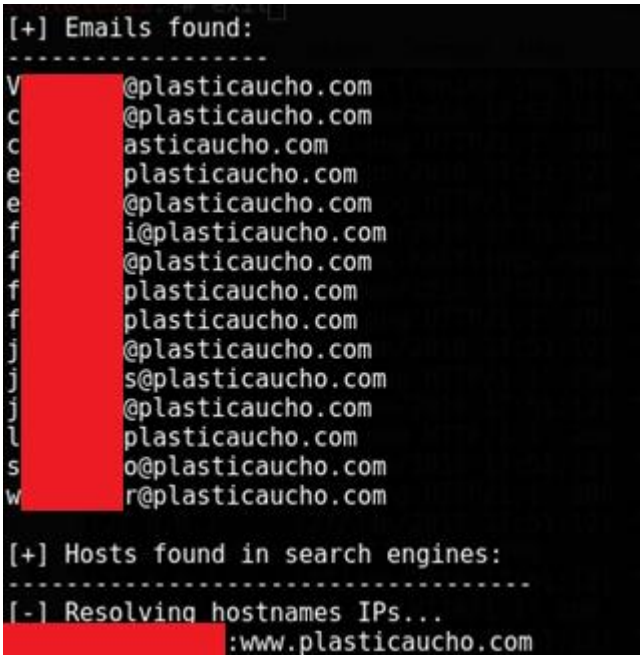


Gráfico 19 - Resultado TheHarvester correos

Se encontraron direcciones de correo que podrían ser de utilidad en las siguientes etapas. Adicionalmente, se obtuvo la IP del servidor en donde se encuentra hosteado el sitio web e incluso dominios adicionales.

Gráfico 20 - Búsqueda TheHarvester dominios

Al obtener como resultado varios dominios que no tienen relación con la empresa se determinó que el sitio web se encuentra alojado en un servidor compartido de algún proveedor de hosting.

- **Whois**

  Tras ejecutar el comando whois en el terminal usando el dominio plasticaucho.com.ec se obtuvo el siguiente resultado:

Gráfico 21 – Resultado parcial Whois plasticaucho.com.ec

Se realizó el mismo proceso con el dominio plasticaucho.com obteniendo el siguiente resultado:

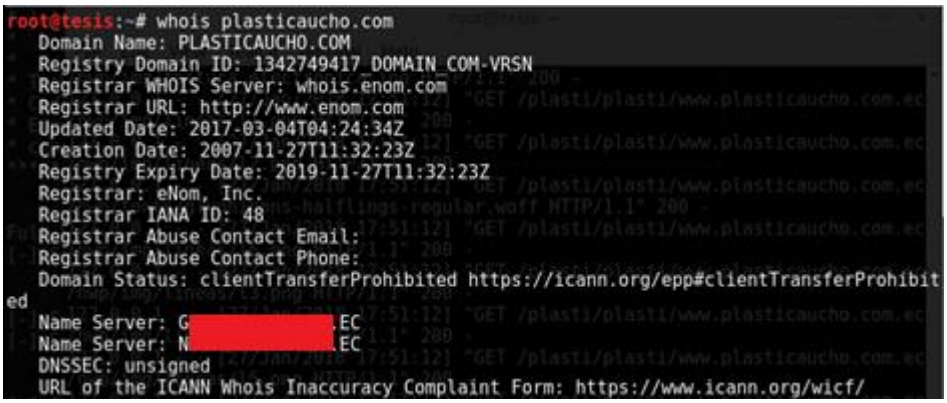


Gráfico 22 –Resultado parcial Whois plasticaucho.com

Se llegó a conocer los servidores DNS e información del registrante de los dominios. Cabe mencionar que también es posible realizar esta consulta a través de sitios de internet, por ejemplo whois.net arrojó el siguiente resultado:

Gráfico 23 - Resultado Whois.net

- **Nslookup**

  Una vez obtenidos los servidores DNS se ejecutó una búsqueda de registros de cualquier tipo (any) principalmente del dominio plasticaucho.com.

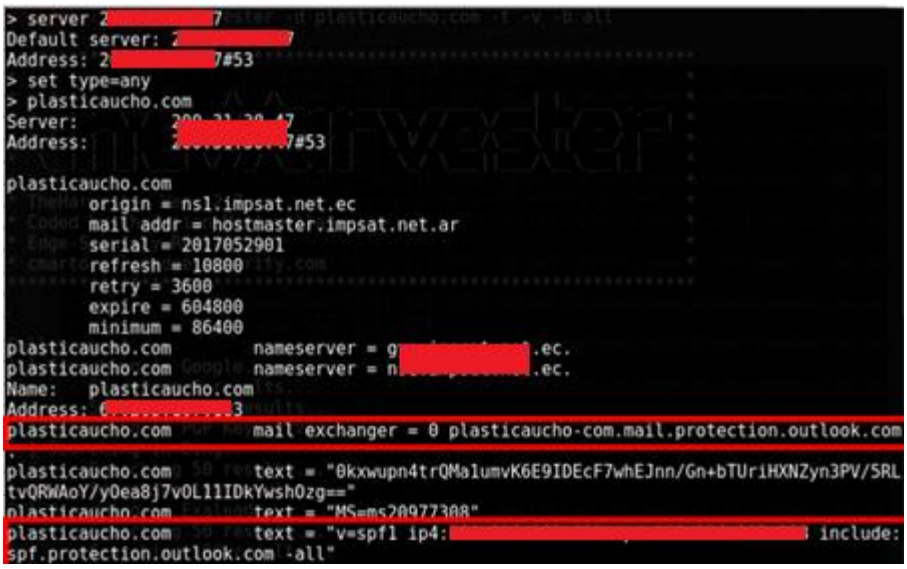


Gráfico 24 - Resultado nslookup

Se identificó que sus servidores de correo corresponden al servicio de Office 365 y además disponen de una configuración SPF que permite el envío a través del mismo servicio.

- **Fierce**

  Se obtuvieron los siguientes resultados al ejecutar la utilidad:

Gráfico 25 - Resultados Fierce

- **FOCA**

  Al usar la herramienta FOCA se encontraron 9 archivos publicados en el sitio web de plasticaucho.com.ec. Sin embargo al ejecutar un análisis de los metadatos no se encontró información relevante como se ve en el gráfico

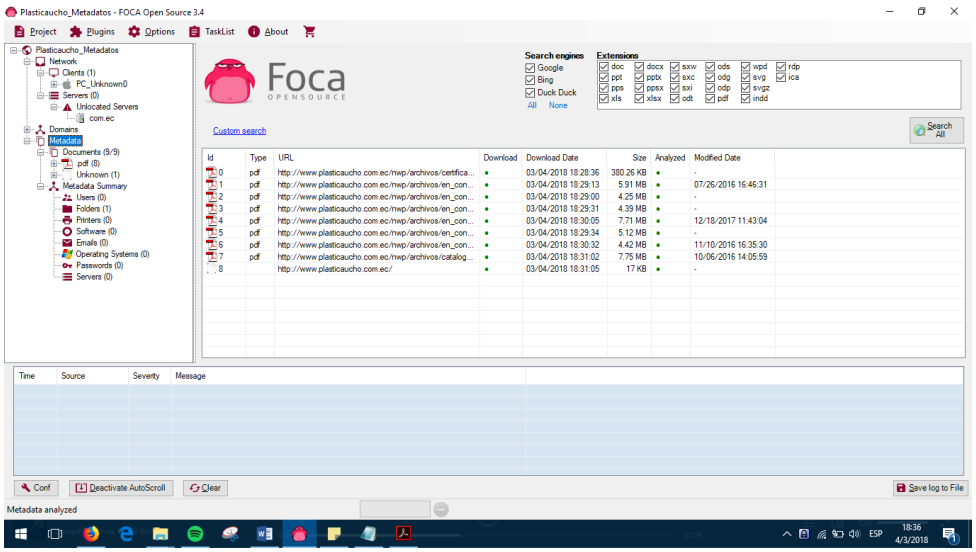


Gráfico 26 – Análisis de metadatos con FOCA

4.3 Enumeración

- **Mapeo de la red**

  Siendo un pentest de caja gris, en esta etapa se tuvo acceso a un punto de red en la infraestructura interna. Adicionalmente, el administrador de redes e infraestructura proporcionó un esquema de la red a nivel corporativo, el que se muestra en la figura 27.

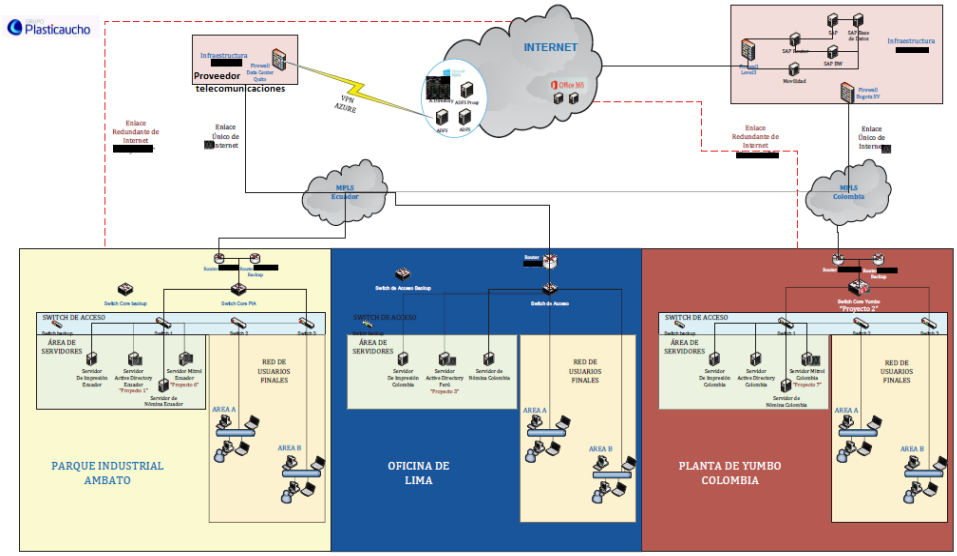


Gráfico 27 - Red corporativa

En el gráfico se observa que Plasticaucho Industrial se enlaza con sus filiales a través de una red MPLS. Dicha red es provista por un proveedor internacional que también suministra el servicio de hosting dedicado para los servidores del ERP. Recalcando lo mencionado en la sección de recolección de información, este proyecto cubre el estudio de lo que sucede en la matriz de la empresa, que está ubicada en Ambato.

Para empezar el análisis de la red interna se ejecutó un ping sweep en horarios fuera de oficina para identificar los hosts activos. Se usó nmap como herramienta y se ejecutó el siguiente comando:

```
nmap -sn -n -T4 -oX listado_hosts.xml --webxml  (rango ip)
```

Gráfico 28 - Descubrimiento de la red interna

Los parámetros fueron "-sn" para que no se realice un escaneo de puertos, "-n" para que no realice una resolución DNS y "-T4" para ejecute un escaneo agresivo. Las opciones siguientes "-oX" y "--webxml" nos permitieron exportar el resultado a un archivo XML que disponga de un estilo legible. El resultado arrojó 150 hosts activos.

```
Nmap done at Sat Feb 3 10:38:31 2018;     # IP addresses (150 hosts up) scanned in 32.68 seconds
```

Gráfico 29 - Número de hosts activos en la red

Una vez obtenido el listado los hosts activos es importante realizar un port scanning. Este escaneo nmap se encarga de enviar peticiones a los 1000 puertos más comunes para identificar detalles de los servicio que se están ejecutando en los mismos [17] y detalles del sistema operativo. El resultado será examinado en la siguiente fase.

Dada la limitante de no poder realizar pruebas en horarios de oficina, se solicita un listado de los sistemas operativos clientes que tiene la empresa con el fin de tomar como muestra tres equipos de cada plataforma y llevar a cabo los análisis siguientes en terminales clientes.

4.4 Análisis

Tras la fase de recolección de la información (reconocimiento pasivo) se determinaron los siguientes puntos:

- El sitio web de la empresa se encuentra alojado con un proveedor de hosting externo (ver gráfico 20).
- La entrada MX indica que disponen del servicio de correo electrónico alojado en Office 365 (ver gráfico 24).

Por lo tanto, en la red interna no debe encontrarse un servidor web ni un servidor de correo electrónico. Es importante ratificar el objetivo general de la presente investigación en la que el estudio se centró en un análisis de

infraestructura y no se buscó detectar vulnerabilidades web u otras a nivel de aplicación.

Tras la fase de enumeración se obtuvo el listado de hosts activos, tanto servidores resultantes del escaneo con nmap y hosts clientes proporcionados por el departamento de TI.

Análisis de Equipos Windows Servers y GNU/Linux

En primera instancia se analizó los host resultantes del escaneo con nmap, en la tabla 2 y gráfico 30 se ilustra la proporción de hosts por sistema operativo.

Resumen de equipos resultantes de escaneo nmap

Sistema Operativo	Porcentaje
-	13%
Aastra	6%
Cisco	2%
Crestron AV2 or CP2E automation system	1%
Crestron MC2E	1%
H3C Comware/3com	1%
HP iLO	1%
HP iLO/HP Officejet	1%
HP Onboard Administrator	1%
Inova Ontime Clock	3%
GNU/Linux	25%
VxWorks	1%
Windows	44%
Xerox Phaser	1%

Tabla 2 - Resumen de SO escaneo nmap

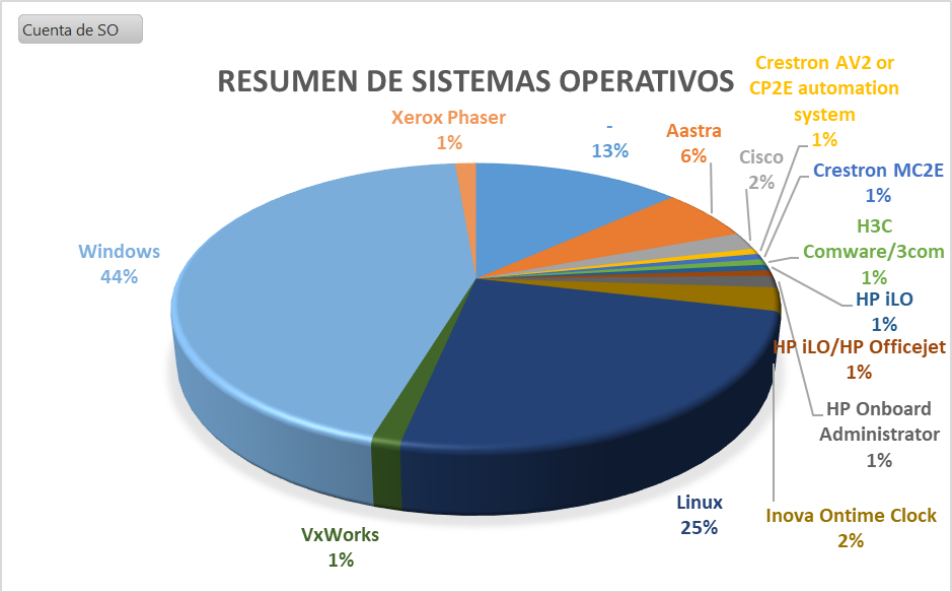


Gráfico 30 - Resumen de SO escaneo nmap

En el resultado del escaneo de la red (tabla 2, gráfico 30) se encontraron en mayor cantidad equipos con sistemas operativos Windows y GNU/Linux. Debido a la gran cantidad de equipos activos en la red se enfocaron los análisis siguientes en examinar los cinco primeros equipos con mayor cantidad de puertos abiertos operando con cada uno de estos sistemas operativos (Windows Server y GNU/Linux). Se tomó este criterio fundamentando en que un puerto abierto ejecuta un servicio y este a su vez puede ser vulnerable permitiendo el acceso al equipo y comprometiendo la seguridad de la infraestructura.

A continuación se resume el reporte de hosts activos bajo las plataformas Windows Server y GNU/Linux con el número de puertos abiertos para cada equipo:

Equipos Windows Server	
Equipos	**N° Puertos Abiertos**
10.192.168.1	23
10.192.168.2	23
10.192.168.3	21
10.192.168.4	20
10.192.168.5	23

Tabla 3 - Equipos Windows Server

Equipos GNU/Linux	
Equipos	**N° Puertos Abiertos**
10.192.168.6	11
10.192.168.7	10
10.192.168.8	8
10.192.168.9	8
10.192.168.10	7

Tabla 4 - Equipos GNU/Linux

Análisis de Vulnerabilidades

Para el análisis de vulnerabilidades se usó las dos herramientas mencionadas en la planificación: OpenVAS (ver gráfico 32) y Nessus (ver gráfico 35). En cada herramienta se analizaron los 5 hosts de Windows Server y GNU/Linux identificados previamente.

Análisis de vulnerabilidades con OpenVAS

Gráfico 31 - Dashboard OpenVAS

Como primer paso se crearon los grupos de targets a ser analizados estructurando los equipos por plataforma, tal y como se ilustra en el gráfico 33.

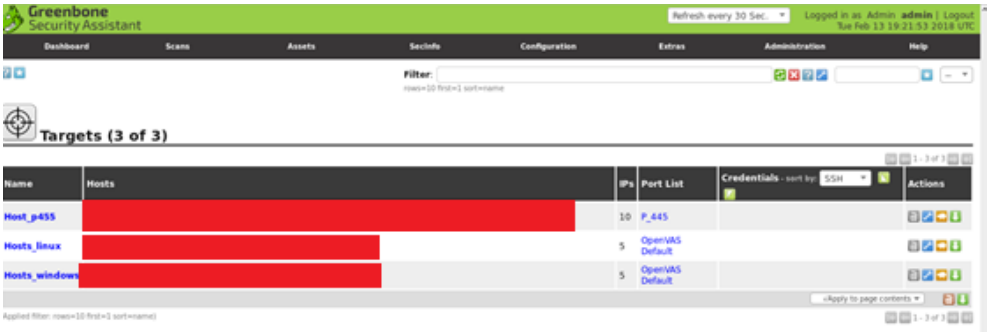


Gráfico 32 - Targets OpenVAS

De manera seguida, se crearon y ejecutaron tareas de escaneo hacia a los targets establecidos, tal y como se muestra en la figura 34.

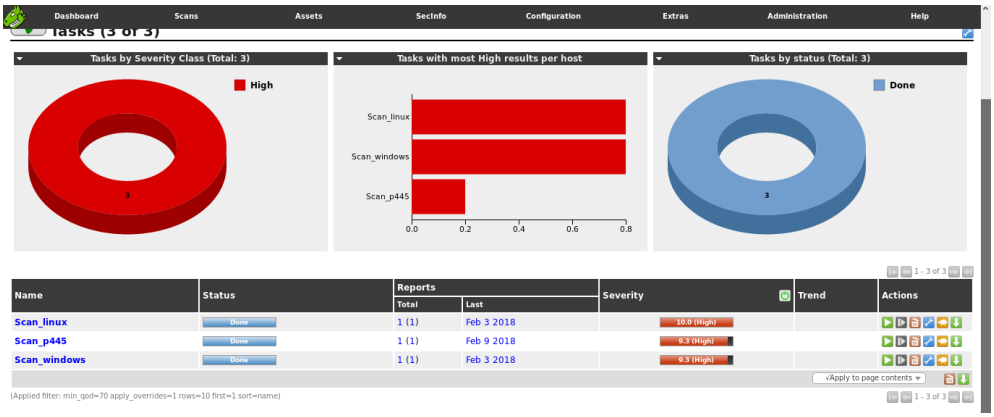


Gráfico 33 - Tasks OpenVAS

Una vez finalizados los procesos de escaneos, los resultados arrojados fueron agrupados en las tablas resumen 5 y 6:

Resumen de vulnerabilidades en equipos Windows Server

Host	High	Medium	Low	Log	False Positive
10.192.168.1	3	40	1	0	0
10.192.168.2	1	4	1	0	0
10.192.168.3	0	10	1	0	0
10.192.168.4	0	16	1	0	0
10.192.168.5	0	8	1	0	0
Total:	**4**	**78**	**5**	**0**	**0**

Tabla 5 - Escaneo OpenVAS hosts Windows Server

Los resultados indican que existen dos equipos con vulnerabilidades de criticidad alta; en el resto de equipos se encontraron vulnerabilidades de criticidad media y baja.

Resumen de vulnerabilidades en equipos GNU/Linux

Host	High	Medium	Low	Log	False Positive
10.192.168.6	4	7	1	0	0
10.192.168.7	0	1	1	0	0
10.192.168.8	0	2	1	0	0
10.192.168.9	0	1	1	0	0
10.192.168.10	0	1	1	0	0
Total:	**4**	**12**	**5**	**0**	**0**

Tabla 6 - Escaneo OpenVAS hosts GNU/Linux

Los resultados indican que se encontró un equipo con vulnerabilidades de criticidad alta. El resto de equipos GNU/Linux tienen vulnerabilidades de criticidad media y baja.

Análisis de vulnerabilidades con NESSUS

Para el proyecto se utilizó la versión home de nessus, que tiene como principales limitantes: el no permitir un análisis de más de 16 ips por escaner, no tiene soporte, no permite realizar comprobaciones de cumplimeintos y no permite usar el dispositivo virtual de Nessus. Sin embargo los módulos de análisis son válidos para llevar a cabo el trabajo propuesto sin incurrir en costos por pago de licencia de software. En esta herramienta, a diferencia de OpenVAS, se crearon directamente las tareas de escaneo incluyendo los hosts requeridos.

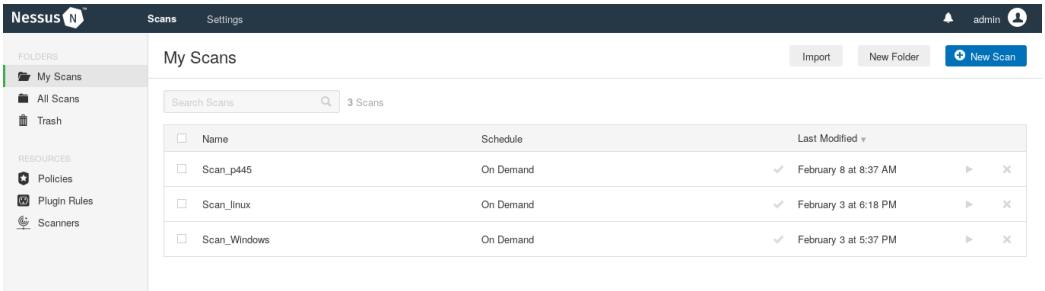


Gráfico 34 - Dashboard Nessus

Nessus proporciona varios tipos de escaneo. Para el caso en cuestión se seleccionó un escaneo de tipo avanzado, tal y como se ilustra en el gráfico 36.

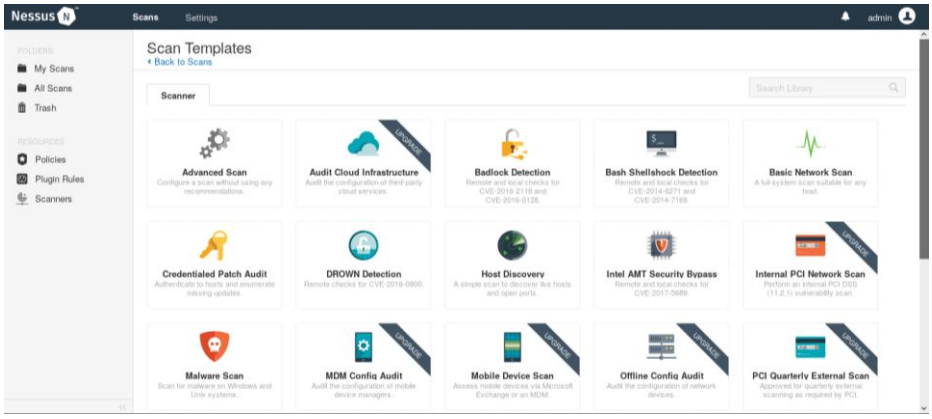


Gráfico 35 - Tipos de escaneos en Nessus

Finalizados los escaneos, se crearon las tablas resumen para analizar la cantidad de vulnerabilidades en dependencia de su criticidad (ver tablas 7 y 8).

Resumen de vulnerabilidades en equipos Windows Server

Host	Critical	High	Medium	Low	Info
10.192.168.1	2	3	15	2	46
10.192.168.2	1	0	12	3	42
10.192.168.3	8	7	13	3	43
10.192.168.4	1	0	15	3	51
10.192.168.5	0	0	8	2	38
Total:	**12**	**10**	**63**	**13**	**220**

Tabla 7 - Escaneo Nessus hosts Windows Server

Nessus arrojó una mayor cantidad de vulnerabilidades de criticidad alta identificadas en uno de los equipos Windows Server. El resto de equipos al igual que con OpenVAS siguen manteniendo vulnerabilidades de criticidad media y baja.

Resumen de vulnerabilidades equipos GNU/Linux

Host	Critical	High	Medium	Low	Info
10.192.168.6	0	0	8	1	26
10.192.168.7	0	0	3	0	40

10.192.168.8	0	0	4	0	39
10.192.168.9	0	0	3	0	22
10.192.168.10	0	0	3	0	22
Total:	**0**	**0**	**21**	**1**	**149**

Tabla 8 - Escaneo Nessus hosts GNU/Linux

El escaneo de hosts GNU/Linux indicó que ningún equipo dispone de vulnerabilidades de criticidad alta ni media, solo de nivel bajo.

Tras realizar una comparación del número de vulnerabilidades arrojadas por cada herramienta se hizo énfasis en explotar las debilidades con criticidad alta de los equipos Windows Server y GNU/Linux y con mayor cantidad de resultados. A continuación se expone un resumen de los mismos.

Host Windows Server 10.192.168.1

Al desglosar los reportes de OpenVAS y Nessus correspondientes al equipo 10.192.168.1, se identifica que una de las principales vulnerabilidades afecta al protocolo SMB puerto 445, este protocolo permite gestionar los recursos compartidos en sistemas Windows, esta vulnerabilidad tiene un puntaje de 9.3 siendo el más alto en OpenVAS lo cual indica que hay una alta probabilidad de explotar esta vulnerabilidad. Adicionalmente se encuentran vulnerabilidades que afectan a los servicios de apache Tomcat y apache server con puntajes de 7.8 y 7.5 correspondientemente (ver gráfico 37).

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

High (CVSS: 7.8)
NVT: Apache Tomcat 'MultipartStream' Class Denial of Service Vulnerability (Windows)

Product detection result
cpe:/a:apache:tomcat:7.0.57
Detected by Apache Tomcat Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800371)

High (CVSS: 7.5)
NVT: Apache HTTP Server Multiple Vulnerabilities June17 (Windows)

Product detection result
cpe:/a:apache:http_server:2.4.12
Detected by Apache Web Server Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900498)

Gráfico 36 - Vulnerabilidades críticas host 10.192.168.1 OpenVAS

En el resultado de Nessus también consta la vulnerabilidad del protocolo SMB por lo que optará por explotar esta debilidad en la siguiente fase.

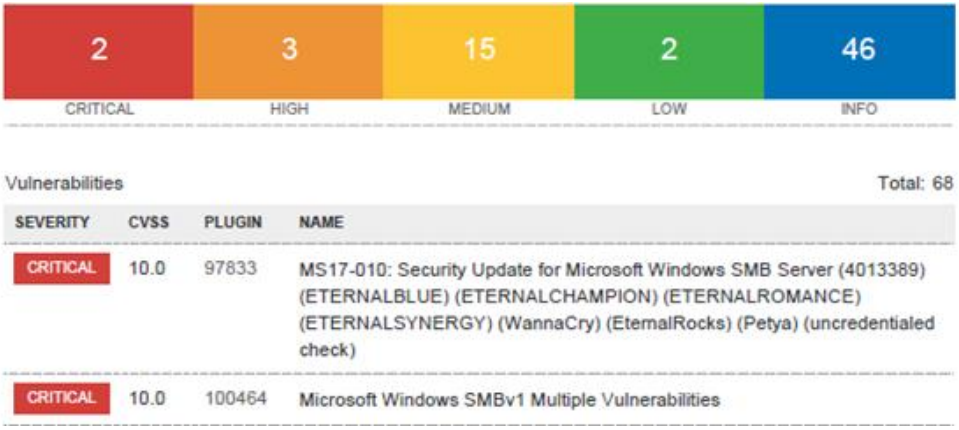


Gráfico 37 - Vulnerabilidades críticas host 10.192.168.1 Nessus

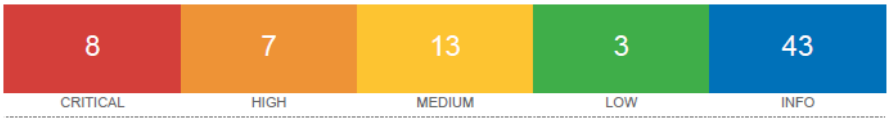
Host Windows Server 10.192.168.3

El resultado de OpenVAS para este equipo solo arrojó vulnerabilidades de criticidad media; sin embargo Nessus arrojó varias vulnerabilidades críticas. La mayoría tiene relación con la administración del sistema HP Managment con un puntaje de 10. No obstante, el reporte denota una vulnerabilidad propia del sistema operativo Windows denominada como MS-15034 la cual puede permitirnos la ejecución de código remoto. A pesar de tener el mismo

puntaje de 10 con las debilidades identificadas en la administración del sistema HP se optará por tratar de explotar esta vulnerabilidad.

Medium (CVSS: 6.8) NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
Summary OpenSSL is prone to security-bypass vulnerability.
Medium (CVSS: 5.0) NVT: DCE/RPC and MSRPC Services Enumeration Reporting
Summary Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.
Medium (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites
Summary This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Gráfico 38 - Vulnerabilidades medias host 10.192.168.3OpenVAS



Vulnerabilities — Total: 74

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53532	HP System Management Homepage < 6.3 Multiple Vulnerabilities
CRITICAL	10.0	58811	HP System Management Homepage < 7.0 Multiple Vulnerabilities
CRITICAL	10.0	82828	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)
CRITICAL	10.0	85181	HP System Management Homepage < 7.2.5 / 7.4.1 Multiple Vulnerabilities (POODLE)
CRITICAL	10.0	90150	HP System Management Homepage < 7.5.4 Multiple Vulnerabilities (Logjam)
CRITICAL	10.0	91222	HP System Management Homepage Multiple Vulnerabilities (HPSBMU03593)
CRITICAL	10.0	94654	HP System Management Homepage < 7.6 Multiple Vulnerabilities (HPSBMU03653) (httpoxy)
CRITICAL	10.0	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities

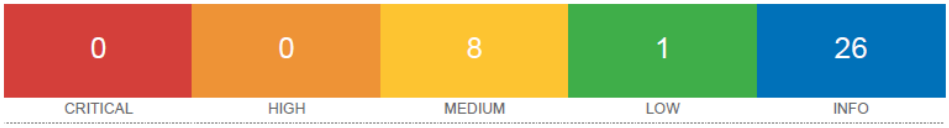
Gráfico 39 -Vulnerabilidades críticas host 10.192.168.3 Nessus

Host GNU/Linux 10.192.168.6

En este host, las vulnerabilidades críticas fueron arrojadas por OpenVAS. Se apreció que una de ellas corresponde al acceso vía telnet con credenciales por defecto. El análisis con Nessus solo arrojó como resultado vulnerabilidades de criticidad media.

High (CVSS: 10.0) NVT: Polycom HDX Default Telnet Credentials
Summary The Polycom device has default telnet credentials or passwordless login.
High (CVSS: 10.0) NVT: Polycom HDX Default Telnet Credentials
Summary The Polycom device has default telnet credentials or passwordless login.
High (CVSS: 7.5) NVT: Lighttpd Multiple vulnerabilities
Summary This host is running Lighttpd and is prone to multiple vulnerabilities
High (CVSS: 7.5) NVT: Lighttpd Multiple vulnerabilities
Summary This host is running Lighttpd and is prone to multiple vulnerabilities

Gráfico 40 - Vulnerabilidades críticas host 10.192.168.6 OpenVAS



Vulnerabilities Total: 35

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm

Gráfico 41 - Vulnerabilidades medias host 10.192.168.6

Análisis Equipos Windows Clientes

En la tabla 9 y gráfico 31 se ilustra la proporción de hosts por sistema operativo cliente de la información proporcionada por la empresa quienes indican que manejan equipos clientes solo con sistema operativo Windows.

Resumen de equipos clientes proporcionados por la empresa

Sistema Operativo	Porcentaje
Windows XP Profesional	1%
Windows 7 Profesional	60%
Windows 8 Pro	1%
Windows 8.1 Pro	30%
Windows 8.1 Enterprise	6%
Windows 10 Pro	2%

Tabla 9 - Resumen SO clientes proporcionados por la empresa

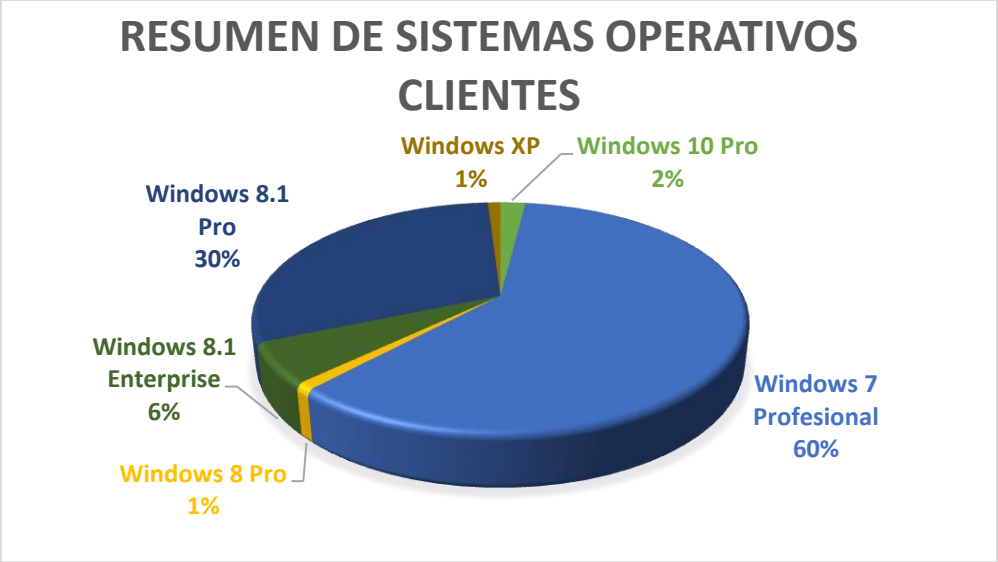


Gráfico 42 - Gráfico SO clientes proporcionados por la empresa

Al igual que con los equipos Windows Servers y GNU/Linux, se hizo uso de las herramientas para análisis de vulnerabilidades con OpenVAS y Nessus.

Para ejecutar el análisis de vulnerabilidades, el administrador de redes e infraestructura nos proporcionó una muestra de tres equipos bajo cada uno de los siguientes sistemas operativos: Windows XP, Windows 7 y 8. No se tuvo acceso a equipos con Windows 10 para realizar las pruebas.

Análisis de vulnerabilidades con OpenVAS

En las siguientes tablas se resumen los resultados de vulnerabilidades encontradas a través de OpenVAS en las muestras de tres equipos cada uno con Windows XP, 7 y 8:

Host	High	Medium	Low	Log	False Positive
10.192.168.50	2	0	0	0	0
10.192.168.51	2	0	0	0	0
10.192.168.52	2	0	0	0	0
Total:	**6**	**0**	**0**	**0**	**0**

Tabla 10 - Resumen de Vulnerabilidades OpenVAS equipos W-XP

Host	High	Medium	Low	Log	False Positive
10.192.168.60	1	8	2	0	0

10.192.168.61	1	3	1	0	0
10.192.168.62	0	4	1	0	0
Total:	**2**	**15**	**4**	**0**	**0**

Tabla 11 - Resumen de Vulnerabilidades OpenVAS equipos W-7

Host	High	Medium	Low	Log	False Positive
10.192.168.70	2	3	1	0	0
10.192.168.71	1	1	1	0	0
10.192.168.72	1	4	1	0	0
Total:	**4**	**8**	**3**	**0**	**0**

Tabla 12 -Resumen de Vulnerabilidades OpenVAS equipos W-8

Análisis de vulnerabilidades con Nessus

En las siguientes tablas se resumen los resultados de vulnerabilidades encontradas a través de Nessus en las muestras de tres equipos cada uno con Windows XP, 7 y 8:

Host	Critical	High	Medium	Low	Info
10.192.168.50	4	0	4	1	22
10.192.168.51	4	0	3	1	30
10.192.168.52	4	0	4	1	22
Total:	**12**	**0**	**11**	**3**	**74**

Tabla 13 - Resumen de Vulnerabilidades Nessus equipos W-XP

Host	Critical	High	Medium	Low	Info
10.192.168.60	2	1	10	2	44
10.192.168.61	1	0	9	2	39
10.192.168.62	2	0	9	2	34
Total:	**5**	**1**	**28**	**6**	**117**

Tabla 14 - Resumen de Vulnerabilidades Nessus equipos W-7

Host	Critical	High	Medium	Low	Info
10.192.168.70	1	0	2	0	27
10.192.168.71	1	0	6	1	36
10.192.168.72	4	0	9	2	34
Total:	**6**	**0**	**0**	**0**	**0**

Tabla 15 - Resumen de Vulnerabilidades Nessus equipos W-8

En la tabla resumen de equipos con sistema operativo Windows XP se muestran 12 vulnerabilidades críticas, sin embargo el reporte de la herramienta Nessus indica de manera duplicada las vulnerabilidades relacionadas con el fin de vida del sistema así y la debilidad con el protocolo SMB en cada equipo.

En la mayor parte del análisis de las muestras se encuentran vulnerabilidades de criticidad alta. Por consiguiente se tomará un equipo de cada versión de Windows para detallar las vulnerabilidades y usarlos en la fase siguiente.

Host Windows XP 10.192.168.50

Con OpenVAS las vulnerabilidades con calificación más alta son las siguientes:

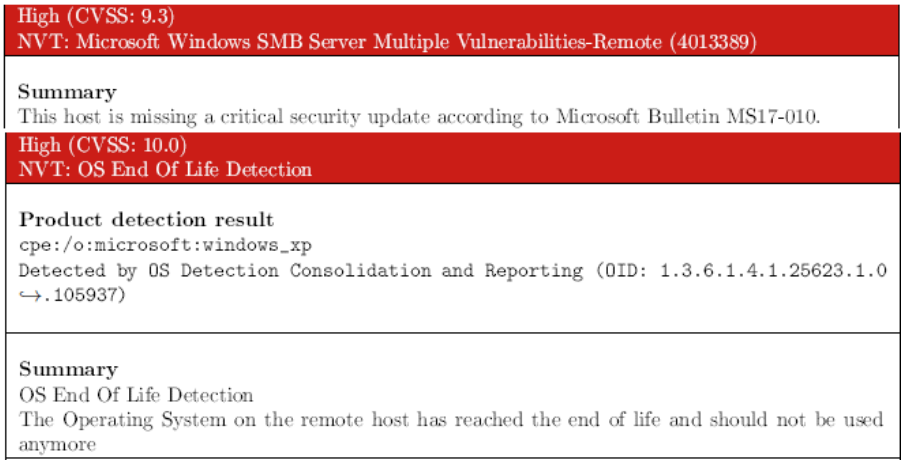


Gráfico 43 - Vulnerabilidades críticas OpenVAS equipo W- XP

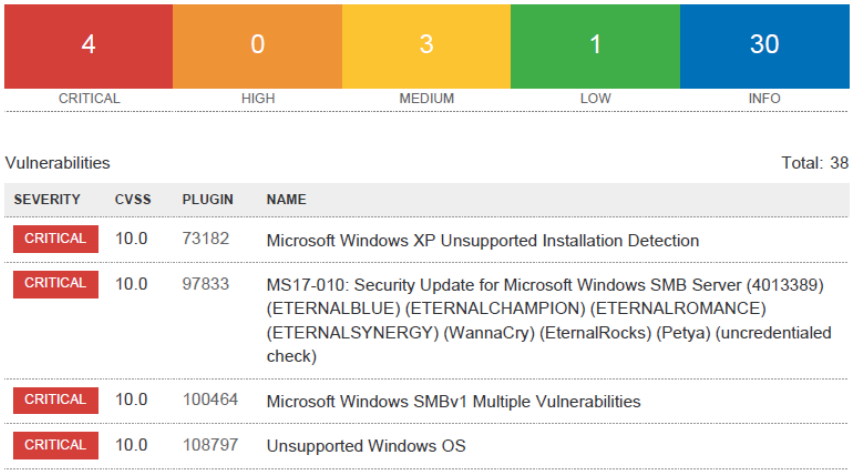


Gráfico 44 - Vulnerabilidades críticas Nessus equipo W- XP

Las principales vulnerabilidades corresponden a que el sistema operativo ya no está soportado por el fabricante lo cual puede incurrir en nuevas vulnerabilidades que se lleguen a encontrar en estos sistemas y no se tenga el soporte para actualizaciones que puedan mitigar esos nuevos agujeros de seguridad. La otra vulnerabilidad contempla la falla del protocolo SMB.

Host Windows-7 10.192.168.60

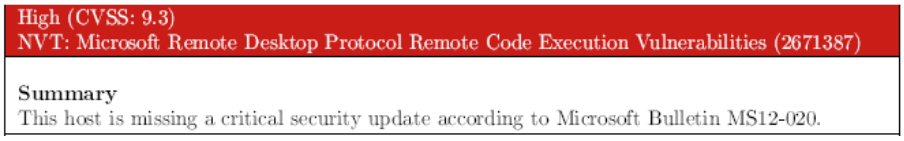


Gráfico 45 - Vulnerabilidades críticas OpenVAS equipoW- 7

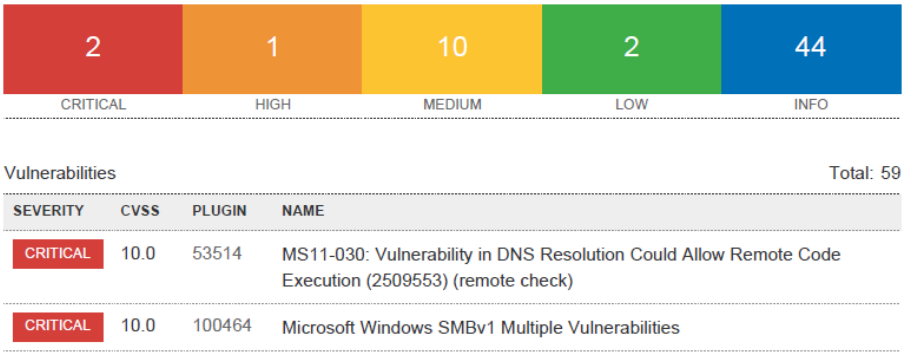


Gráfico 46 - Vulnerabilidades críticas Nessus equipoW-7

Host Windows-8 10.192.168.70

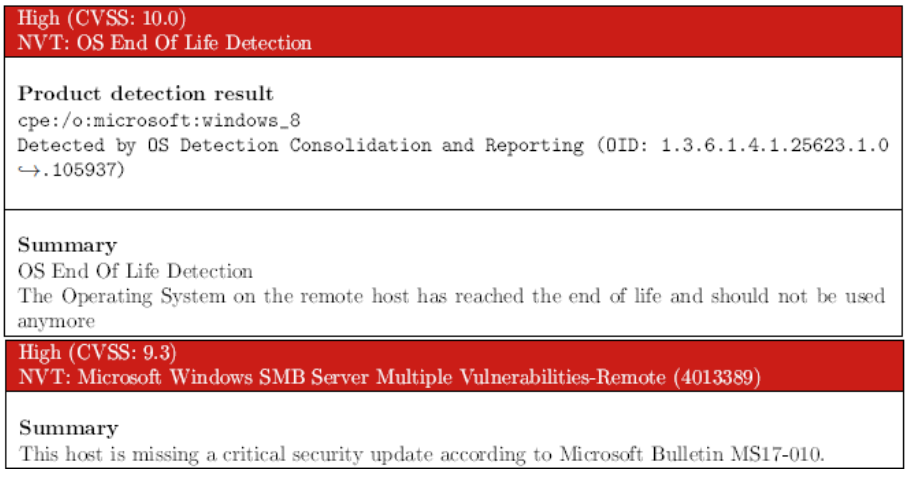


Gráfico 47 - Vulnerabilidades críticas OpenVAS equipo W-8

4	0	9	2	34
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 49

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
CRITICAL	10.0	88561	Microsoft Windows 8 Unsupported Installation Detection
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS

Gráfico 48 - Vulnerabilidades críticas Nessus equipo W- 8

4.5 Explotación

Después de haber analizado el conjunto de vulnerabilidades críticas detectadas en los equipos explorados, se buscó aprovechar y explotar las mismas para comprometer la seguridad de la infraestructura. Se empleó Metasploit (ver gráfico 43) como framework de explotación, tal y como se acordó en la fase de planificación.

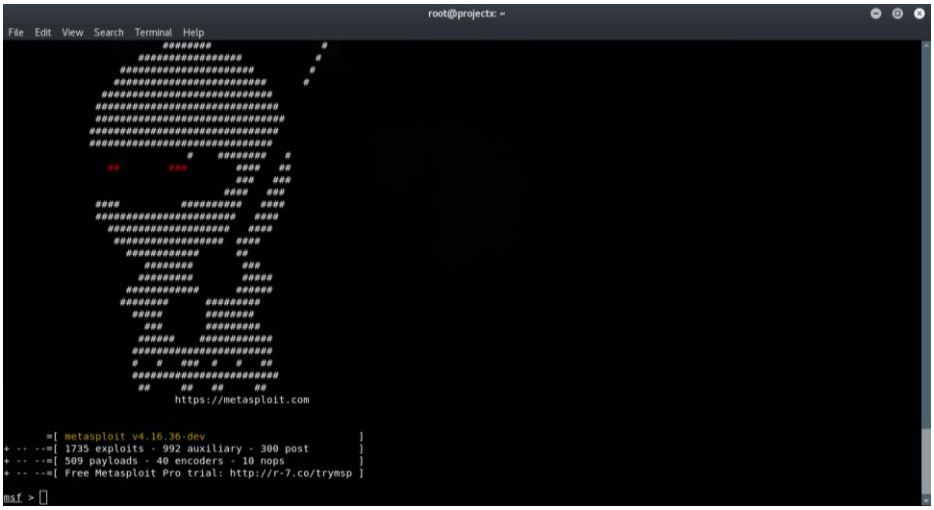


Gráfico 49 - Consola de Metasploit

Explotación Host Windows Server 10.192.168.1

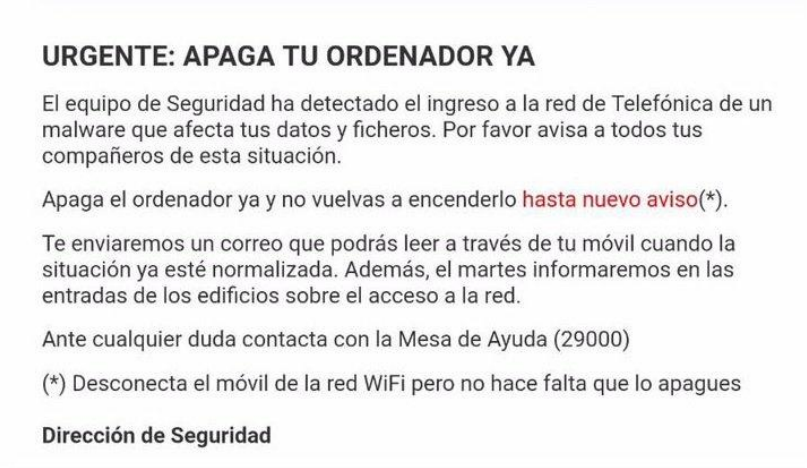
En este equipo se identificó como vulnerabilidad crítica una debilidad en el protocolo SMB. Este protocolo permite hacer uso de recursos compartidos

(archivos, impresoras, etc.) entre equipos con sistema operativo Windows Server a través de la red.

El año pasado, en el mes de abril, un grupo de hackers autodenominados *The Shadow Brokers* dieron a conocer un leak de exploits que se eran usados por la Agencia de Seguridad Nacional (NSA) de los estados Unidos. Esta noticia causó conmoción debido al acceso que en su momento tuvo la agencia gracias a sus exploits. A fecha de la noticia muchos de los exploits ya no funcionaban puesto que Microsoft ya había creado y publicado gran parte de los parches requeridos para las diferentes versiones de su sistema operativo [24].

A pesar de que la mayoría de los exploits no funcionaban en las versiones parchadas de Windows Server, hubo algunos que todavía eran efectivos a la práctica. Uno de ellos denominado "Eternalblue" (CVE-2017-0144) aprovechaba una debilidad en el protocolo SMB y explotando la misma conseguía acceso al equipo víctima. Microsoft lanzó el *Security Bulletin* MS17-010 publicando el parche para la vulnerabilidad [25].

Lamentablemente, no todas las empresas tomaron las medidas pertinentes y parchearon sus sistemas. Esto fue aprovechado por ciberdelincuentes que lanzaron ataques masivos de ransomware aprovechando "Eternalblue". Empresas de la talla de Telefónica Movistar, en España, fueron unas de las primeras víctimas [26] e incluso tuvieron que tomar medidas extremas llegando a indicar a sus empleados que apagaran sus equipos para que no continuara la propagación del ataque (ver gráfico 44).



URGENTE: APAGA TU ORDENADOR YA

El equipo de Seguridad ha detectado el ingreso a la red de Telefónica de un malware que afecta tus datos y ficheros. Por favor avisa a todos tus compañeros de esta situación.

Apaga el ordenador ya y no vuelvas a encenderlo hasta nuevo aviso(*).

Te enviaremos un correo que podrás leer a través de tu móvil cuando la situación ya esté normalizada. Además, el martes informaremos en las entradas de los edificios sobre el acceso a la red.

Ante cualquier duda contacta con la Mesa de Ayuda (29000)

(*) Desconecta el móvil de la red WiFi pero no hace falta que lo apagues

Dirección de Seguridad

Gráfico 50 – Comunicado interno de Telefónica Movistar tras Wannacry [27]

Después del ataque de Wannacry, aparecieron variantes de este ransomware; fueron conocidas como Petya - NotPetya y usaban la misma debilidad de "Eternalblue". Varias empresas y entidades públicas, como hospitales, vieron como sus archivos y bases de datos fueron encriptados. El 2017 fue un año en donde este tipo de malware causó mucho daño [28].

El equipo 10.192.168.1 era vulnerable a EternalBlue de acuerdo a los reportes arrojados por OpenVAS y Nessus. Se trató de explotar dicha vulnerabilidad siguiendo el trabajo de Berta [25], pero no se tuvo éxito ya que se necesitaba que la cuenta de invitado se encuentre activa en el equipo víctima o a su vez disponer de credenciales de alguna cuenta y parametrizarlas en el exploit. Se realizaron pruebas adicionales siguiendo los post de iHackLabs [29] y Undercode [30] pero tampoco se tuvo éxito.

Retomando el reporte de Nessus referente a esta vulnerabilidad, el detalle indicaba que el host también era vulnerable a otros exploits. En la investigación se encontró que un usuario en la plataforma GitHub de metasploit realizó una actualización de tres exploits de la NSA de aquel leak de abril del año pasado [24]. Los tres exploits fueron EternalChampion, EternalRomance y EternalSynergy [31].

El investigador denominado "zerosum0x0" actualizó los exploits que en su momento fueron lanzados por el usuario "worawit". Estos cambios permiten

que se pueda tomar el nombre de las Named Pipe (canales de comunicación entre procesos) que sean accesibles para inicios de sesión anónimos. El proceso se pudo llevar a cabo usando dos scripts dentro del módulo auxiliar y el módulo de explotación en Metasploit respectivamente [32]. El equipo técnico de Rapid7 publicó un video demostrativo a los pocos días confirmando el éxito de estos scripts en la práctica [33].

Primero se inició Metasploit a través del comando msfconsole en una terminal, una vez que cargada la consola, se invocó el script correspondiente al escáner ubicado dentro del módulo auxiliar y se configuró el objetivo. Para ello se usó el parámetro "use" seguido del nombre y ubicación del script en este caso "auxiliary/admin/smb/ms17_010_command". Se configuró la IP del host con el comando "RHOSTS" seguido de la IP o rango, tal y como se puede observar en el gráfico 46.

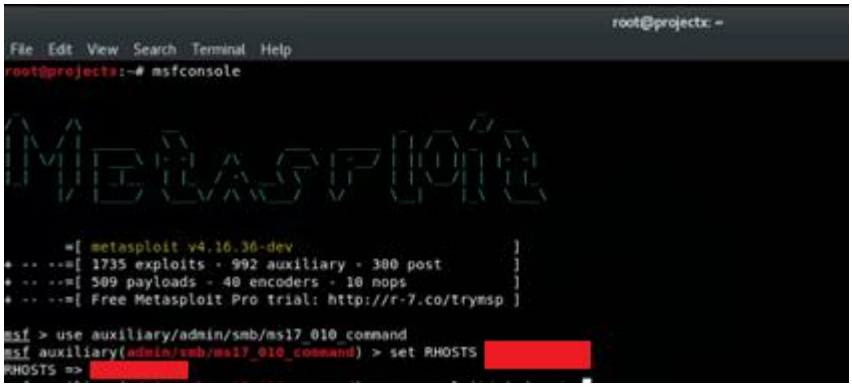


Gráfico 51 - Módulo Auxiliar ms17_010_command

Dentro de Metasploit se puede ejecutar cualquier script cargado y configurado con el parámetro "run". El resultado para este caso dejó claro que el host objetivo era vulnerable. Adicionalmente, en el resultado aparecieron nombres de usuario de miembros del grupo Administradores de Dominio (el servidor atacado es un controlador de dominio).

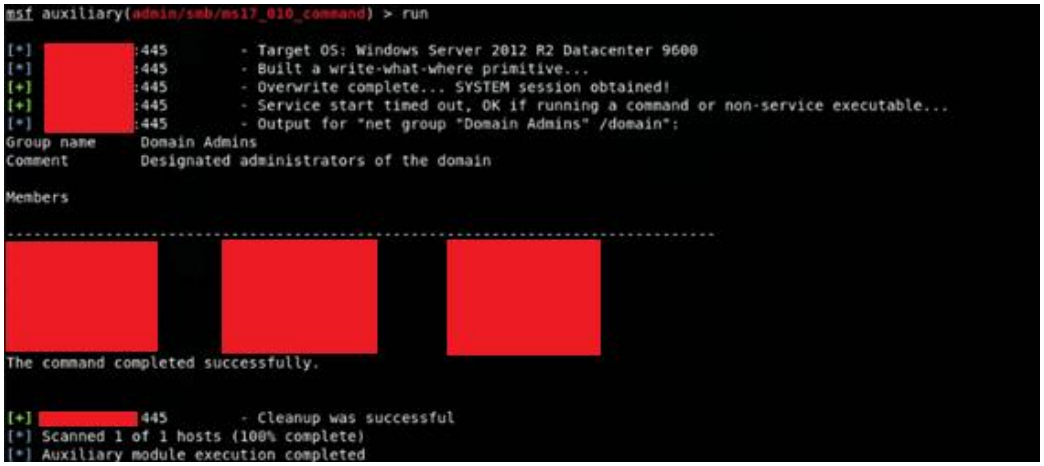


Gráfico 52 - Resultado ejecución ms17_010_command

Acto seguido, se recurrió al script del módulo de explotación y se configuró el host con el comando "RHOST" (ver figura 47).

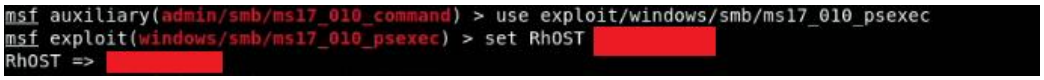


Gráfico 53 - Módulo de explotación ms17_010_psexec

La ejecución del script de explotación arrojó una sección de meterpreter con conexión reversa, que permitió el acceso al equipo.

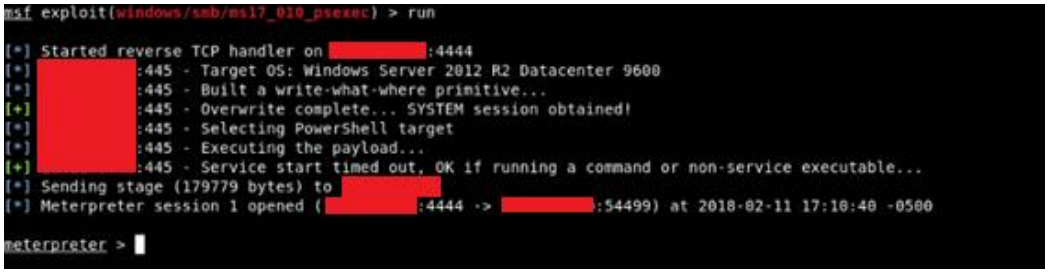


Gráfico 54 - Resultado ejecución ms17_010_psexec

En la sesión de meterpreter, se creó una instancia de powershell en el equipo objetivo. En este punto fue muy importante escalar privilegios. Para ello se usó el comando "getsystem".

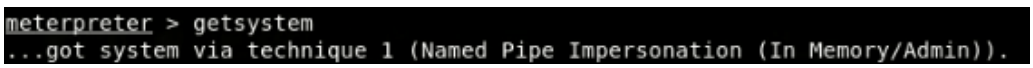


Gráfico 55 - Ejecución getsystem

Para disponer de una sesión más estable se migró la sesión a otro proceso. Para ello, se obtuvo el listado de todos los procesos que se encontraban

ejecutándose en el equipo víctima a través del comando “ps”. Del listado se seleccionó el proceso winlogon con PID 20500:

Gráfico 56 - PID proceso local

Para migrar el proceso simplemente se ejecutó el comando “migrate” seguido del PID seleccionado (ver gráfico 51).

Gráfico 57 - Migración de proceso meterpreter

Tras la migración exitosa del proceso, se decidió buscar credenciales de usuarios en el equipo. Se optó por la herramienta Mimikatz que viene por defecto en Kali Linux y permite extraer credenciales que se encuentran en la memoria del equipo [34]. Para ejecutar esta herramienta fue necesario cargarla al equipo víctima a través del comando “upload” y definiendo el path.

De manera seguida se invocó una Shell de Windows con el comando “shell”. A partir de ahí, se cambió la ubicación al path donde se subió el archivo y se ejecutó el mismo.

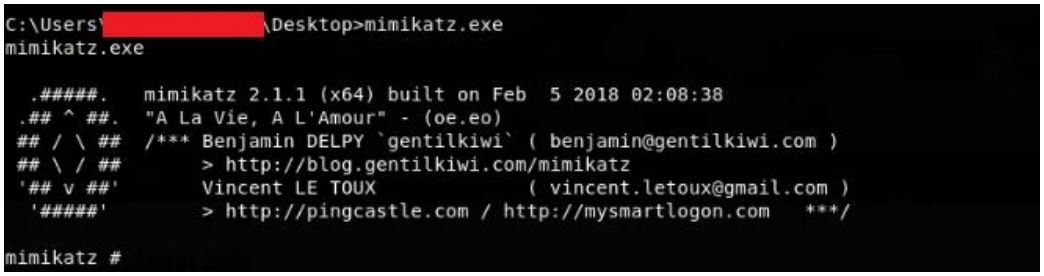


Gráfico 58 – Consola Mimikatzs

Finalmente, se ejecutó el comando “sekurlsa::logonpasswords”, el que permitió obtener las credenciales almacenadas en la memoria del equipo, según se muestra en el gráfico 53.

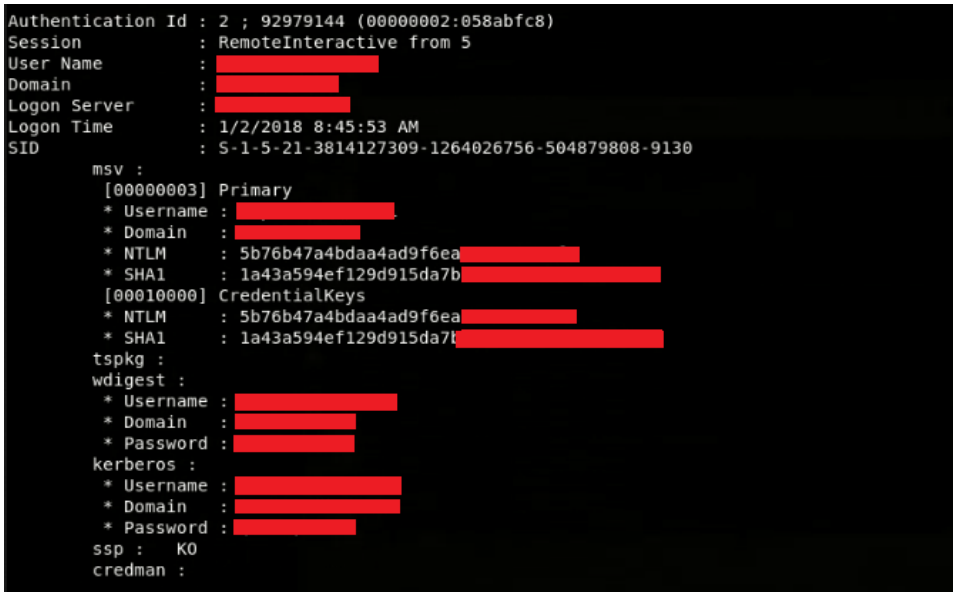


Gráfico 59 - Credenciales obtenidas Mimikatz

Explotación Host Windows Server 10.192.168.3

La principal vulnerabilidad en este equipo fue la identificada en el CVE-2015-1635. Esta vulnerabilidad permite la ejecución remota en la pila del protocolo HTTP; se produce cuando HTTP.sys analiza incorrectamente solicitudes HTTPS especialmente diseñadas [35]. El explotar esta vulnerabilidad causa el reinicio del equipo y por ende la indisponibilidad del servicio. Debido a la importancia del servidor identificado, el departamento de Tecnología nos indicó que no se validara en la práctica la existencia de esta vulnerabilidad.

Sin embargo, para realizar la validación en función del presente ejercicio académico, se reprodujo el ambiente en cuestión utilizando una máquina virtual provista por Rapid7. La misma es denominada como Metasplotaible 3 [36] y fue creada para realizar pruebas de penetración. En la misma se levantó el servicio de IIS.

Se realizó un escaneo de vulnerabilidades con Nessus para validar que se encuentre la misma debilidad que el servidor de producción, lo que se corroboró, como lo indica el gráfico 54).

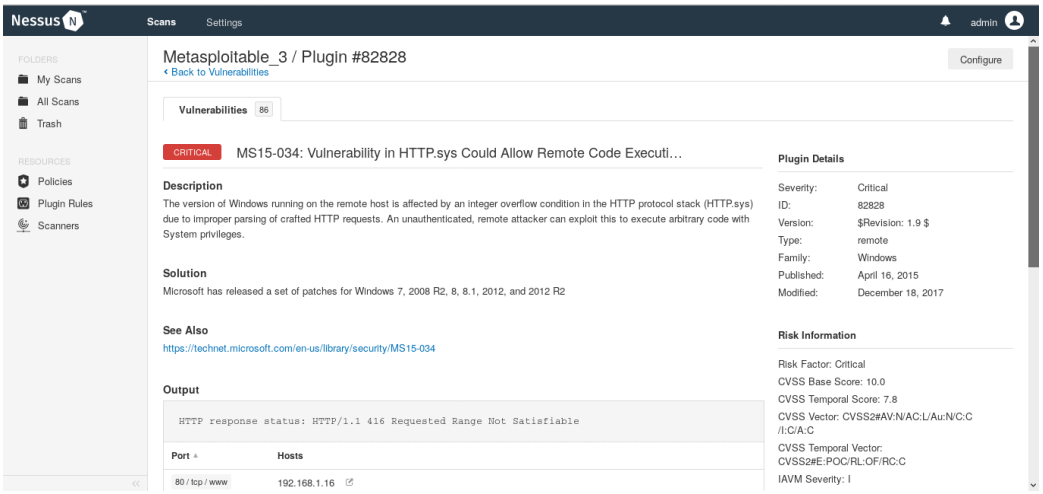


Gráfico 60 - Vulnerabilidad MS15-034 metasploitable

Para el proceso de explotación se usó un script del módulo auxiliar de metasploit denominado "ms15_034_ulonglongadd" [37]. Para configurar el script solo se necesitó como parámetro la dirección IP del host víctima. Se configuró la IP a través del comando "RHOST" y se ejecutó con el comando "run" (como se aprecia en el gráfico 55).

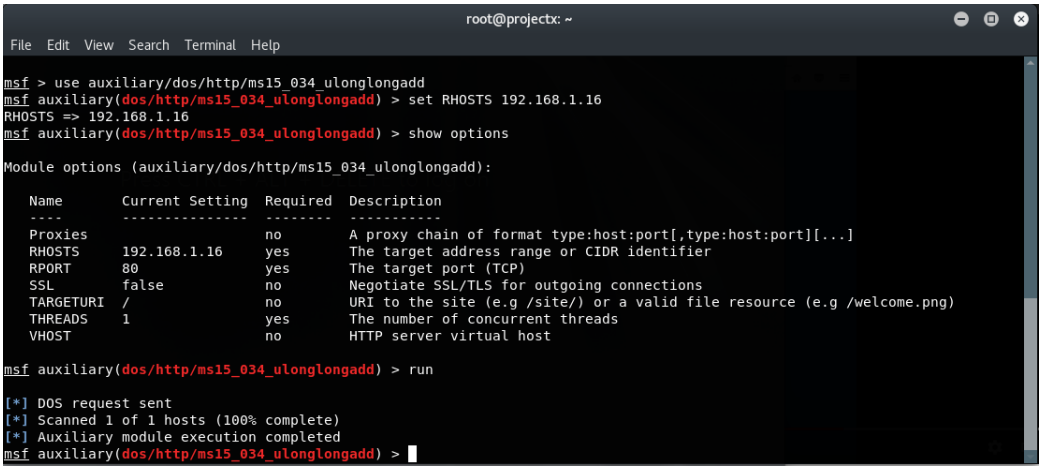


Gráfico 61 - Ejecución exploit ms15_034_ ulonglongadd

El equipo víctima se reinició y se ratificó el ataque en el visor de eventos de Windows. En el gráfico 57 se evidencia el proceso de reinicio del servidor, que tuvo lugar.

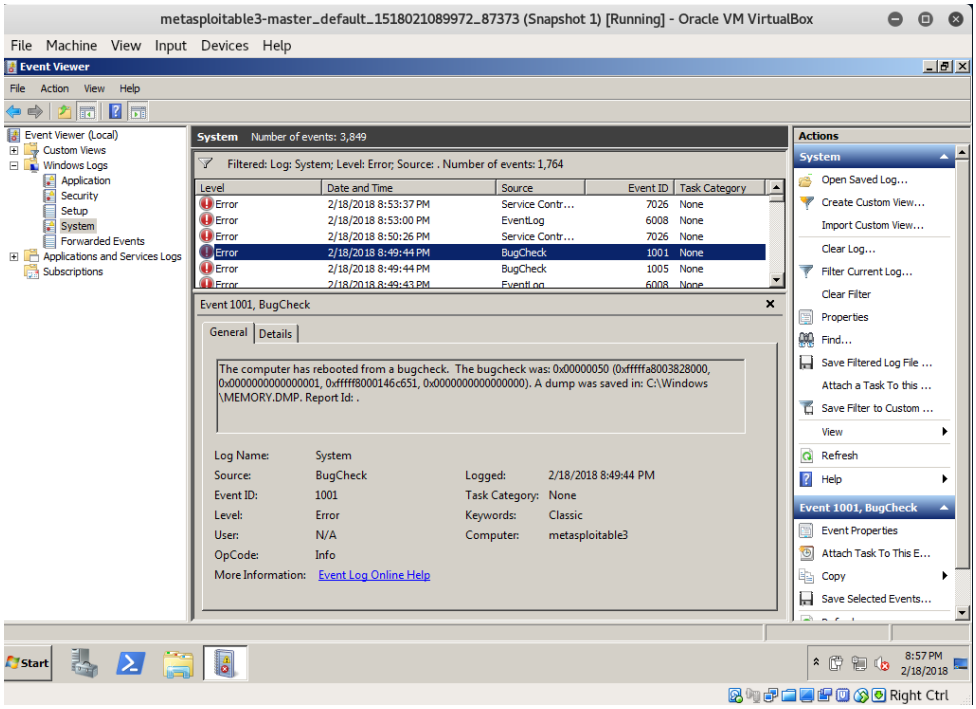


Gráfico 62 - Event Viewer error en el sistema

Explotación Host GNU/Linux 10.192.168.6

En este caso, particularmente no fue necesario usar un exploit pues la principal vulnerabilidad fue el acceso al equipo vía telnet sin colocar ningún tipo de usuario o contraseña.

Para la demostración simplemente se ejecutó una sesión de telnet a través de la utilidad Putty hacia la IP del equipo y el puerto 23.

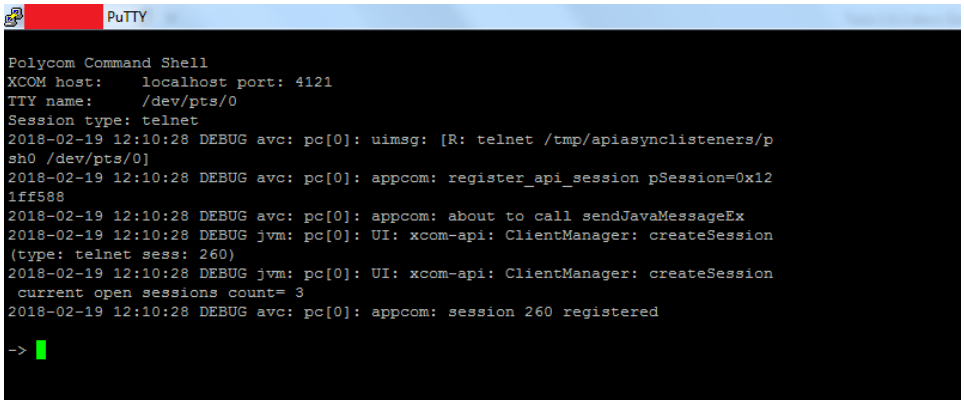


Gráfico 63 - Resultado acceso telnet sin credenciales

Explotación Host Windows XP 10.192.168.50

Se explotó la vulnerabilidad relacionada al protocolo SMB, usando el mismo exploit que se usó para los servidores consiguiendo una sesión de meterpreter exitosamente.

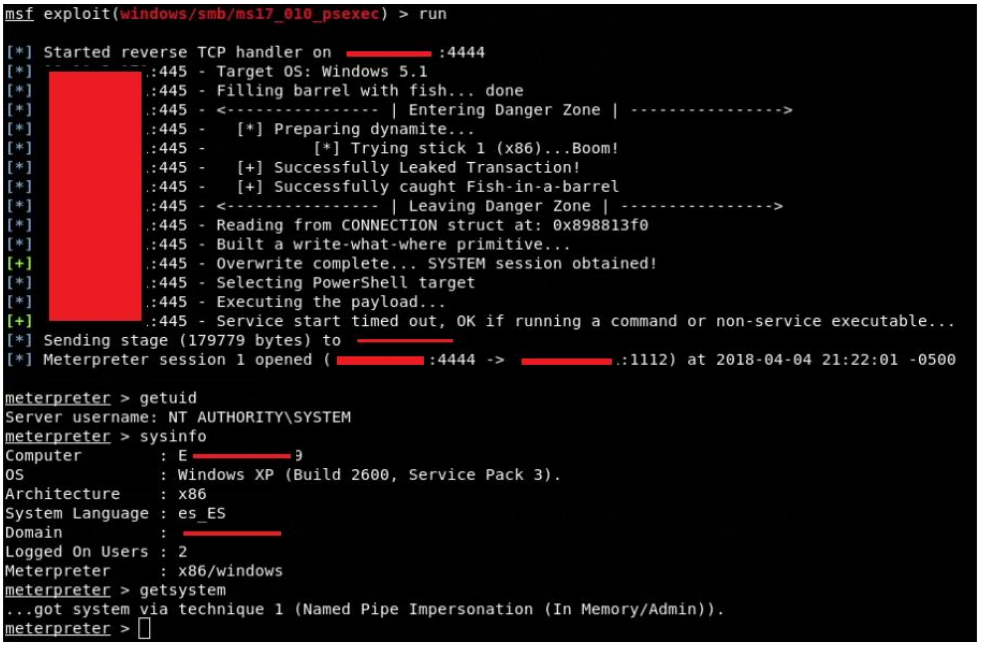


Gráfico 64 - Vulnerabilidad protocolo SMB equipo W-XP

A diferencia de la explotación del servidor, los mensajes del proceso de explotación son distintos haciéndolos un poco más jocosos.

Explotación Host Windows 7 10.192.168.60

En este equipo se identificaron tres vulnerabilidades críticas incluyendo una vez más la relacionada con el protocolo SMB a la cual se suma una vulnerabilidad que permite realizar un ataque de denegación de servicio. Se realizó el proceso de explotación a esta vulnerabilidad publicada en el boletín de seguridad de Microsoft MS12-020. Para ello lo único que hizo uso del exploit *ms12_020_maxchannelids* parametrizando únicamente el host contra el que se lanza el ataque:

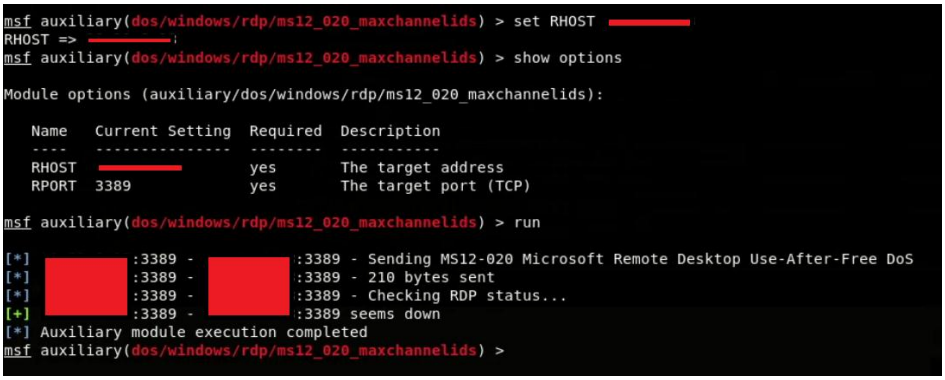


Gráfico 65 - Vulnerabilidad al protocolo RDP

Explotación Host Windows 8 10.192.168.70

En este equipo se identificaron varias vulnerabilidades catalogadas como críticas, siendo el tiempo de vida útil del sistema operativo uno de ellos ya que corresponde a la versión de Windows 8. Adicional a esta se encontraron vulnerabilidades relacionadas al boletín de Microsoft MS14-066, sin embargo no se encontró un exploit dentro de metasploit para poder llevar a cabo el proceso de explotación. Se recurrió a la vulnerabilidad del protocolo SMB sin embargo el exploit usado no pudo obtener una sesión de meterpreter.

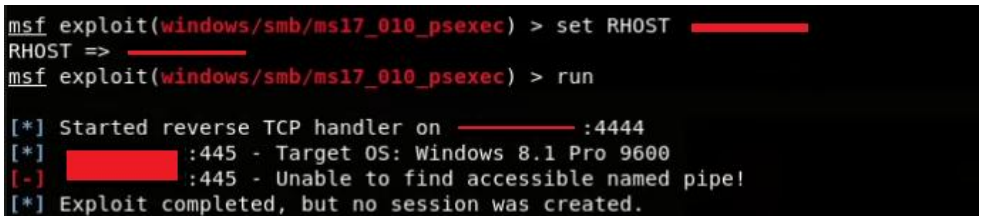


Gráfico 66 - Vulnerabilidad SMB equipo W-8

4.6 Documentación

En esta etapa se debe realizar dos informes que expliquen en resumen los hallazgos identificados en el ejercicio de hacking ético. El primero se denomina informe ejecutivo ya que está dirigido hacia los directivos de la empresa y por tanto no debe contener palabras muy técnicas, sin embargo es importante que se recalquen los riesgos a los que se encuentra expuesta la empresa.

El segundo es el informe técnico, en este se detallan las pruebas realizadas y las vulnerabilidades que fueron encontradas considerando el daño que se

puede percibir tras haber materializado las mismas en la fase de explotación. En este informe también se reseñan las medidas de remediación y mitigación.

Informe Ejecutivo

La ejecución del presente proyecto realizado a la empresa Plasticaucho Industrial S.A. permitió poner a prueba su infraestructura tecnológica sin ocasionar problemas de indisponibilidad, confidencialidad o integridad en ninguna de las fases. Cabe recalcar que en todo momento se tuvo el consentimiento de los involucrados. El análisis resultante busca demostrar la perspectiva que puede llegar a tener un atacante y los posibles caminos que puede optar para comprometer la seguridad tecnológica de la empresa.

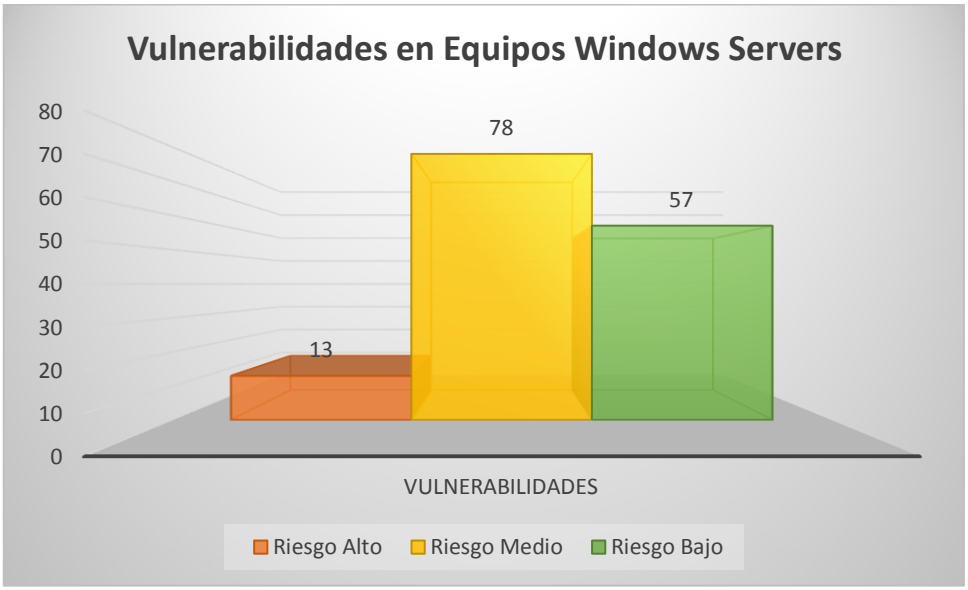
A continuación se muestra una escala de riesgos misma que servirá de base para clasificar las diferentes vulnerabilidades y debilidades que fueron identificadas en el desarrollo del proyecto.

Riesgo Alto: Estos hallazgos identifican situaciones que podrían comprometer directamente una red, sistema, aplicación, información o el acceso no autorizado de los mismos.

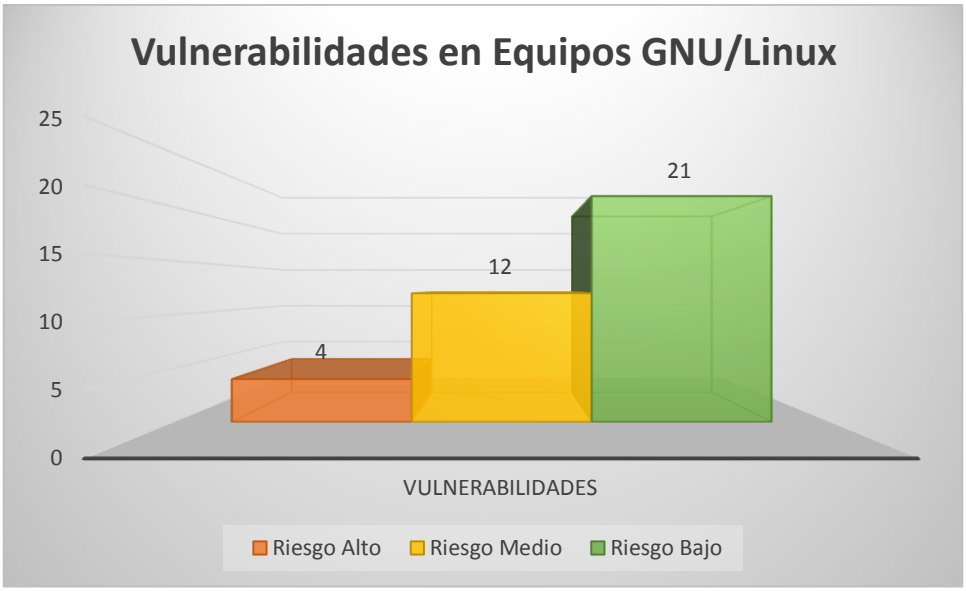
Riesgo Medio: Estos hallazgos identifican situaciones que no podrían comprometer directamente una red, sistema, aplicación, información o el acceso no autorizado de los mismos, pero proporcionan una funcionalidad o información que podrían en combinación con el conocimiento del atacante llegar a comprometer una red, sistema, aplicación, información o el acceso no autorizado de los mismos.

Riesgo Bajo: Estos hallazgos identifican situaciones que no podrían comprometer directamente una red, sistema, aplicación, información o el acceso no autorizado de los mismos, pero proporcionan en menor grado información que en combinación con otras funcionalidades y el conocimiento del atacante pueden llegar a comprometer una red, sistema, aplicación, información o el acceso no autorizado de los mismos. Hallazgos de bajo riesgo también pueden demostrar un enfoque incompleto a la aplicación de medidas de seguridad en el entorno.

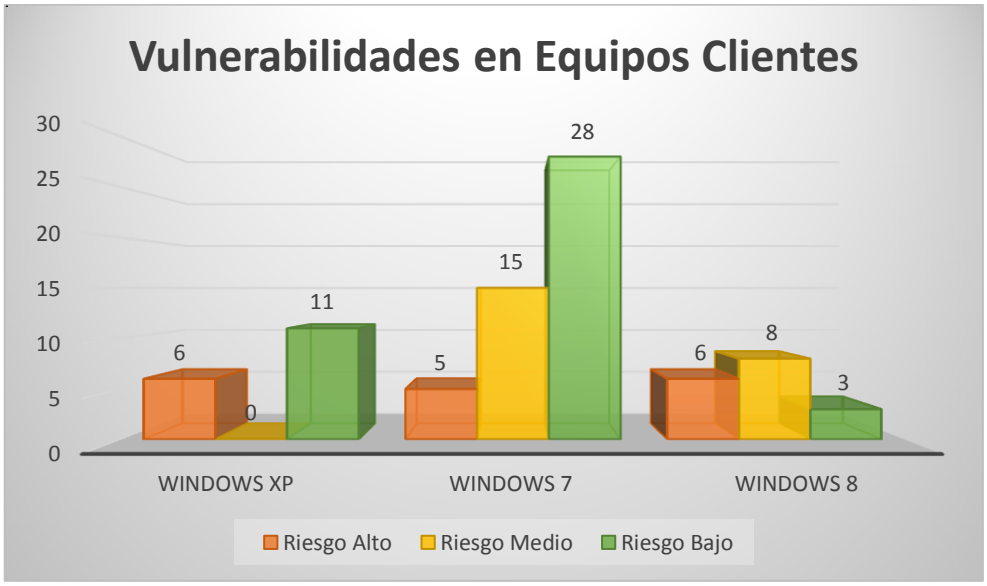
Criticidad de las Vulnerabilidades



A pesar de haber identificado un bajo número de vulnerabilidades categorizadas con riesgo alto, las mismas fueron suficientes para acceder a los sistemas y comprometer la infraestructura. Se encontraron en mayor número, vulnerabilidades categorizadas con un riesgo medio, sin embargo la factibilidad para explotar estas vulnerabilidades es menor. Finalmente existe un número también significativo de vulnerabilidades con riesgo bajo que en su mayoría solo son informativas.



Entre las 4 vulnerabilidades identificadas con riesgo alto, una de ellas permite el acceso sin credenciales aprovechando malas configuraciones. Le siguen un número menor en cuanto a vulnerabilidades de riesgo medio y finalmente una alta cifra de vulnerabilidades con riesgo bajo, mismas que no comprometen el acceso a la infraestructura.



A pesar que los sistemas operativos Windows analizados se encuentran licenciados, requieren un upgrade o cambio inmediato de versión como es el caso de los equipos con sistemas operativos Windows XP y Windows 8. Estos equipos evidencian mayor cantidad de vulnerabilidades críticas, una de

las razones es que ya no se encuentran soportados por el fabricante y están altamente expuestos ante nuevas amenazas.

Respecto a la muestra tomada de los sistemas operativos con Windows 7 se encontraron un número menor de debilidades con riesgo alto sin embargo fueron suficientes para quebrantar los sistemas.

Es importante recalcar que el impacto resultante de la materialización de vulnerabilidades con riesgo alto implicaría la indisponibilidad de servicios tecnológicos así como el robo o acceso no autorizado a aplicaciones e información de la empresa.

Informe Técnico

El presente proyecto se desarrolló en conjunto con el personal de infraestructura del departamento de TI, conociendo las actividades que fueron llevadas a cabo. A continuación se resume el proceso realizado y el detalle de las vulnerabilidades identificadas así como las medidas de remediación que se sugieren. Cabe mencionar las principales herramientas usadas en el ejercicio de hacking ético:

- Kali GNU/Linux Rolling 2018.1: Plataforma de testeo.
- Windows 10 Pro: Plataforma de testeo y documentación
- TheHarvester 2.7: herramienta de recolección de información.
- Whois Version 5.3.0: herramienta de recolección de información.
- Nslookup Kali GNU/Linux Rolling 2018.1: herramienta DNS.
- Fierce 0.9.9: herramienta de recolección de información.
- FOCA 3.4: análisis de metadatos.
- Nmap version 7.60: escaneo de la red y puertos.
- Nessus Home 7.0.3: herramienta para análisis de vulnerabilidades.

- OpenVAS Version 7.0.2: herramienta para análisis de vulnerabilidades.
- Metasploit 4.16.36-dev: herramienta para explotación.

Para llevar a cabo el proyecto se plantearon el siguiente conjunto de etapas:

La calificación de las vulnerabilidades encontradas se basa en el CVSS (Common Vulnerability Score System) que se utiliza para estimar el impacto derivado de las vulnerabilidades.

Resumen de Vulnerabilidades

Microsoft Windows SMB Múltiples Vulnerabilidades CVE-2017-0144

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	**Alto**	**Alta**	**Bajo**

Detalle de la vulnerabilidad

Un fallo en el protocolo SMB para gestionar recursos compartidos de Windows permite la ejecución de código remota.

Equipos Afectados

- Windows Server 10.192.168.1
- Windows Server 10.192.168.3
- Windows XP 10.192.198.50 – 10.192.198.52

- Windows 7 10.192.198.60 -10.192.168.62
- Windows 8 10.192.198.70 -10.192.168.72

Remediación

Realizar la actualización de seguridad publicada por Microsoft en el boletín MS17-010. La misma incluye el parche para todas las versiones de sus sistemas operativos incluyendo Windows XP debido a la criticidad de la vulnerabilidad.

Vulnerabilidad Apache HTTP Server

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	Alto	Media	Bajo

Detalle de la vulnerabilidad

El Servidor Apache HTTP contiene una vulnerabilidad en el manejo de ciertas solicitudes HTTP codificadas en fragmentos que pueden permitir a los atacantes remotos ejecutar código arbitrario y una denegación de servicio (DoS).

Equipos Afectados

- Windows Server 10.192.168.1

Remediación

Actualizar Apache HTTP Server a la versión 2.4.26 o superior.

Vulnerabilidad Apache Tomcat

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	Alto	Media	Bajo

Detalle de la vulnerabilidad

La falla se debe a un error en la clase ´MultipartStream' en ‘Apache Commons Fileupload’ al procesar solicitudes de varias partes. La explotación

exitosa de esta debilidad puede materializarse en un ataque de denegación de servicio.

Equipos Afectados

- Windows Server 10.192.168.1

Remediación

Actualizar a las versiones 7.0.70, 8.0.36, 8.5.3, 9.0.0.M7, o superiores.

Microsoft Windows Vulnerabilidad HTTP.sys CVE-2015-1635

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	Alto	Media	Bajo

Detalle de la vulnerabilidad

Existe una vulnerabilidad de ejecución remota de código en la pila de protocolo HTTP (HTTP.sys) que se produce cuando HTTP.sys analiza incorrectamente solicitudes HTTP especialmente diseñadas. Puede convertirse en un ataque de denegación de servicio.

Equipos Afectados

- Windows Server 10.192.168.3

Remediación

Realizar la actualización de seguridad publicada por Microsoft en el boletín MS15-034. La misma incluye el parche para todas las versiones de sus sistemas operativos debido a la criticidad de la vulnerabilidad.

Vulnerabilidades en HP System Management Homepage HPSBMU03112

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	Alto	Medio	Alto

Detalle de la vulnerabilidad

Fueron identificadas varias vulnerabilidades y podrían explotarse de forma remota, lo que da como resultado la creación de secuencias de comandos entre sitios (XSS), la falsificación de solicitudes entre sitios (CSRF), la divulgación no autorizada de información, la denegación de servicio (DoS) y el clickjacking.

Equipos Afectados

- Windows Server 10.192.168.3

Remediación

Se recomienda seguir el procedimiento de actualización de acuerdo al boletín de seguridad **c04463322** publicado por HP. Se aconseja determinar la aplicabilidad de esta información a sus situaciones individuales y tomar las medidas apropiadas previa ejecución.

Acceso sin credenciales

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	**Alto**	**Bajo**	**Medio**

Detalle de la vulnerabilidad

Una debilidad como el acceso sin credenciales puede permite a un atacante ingresar al equipo y comprometer información o a su vez manipular la configuración del mismo.

Equipos Afectados

- GNU/Linux 10.192.168.6

Remediación

Realizar una correcta configuración de acceso a los equipos a través de los diferentes protocolos que pueden permitir el ingreso sin restricción a un atacante.

Microsoft Windows Vulnerabilidad en resolución DNS CVE-2016-0128

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	**Alto**	**Bajo**	**Bajo**

Detalle de la vulnerabilidad

La vulnerabilidad podría permitir la ejecución remota de código si un atacante obtuviera acceso a la red y luego crear un programa personalizado para enviar consultas de transmisión LLMNR especialmente diseñadas a los sistemas de destino, llegando a provocar una denegación de servicio.

Equipos Afectados

- Windows 7 10.192.168.50

Remediación

Realizar la actualización de seguridad publicada por Microsoft en el boletín MS11-030.

Microsoft Windows Vulnerabilidad en Escritorio Remoto CVE-2012-0152

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	**Alto**	**Bajo**	**Bajo**

Detalle de la vulnerabilidad

La vulnerabilidad podría permitir la ejecución remota de código si un atacante envía una secuencia de paquetes RDP especialmente diseñados a un sistema afectado.

Equipos Afectados

- Windows 7 10.192.168.50

Remediación

Realizar la actualización de seguridad publicada por Microsoft en el boletín MS12-020. Adicionalmente desactivar las conexiones de asistencia remota.

Microsoft Windows Fin de Vida de Producto (EOL)

Riesgo	Impacto	Dificultad de Explotación	Trabajo de Remediación
Alto	**Alto**	**Medio**	**Medio**

Detalle de la vulnerabilidad

El sistema operativo en los hosts remotos analizados han alcanzado el fin de vida dispuesto por el proveedor y deben dejar de ser usados.

Equipos Afectados

- Windows XP 10.192.168.50 – 10.192.168.52
- Windows 8 10.192.168.70 – 10.192.168.72

Remediación

Realizar la actualización de los sistemas operativos a nuevas versiones soportadas por el fabricante.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Tras el análisis realizado a la infraestructura de la empresa se identificó que los sistemas operativos en su mayoría son “Windows 7 Profesional”.

Adicionalmente en la infraestructura interna no se encontraron servidores relacionados a servicios de correo electrónico y hosting web, se convalidó lo mencionado analizando las entradas DNS del dominio. El factor de contratar infraestructura tecnológica con proveedores especializados disminuye el riesgo de afectación a estos servicios.

- Se identificó un número considerable de vulnerabilidades críticas en los equipos analizados permitiendo evaluar la exposición de las mismas ante ataques conocidos. Se demostró que conllevan un riesgo considerablemente alto con un impacto que puede llegar a ocasionar la denegación de servicios tecnológicos así como el acceso a información privilegiada de la infraestructura.
- Se encontraron debilidades en la configuración de acceso a equipos GNU/Linux en los cuales no es necesario disponer de credenciales de acceso, resultando sumamente fácil el ingreso a los mismos con tan solo conocer la dirección IP. Esto conllevaría la manipulación total de los equipos a disposición de un atacante.

5.2 Recomendaciones

- Se sugiere revisar el proceso de despliegue de actualizaciones tanto en los equipos clientes como en los servidores considerando los horarios para estas instalaciones y la disponibilidad del canal de comunicaciones. Esto reducirá en gran medida que la infraestructura se vea comprometida ante un ataque real.
- Se recomienda revisar la configuración de acceso a través de los diferentes protocolos (telnet, http, etc) en los diferentes equipos de modo que siempre soliciten credenciales y estas a su vez no sean usuarios por defecto y dispongan de contraseñas robustas. Esto reducirá el acceso de credenciales por defecto o ataques de fuerza bruta.

- Se sugiere realizar un ejercicio de Hacking Ético de manera periódica dado que permitirá corroborar si las vulnerabilidades identificadas anteriormente fueron corregidas y a su vez conocer si se encuentran nuevas debilidades en la infraestructura de Plasticaucho Industrial SA.

Bibliografía

[1] B. Rossi, «Information Age,» 23 05 2016. [En línea]. Available: http://www.information-age.com/five-years-information-security-what-has-changed-123461477/. [Último acceso: 20 07 2017].

[2] P. Argentina, «PwC Argentina: contruyendo relaciones, creando valor,» 2016. [En línea]. Available: https://www.pwc.com.ar/es/publicaciones/assets/resultadosdelaencuestaglobaldeseguridaddelainformacion.pdf. [Último acceso: 07 20 2017].

[3] K. Fernández, «¿Cuáles fueron los ciberataques más grandes de 2016?,» *ITNOW,* 2017.

[4] E. Comercio, «Filtración a Hacking Team revela posible espionaje a escala mundial,» *El Comercio,* 11 07 2015.

[5] S. K. A. Suriya Gebum*, «A COMPREHENSIVE STUDY ON ETHICAL HACKING,» *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY,* vol. 4, pp. 2-5, 2016.

[6] H. Berger y A. Jones, «Cyber Security & Ethical Hacking For SMEs,» *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society,* nº 12, pp. 1-6, 2016.

[7] Y. Wang y J. Yang, «Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool,» *31st International Conference on Advanced Information Networking and Applications Workshops,* pp. 110-113, 2017.

[8] C. Tori, Hacking Ético, Rosario, 2008.

[9] C. Alonso, «Un informático en el lado del mal,» 09 07 2012. [En línea]. Available: http://www.elladodelmal.com/2012/07/los-hackers-son-malos-o-todo-lo.html. [Último acceso: 24 05 2017].

[10] K. Beaver, Hacking for dummies 4th Edition, New Jersey: John Wiley & Sons, Inc., 2014.

[11] R. E. L. d. Jimenez, «Pentesting on Web Applications using Ethical,» *Central American and Panama Convention (CONCAPAN XXXVI), 2016 IEEE 36th,* p. 6, 2016.

[12] M. E. H. S. Luis Alcides Mendaño Mendaño, *IMPLEMENTACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA EL DESCUBRIMIENTO Y EVALUACIÓN DE VULNERABILDIADES DE LA RED DE UNA CARTERA DE ESTADO,* Quito, 2016.

[13] Dragon, «DragonJar,» [En línea]. Available: https://www.dragonjar.org/como-

realizar-un-pentest.xhtml. [Último acceso: 16 01 2018].

[14] L. C. Sandoval Melendez y A. E. Vaca Herrera, «IMPLANTACIÓN DE TÉCNICAS Y ADMINISTRACIÓN DE LABORATORIO PARA INVESTIGACIÓN DE ETHICAL HACKING,» Quito, 2013.

[15] Wikipedia, «Wikipedia,» 10 06 2017. [En línea]. Available: https://es.wikipedia.org/wiki/Google_Hacking. [Último acceso: 26 01 2018].

[16] mschwager, «GitHub,» [En línea]. Available: https://github.com/mschwager/fierce. [Último acceso: 29 01 2018].

[17] D. P. Engebretson, The Basics of Hacking and Penetration Testing, Waltham, USA: Syngress, 2013.

[18] J. Tibaquira, «Youtube,» 13 03 2017. [En línea]. Available: https://www.youtube.com/watch?v=I3fzrEW1vf4. [Último acceso: 02 02 2018].

[19] T. Al-Otaibi, «Exploit Database,» 29 11 2017. [En línea]. Available: https://www.exploit-db.com/ghdb/4626/. [Último acceso: 16 01 2018].

[20] Anónimo, «Exploit Database,» 31 07 2017. [En línea]. Available: https://www.exploit-db.com/ghdb/4565/. [Último acceso: 16 01 2018].

[21] Dxtroyer, «Exploit Database,» 07 06 2017. [En línea]. Available: https://www.exploit-db.com/ghdb/4513/. [Último acceso: 16 01 2018].

[22] Dxtroyer, «Exploit Datase,» 06 04 2017. [En línea]. Available: https://www.exploit-db.com/ghdb/4414/. [Último acceso: 16 01 2018].

[23] O. Security, «Exploit Database,» [En línea]. Available: https://www.exploit-db.com/. [Último acceso: 15 01 2018].

[24] D. Goodin, «ARS TECHNICA,» 14 Abril 2017. [En línea]. Available: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/. [Último acceso: 09 02 2018].

[25] S. A. Berta, «EXPLOTAR ETERNALBLUE PARA OBTENER UNA SHELL DE METERPRETER EN WINDOWS SERVER 2012 R2,» 2017.

[26] «Hipertextual,» 12 05 2017. [En línea]. Available: https://hipertextual.com/2017/05/wannacry-ransomware-ataque-telefonica. [Último acceso: 10 02 2018].

[27] E. P. Economía, «Twitter,» 12 05 2017. [En línea]. Available: https://twitter.com/EPeconomia/status/863004888543973377/photo/1?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fhipertextual.com%2F2017%2F05%2Fwannacry-ransomware-ataque-telefonica. [Último acceso: 10 02 2018].

[28] A. Hern, «The Guardian,» 30 12 2017. [En línea]. Available:

https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware. [Último acceso: 10 02 2018].

[29] C. P. Gonzalez, «iHackLabs,» 08 05 2017. [En línea]. Available: https://www.ihacklabs.com/es/poc-eternalblue-y-doublepulsar-en-kali-2017-1-explotando-servicio-smb-en-windows-7/. [Último acceso: 10 03 2018].

[30] Xyz, «Undercode,» 08 02 2018. [En línea]. Available: https://blog.underc0de.org/obteniendo-un-meterpreter-con-eternalblue/. [Último acceso: 10 02 2018].

[31] C. Borghello, «Blog Segu-Info,» 08 02 2018. [En línea]. Available: https://blog.segu-info.com.ar/2018/02/actualizan-y-re-publican-tres-exploits.html. [Último acceso: 12 02 2018].

[32] zerosum0x0, «GitHub,» 03 02 2018. [En línea]. Available: https://github.com/rapid7/metasploit-framework/pull/9473. [Último acceso: 12 02 2018].

[33] Metasploit, «Youtube,» 08 02 2018. [En línea]. Available: https://www.youtube.com/watch?v=cYtDxfKdlqs. [Último acceso: 10 02 2018].

[34] gentilkiwi, «GitHub,» 06 04 2014. [En línea]. Available: https://github.com/gentilkiwi/mimikatz. [Último acceso: 12 02 2018].

[35] Microsoft, «Microsoft,» 14 04 2015. [En línea]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-034. [Último acceso: 12 02 2018].

[36] W. Chen, «Rapid 7,» 2016 11 2016. [En línea]. Available: https://blog.rapid7.com/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/. [Último acceso: 19 02 2018].

[37] «Rapid 7,» [En línea]. Available: https://www.rapid7.com/db/modules/auxiliary/dos/http/ms15_034_ulonglongadd.

[38] Hipertextual, «www.hipertextual.com,» 20 05 2016. [En línea]. Available: https://hipertextual.com/2016/05/hackeo-banco-del-austro. [Último acceso: 12 05 2017].

[39] C. Palmer, «Ethical Hacking,» *IBM Systems Journal,* vol. 40, pp. 769-780, 2001.

[40] K. Beaver, Hacking For Dummies®, John Wiley & Sons, Inc., 2013.

[41] Dragon, «DragonJar,» 2014. [En línea]. Available: https://www.dragonjar.org/owasp-testing-guide-4-0-en-espanol.xhtml. [Último acceso: 18 02 2018].

ANEXOS

Anexo A

EXPECTATIVAS, OBSERVACIONES Y RECOMENDACIONES DE AUDITORÍA

I. Debilidades Relacionadas al Proceso – Expectativas, Observaciones y Recomendaciones

Expectativa:	**FUENTE:**
No existe una política o procedimiento.	

Observación 1: ***No existe una actividad de control que permita realizar auditorías de ethical hacking y verificar vulnerabilidades para evitar que hackers ingresen en los sistemas de la empresa.***	
Condición: Se puede evidenciar que no existe una actividad de control establecida en la normativa del área de Tecnología de la Información que permita realizar auditorías de ética hacking y verificar vulnerabilidades para evitar que hackers ingresen a los sistemas de la empresa. *Efecto*: Robo de la información y pérdida de confidencialidad de la información sensible para la empresa y por ende perdidas económicas.	
Análisis de la causa	**Riesgo**
No se ha ejecutado por modificaciones en el presupuesto para adquirir un programa de ética hacking. No se encuentra establecida una actividad interna de control que permita realizar auditorías de ética hacking y determinar vulnerabilidades para solventarlas por el propio personal de TI.	Particularmente Severo
Recomendación	
Se recomienda al área de Tecnología de la Información implementar una actividad de control que permita realizar auditorías de ética hacking con los recursos disponibles, además de incluir políticas y procedimientos al respecto.	

Anexo B

ACUERDO DE CONFIDENCIALIDAD

Los comparecientes por medio del presente acuerdo de confidencialidad y con base en la documentación presentada para el proyecto de investigación de "Ethical Hacking" conforme a las demás condiciones que se indican a continuación y las especificaciones detalladas acuerdan que según se utiliza en el presente, "Información Confidencial" incluirá, sin carácter limitativo, los siguientes conceptos:

a. Toda información relativa a cualquiera de las Partes [la "Parte Divulgadora"), a la cual se otorga acceso a la otra parte (la "Parte Receptora"}, ya sea que dicha información sea divulgada en forma electrónica, visual, escrita o mediante cualquier otra forma tangible y que sea identificada como confidencial o de propietaria por la Parte Divulgadora, o que la Parte Receptora entienda razonablemente que es confidencial o de propiedad de la Parte Divulgadora;

b. Todo conocimiento, ideas, métodos de operación, procesos, conocimientos técnicos, tecnología, datos, fórmulas, bases de datos, especificaciones, secretos comerciales, software, mejoras, planes y estrategias de marketing, pronósticos y oportunidades de negocios, listas de clientes e interfaces gráficas de usuario en relación con el código objeto, código fuente, software, productos de software, servicios y sistemas relacionados que la Parte Divulgadora considera confidenciales y propietarios y que, si fuesen divulgados a terceros, podrían resultar en un perjuicio a nivel de la competencia para la Parte Divulgadora; y,

c. Todo el software y propiedad intelectual de terceros que cada una de las Partes pudiese estar obligada a proteger.

OBLIGACIONES ESPECÍFICAS.

En contraprestación de proporcionar dicha información y evaluar, promover o concretar el proyecto presentado, cada uno de los signatarios por el presente acepta lo siguiente:

a. La Parte Receptora mantendrá en confidencialidad y no divulgará: (a) cualquier Información Confidencial obtenida directa o indirectamente de la Parte Divulgadora; (b) cualquier información que resulte del acceso de la Parte Receptora o de la evaluación de dicha información; y, (c) cualquier trabajo de desarrollo realizado por la Parte Receptora utilizando la Información Confidencial.

b. La Parte Receptora acuerda no utilizar la Información Confidencial, ni parte de la misma, para ningún fin distinto de los relativos a la prestación de los servicios contemplados en los acuerdos comerciales que pudieren resultar entre las Partes.

c. La Parte Receptora no permitirá que la Información Confidencial sea puesta a disposición de terceros salvo que la Parte Divulgadora apruebe dicha divulgación por

escrito y se celebre un acuerdo de no divulgación entre el tercero y la Parte Receptora, conforme a términos aceptables para la Parte Divulgadora y sus otros proveedores. La divulgación interna de la Información Confidencial por la Parte Receptora será destinada sólo a aquellos empleados o agentes que tengan necesidad de tomar conocimiento de dicha información para cumplir con sus obligaciones. La Parte Receptora será responsable del cumplimiento de dichos empleados y agentes con las disposiciones del presente Acuerdo y, así mismo, será responsable de toda divulgación o uso erróneo por parte de los mismos.

d. En caso de incluir la Información Confidencial en otros documentos, ya sea generados en forma individual o conjunta por las Partes, estos documentos se deberán identificar como tales y la Información Confidencial se deberá considerar según los términos del presente Acuerdo.

e. La divulgación o recepción de la Información Confidencial conforme al presente Acuerdo, no obliga a las Partes a entablar acuerdos comerciales con la otra.

MEDIDAS DE PROTECCIÓN.

Las Partes convienen en que toda la Información confidencial que sea obtenida será mantenida como tal y guardada al menos con el nivel de protección y cuidando que actualmente o en el futuro establezcan los sistemas y/o políticas para la protección de información confidencial de cada una de las Partes y/o sus Subsidiarias. Cada una de las Partes reconoce y manifiesta que mantiene a la fecha dichos sistemas y/o políticas de protección de información confidencial y que estos últimos cumplen al menos con los estándares ordinarios que prevalecen en la industria.

EXCEPCIONES.

Las obligaciones de confidencialidad y uso limitado establecidas en el presente Acuerdo no se aplicarán a la información recibida conforme al presente Acuerdo en caso que:

a. Sea o pase a ser del dominio público por medios distintos de una violación del presente Acuerdo por la Parte Receptora; o

b. Ya sea de conocimiento de la Parte Receptora al momento de la divulgación, según se demuestra en la documentación por escrito de la Parte Receptora, siempre que la Parte Receptora no la haya obtenido previamente en forma directa o indirecta de manos de la Parte Divulgadora;

c. Sea legalmente recibida por la Parte Receptora de un tercero sin que medie violación del presente Acuerdo ni violación de ningún otro acuerdo entre la Parte Divulgadora y dicho tercero; o

d. Sea desarrollada en forma independiente por los empleados de la Parte Receptora que no han tenido acceso directo o indirecto a la información confidencial conforme al presente Acuerdo, ni la recibieron en forma directa o indirecta; o

e. Sea proporcionada a un tercero por la Parte Divulgadora sin que medie restricción al derecho de divulgación del tercero; o

f. Sea autorizada por escrito por la Parte Divulgadora para ser eximida de las obligaciones de confidencialidad del presente Acuerdo.

La información específica no será considerada parte de dichas excepciones meramente por estar incluida dentro de la información general que se encuentra entre las excepciones.

Si la Parte Receptora tuviese motivos para creer que podría estar legalmente obligada a divulgar información conforme al presente Acuerdo, la misma cursará notificación por escrito de inmediato a la Parte Divulgadora de modo que ésta pueda procurar una medida cautelar u otro recurso legal adecuado.

Para constancia y conformidad con las declaraciones precedentes, las Partes suscriben el presente documento.