
# UTMACH

## FACULTAD DE INGENIERÍA CIVIL

## CARRERA DE INGENIERÍA DE SISTEMAS

# SEGURIDAD EN REDES DISTRIBUIDAS DE COMPUTADORAS EN ENTORNOS EMPRESARIALES USANDO ETHICAL HACKING

SOLANO RIVAS YORDAN VINICIO
INGENIERO DE SISTEMAS

MACHALA
2022


# UTMACH

## FACULTAD DE INGENIERÍA CIVIL

## CARRERA DE INGENIERÍA DE SISTEMAS

# SEGURIDAD EN REDES DISTRIBUIDAS DE COMPUTADORAS EN ENTORNOS EMPRESARIALES USANDO ETHICAL HACKING

SOLANO RIVAS YORDAN VINICIO
INGENIERO DE SISTEMAS

MACHALA
2022


# UTMACH

## FACULTAD DE INGENIERÍA CIVIL

## CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

# SEGURIDAD EN REDES DISTRIBUIDAS DE COMPUTADORAS EN ENTORNOS EMPRESARIALES USANDO ETHICAL HACKING

SOLANO RIVAS YORDAN VINICIO
INGENIERO DE SISTEMAS

CÁRDENAS VILLAVICENCIO OSCAR EFRÉN

MACHALA, 24 DE FEBRERO DE 2022

MACHALA
2022

# SEGURIDAD EN REDES DISTRIBUIDAS DE COMPUTADORAS EN ENTORNOS EMPRESARIALES USANDO ETHICAL HACKING

INFORME DE ORIGINALIDAD

| 2% | 2% | 0% | 1% |
|---|---|---|---|
| INDICE DE SIMILITUD | FUENTES DE INTERNET | PUBLICACIONES | TRABAJOS DEL ESTUDIANTE |

FUENTES PRIMARIAS

| | | |
|---|---|---|
| 1 | scielo.sld.cu<br>Fuente de Internet | 1% |
| 2 | repository.unad.edu.co<br>Fuente de Internet | 1% |
| 3 | core.ac.uk<br>Fuente de Internet | <1% |

| | | | |
|---|---|---|---|
| Excluir citas | Activo | Excluir coincidencias | < 10 words |
| Excluir bibliografía | Activo | | |

## CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, SOLANO RIVAS YORDAN VINICIO, en calidad de autor del siguiente trabajo escrito titulado SEGURIDAD EN REDES DISTRIBUIDAS DE COMPUTADORAS EN ENTORNOS EMPRESARIALES USANDO ETHICAL HACKING, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 24 de febrero de 2022

SOLANO RIVAS YORDAN VINICIO
0705710820

## DEDICATORIA

Dedico el presente trabajo de titulación primeramente a Dios por la salud y vida brindada, a mis padres Vinicio Solano y Lourdes Rivas que han sido el pilar más importante en mi vida durante todos los años de carrera universitaria, por haberme educado e inculcado buenos valores desde que era niño hasta la actualidad, por su apoyo económica pero mucho más por su apoyo emocional para no rendirme en cada obstáculo que se ha presentado, sin nada de eso no habría podida llegar hasta donde estoy, así también dedico este trabajo a mis abuelos Felipe Rivas e Irene Rodríguez que han sido mis segundos padres y han estado conmigo siempre ayudándome con sus consejos y a mis hermanos para que esto les sirva como ejemplo a seguir en un futuro.

También al resto de familiares y amigos en general que han estado presentado durante todos estos años, que de alguna u otra forma aportaron en mi crecimiento y motivación.

**Sr. Yordan Vinicio Solano Rivas**

**AGRADECIMIENTO**

Agradecer primero a Dios por acompañarme en todo este camino con muchas bendiciones y más por las pruebas que me ha puesto para poder superarme y ser mejor profesional y mejor persona, una vez más a mis padres por ser un ejemplo a seguir y enseñarme a cómo afrontar los retos de la vida y como levantarme de las caídas.

Quiero agradecer también a mis compañeros de la 19ava. Promoción de Ingenieros de Sistemas de la Universidad Técnica de Machala, sin duda han sido la mejor compañía durante este trayecto demostrando siempre un gran compañerismo y amistad.

A la Universidad Técnica de Machala por haberme dado la oportunidad de formarme como un profesional con una educación de calidad, a todos los docentes que han sido parte en mi aprendizaje y compartir sus conocimientos sin egoísmo alguno.

Por último, agradecer a mi tutor el Ing. Oscar Cárdenas por su paciencia y generosidad durante este proceso de titulación, siempre dispuesto a ayudarme y motivarme a que sea un gran profesional y ser humano.

**RESUMEN**

La Seguridad en redes distribuidas de computadores se trata de una disciplina transversal, muchas veces con problemas en varias etapas como el desarrollo, diseño mantenimientos e implementación de las tecnologías antes mencionadas, el objetivo de la seguridad es proteger los recursos en los sistemas de una organización o empresa por ello las únicas personas que pueden tener acceso a la información son aquellas autorizadas. Las empresas están obligadas a implementar medidas de seguridad para proteger la privacidad y confidencialidad de la información que poseen o procesan y una de las actividades más comunes que usan las empresas es el pentesting o pruebas de penetración hacia su red.

Estas pruebas de penetración implican exponer uno o varios equipos de una red a un ataque informático, y detectar vulnerabilidades para desarrollar medidas que permitan prevenir estos ataques externos. Es importante observar el entorno en el que opera la empresa, como las herramientas que utiliza o la forma en que trabajan sus empleados, siendo el factor humano una de las principales razones por las que el malware se infiltra en el sistema.

Generalmente se pueden encontrar muchas vulnerabilidades en los recursos críticos de una organización, si bien la realización de pruebas de penetración requiere experiencia y conocimiento, este no es solo para grandes organizaciones con un conjunto de servidores que brindan diferentes servicios y segmentos de red que cubren cantidades de equipos computacionales, estas pruebas se pueden realizar en un equipo independiente e incluso a un equipo personal; por supuesto, no serán tan precisas como las de forma profesional, aun así, son suficientes para lo que se requiere. Las vulnerabilidades más obvias se pueden encontrar facilitando la implementación de controles y precauciones de seguridad para evitar la intrusión y el comportamiento no deseado del producto o servicio que se evalúa.

A causa de esto se implementó una red empresarial de forma virtualizada y controlada, y poner a prueba varios aspectos en su seguridad y presentar los problemas que existen generalmente en la vida real contra ataques que comúnmente son provenientes de ciber atacantes o hackers.

Una vez listo el entorno para ser utilizado se continuó con el desarrollo de las pruebas

de penetración la red desde el sistema operativo Parrot Security que viene acompañado de su suite de herramientas para auditorias y pentesting de varios tipos de entornos.

El estándar de ejecución de pruebas de penetración (PTES) está constituido de siete fases, que inicia desde unas preguntas previas que definieron al alcance del trabajo de testeo hasta la elaboración de un informe, además se añadió una fase final que costa de correcciones o medidas de seguridad hacia las vulnerabilidades que se encontraron durante el desarrollo de las pruebas.

El resultado de la evaluación dio a lugar a múltiples soluciones y medidas de seguridad posibles a ser ejecutadas para contrarrestar cada ataque realizado durante las pruebas de penetración, las cuáles son mayormente recomendadas por las grandes comunidades de profesionales en el área de la seguridad informática.

**Palabras clave:** Entorno empresarial, ciberataques, pentesting, hacking ético, vulnerabilidad, red distribuida de computadoras, seguridad.

**ABSTRACT**

Security in distributed computer networks is a transversal discipline, often with problems in various stages such as development, design, maintenance and implementation of the aforementioned technologies. The goal of security is to protect the resources in the systems of an organization or company. In addition, the only people who can have access to the information are those authorized to do so. Companies are required to implement security measures to protect the privacy and confidentiality of the information they hold and process. One of the most common activities used by companies is pentesting or penetration testing of their network.

These penetration tests involve exposing one or more computers on a network to a computer attack, and detecting vulnerabilities to develop measures to prevent these external attacks. It is important to look at the environment in which the company operates, such as the tools it uses or the way its employees work, since the human factor is one of the main reasons malwares infiltrates the system.

Many vulnerabilities can generally be found in an organization's critical resources, while performing penetration testing requires experience and knowledge, it is not just for large organizations with a set of servers providing different services and network segments covering large amounts of data. of computer equipment, these tests can be performed on an independent computer and even on a personal computer; Of course, they won't be as accurate as professional ones, but they're still good enough for what's required. The most obvious vulnerabilities can be found by making it easy to implement security controls and precautions to prevent intrusion and unwanted behavior of the product or service under test.

Because of this, a corporate network was implemented in a virtualized and controlled way, and to test various aspects of its security and present the problems that generally exist in real life against attacks that commonly come from cyber attackers or hackers.

Once the environment was ready to be used, the development of network penetration tests continued from the Parrot Security operating system, which is accompanied by its suite of tools for auditing and pentesting of various types of environments.

The Penetration Test Execution Standard (PTES) is made up of seven phases, which start from some preliminary questions that defined the scope of the testing work until

the preparation of a report, in addition, a final phase was added that costs corrections or measures of security towards the vulnerabilities that were found during the development of the tests.

The result of the evaluation gave rise to multiple solutions and possible security measures to be executed to counteract each attack carried out during the penetration tests, which are mostly recommended by the large communities of professionals in the area of computer security.

**Keywords:** Business environment, cyberattacks, pentesting, ethical hacking, vulnerability, distributed computer network, security.

**CONTENIDO**

**INDICE DE TABLAS**



**INDICE DE ILUSTRACIONES**

## INTRODUCCIÓN

Desde hace muchos años, la información ha sido la materia prima del conocimiento. En la actualidad, una organización corporativa no puede formarse sin tratamiento adecuado, desde la información externa que se debe gestionar la forma de ingresar al mercado hasta la información privilegiada para el mejor control y uso justo de todos sus propios recursos, con el objetivo de potenciarlos de manera más efectiva y eficiente. Incluye el uso justo de la información procesada en el sitio y tiempo exacto, para ello, el sistema de búsqueda y recuperación de la información es una herramienta indispensable para la implementación de cualquier actividad en la vida moderna.

Con el rápido desarrollo tecnológico de las últimas décadas, los medios actuales de acceso, la forma en que las personas adquieren conocimientos hoy en día ha cambiado drásticamente, para cualquier profesional, las tecnologías de la información y la comunicación se han convertido en un reto, pero para los encargados de la selección, regulación y también de brindar el acceso a la información a la comunidad de usuarios es más que un desafío, constituye una obligación.

Las conexiones en red han aumentado; además, las aplicaciones y el software son cada vez más fáciles de usar y accesibles, por lo que todos tienden a conectarse a la red para compartir los mismos recursos, pero esta facilidad de comunicación o conexión también aumenta los niveles de riesgos, haciendo que la información y recursos de la organización pueden verse comprometidos, por ello se requiere tomar medidas de seguridad para la protección de la información y activos de las organizaciones.

Los ciber atacantes monitorean constantemente las redes en busca de lagunas o debilidades en los sistemas de información como de entornos empresariales, se han desarrollado software para hacer que la configuración y uso sean cada vez más fáciles, por lo que las amenazas a la seguridad siempre están ocultas, usualmente los servidores o equipos de red pueden ser vulnerados con fines perjudiciales en la funcionalidad u otros aspectos de una empresa u organización.

El propósito del presente trabajo es crear un entorno empresarial que está conformado por un controlador de dominio y dos equipos conectados a el que estarán

compartiendo recursos por medio de un directorio activo, este escenario será testeado mediante diversos tipos de ataques de penetración mediante el uso de la metodología PTES, a lo que se añadirá una nueva fase que constará de las correcciones o medidas de seguridad para las vulnerabilidades que se encontrarán.

La estructura del presente trabajo se conforma de los siguientes capítulos:

**Capítulo I:** Se comenta sobre el contexto y el hecho de interés, se identifican los requisitos a cumplir, la justificación por la que se va a tratar el tema propuesto, se detallan los problemas y sus posibles soluciones.

**Capítulo II:** Este capítulo se desglosa el desarrollo del proyecto desde su definición del escenario, sus fundamentos teóricos y todo el proceso de implementación.

**Capítulo III:** Se presenta un plan de evaluación para los resultados de las pruebas de penetración realizadas en el capítulo anterior, y así seguir con las conclusiones y recomendaciones del mismo que servirán para futuros trabajos o investigaciones.

# 1. CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

## 1.1. ÁMBITO DE APLICACIÓN: DESCRIPCIÓN DEL CONTEXTO Y HECHOS DE INTERÉS.

Las organizaciones gubernamentales o las empresas enfrentan muchos desafíos cuando se trata de problemas de seguridad, son objetivos preferidos por los ciberdelincuentes que buscan grandes ganancias financieras o un impacto negativo en la confiabilidad y participación de mercado de las grandes empresas por una variedad de razones. [1]

Según [2] los ataques cibernéticos van en aumento, principalmente contra instituciones financieras en Latinoamérica, la pandemia del COVID-19 y el crecimiento de la actividad digital que ha generado han hecho aún más evidentes las vulnerabilidades del espacio digital alrededor del mundo. El informe ThreatMetrix Cybercrime identificó a esta región como un punto crítico para el fraude de creación de cuentas, que representa alrededor del 20% del volumen total en comparación con el promedio de la industria del 12,2%. Durante cada año, 1 millón de nuevos usuarios en América Latina y el Caribe se conectan a Internet por primera vez, esto a su vez, crea un nuevo conjunto de clientes que no son tan expertos en tecnología como los clientes más maduros, lo que genera un entorno de alto riesgo.

En un informe de Cybersecurity Ventures en 2017, predice que el daño producido por el ransomware le costaría al mundo $5 mil millones, frente a $325 millones en 2015, un aumento de 15 veces en tan solo 2 años, se esperaba que las pérdidas en 2018 alcancen los $8 mil millones y en 2019 a $11,5 mil millones. La predicción más reciente es que el costo global del daño ocasionado por ransomware llegaría a los $20 mil millones para 2021, siendo 57 veces más que en el año 2015, convirtiendo a este tipo de delito como el que se propaga con más rapidez. [3]

Si bien en muchos casos el problema es la implementación de sistemas de seguridad de la información contable y financiera, muchos de estos problemas no son solucionados de manera efectiva debido a que la empresa dedica gran parte de sus empleados a sus empleados para adquirir y gestionar el conocimiento. Los tipos de situaciones involucradas en sus actuaciones, y simplemente delegar esa responsabilidad o carga a los profesionales que los contratan. [4]

## 1.2. ESTABLECIMIENTO DE REQUERIMIENTOS

La seguridad de la información o ciberseguridad es el campo relacionado con la tecnología de la información que se encarga de asegurar y proteger todo lo relacionado con la infraestructura de tecnología de la información, especialmente la seguridad, privacidad y procesamiento de la información contenida en los diversos dispositivos que crea. Además, en los últimos años se ha convertido en una de las áreas más relevantes del sector tecnológico debido al aumento de los ciberataques y robos masivos de datos, que cada año provocan grandes daños tanto económicos como humanos. [5]

Las empresas se ven obligadas a anticipar diversas situaciones de riesgo de la información, debido al rápido desarrollo de la tecnología de la información, los continuos cambios tecnológicos y el rápido desarrollo de muchas transacciones comerciales, donde los dispositivos de información y las computadoras están expuestos a situaciones como ataques de piratas informáticos, usuarios del sistema, amenazas lógicas y muchos otros. Sin embargo, debido a la falta de conocimiento sobre cómo protegerlo adecuadamente o la complejidad requerida por muchos estándares internacionales y mejores prácticas en evolución, cada vez más organizaciones se niegan a protegerlo. [6]

Las empresas que prestan servicios de test de penetración en la red, no siempre sus resultados presentan que evidencien que la seguridad de la empresa no tenga ningún tipo de vulnerabilidad, por tal razón es recomendable que alguien especializado en el tema realice las pruebas de forma presencial para garantizar que los resultados sean más exactos y con ello poder recomendar a los encargados de seguridad que medidas o cambios deben realizar en su red para asegurar su información.

## 1.3. JUSTIFICACIÓN DEL REQUERIMIENTO A SATISFACER

Generalmente el área administrativa de una empresa u organización es la encargada de conseguir el objetivo que se planteen. A fin de obtenerlo, nace la importancia y necesidad de conocer diversas formas, y la Internet es la mejor y más económica manera como herramienta para una comunicación de gran proporción.

Normalmente las empresas manejan información ya sea de ámbito público como también privada la cuál debe estar protegida con tecnología y personal calificado para ello. Por lo tanto, una red empresarial al estar expuesta al Internet, su información está corriendo altos riesgos por las vulnerabilidades que Cibercriminales podrían aprovechar para penetrar ataques con la finalidad de dañar u obtener lo que deseen. [7]

Para poder ejecutar las pruebas de penetración se optó por utilizar el estándar PTES, ofreciendo la facilidad de adecuarse a cualquier tipo de empresa y sus necesidades, cubriendo con todo lo relacionado a las pruebas que se requieren realizar, desde una encuesta inicial para recopilar información y modelar las amenazas con la ayuda de la búsqueda de vulnerabilidades, explotación y post explotación hasta la elaboración de informes que capturen todo el proceso para el cliente.

Hoy en día es difícil establecer un listado de formas de ataque que realizan los hackers dentro de las organizaciones y sus infraestructuras. Con el fin de evitarlo, se debe cambiar la perspectiva de como vemos el tema de la seguridad.

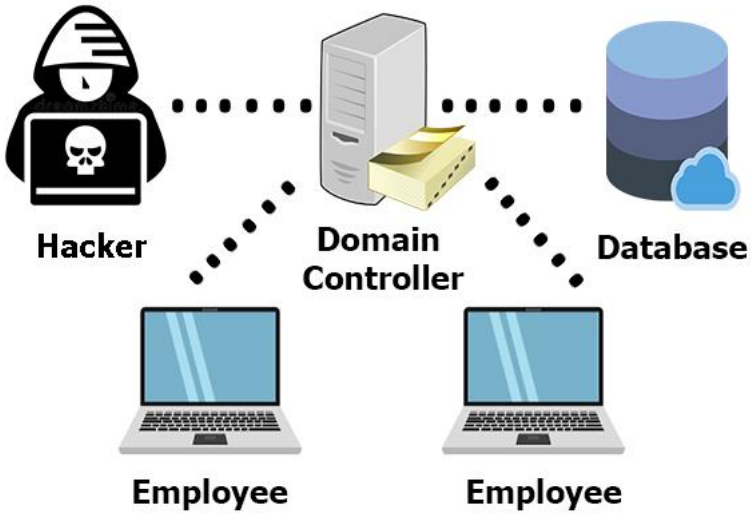
De esta manera se justifica esta propuesta para poder mantener seguras las redes distribuidas de computadores de las empresas y así disminuir los riesgos de posibles ataques, a través de la ejecución de un escenario que nos permita ejecutar diversas utilidades de hacking ético para identificar, explotar y corregir vulnerabilidades en este tipo de entornos empresariales.

# 2. CAPÍTULO II. DESARROLLO DEL PROYECTO

## 2.1. DEFINICIÓN DEL ESCENARIO BÁSICO DE UN ENTORNO EMPRESARIAL.

El escenario para este trabajo está constituido por un esquema de red distribuida de computadoras, tal como se muestra en la ilustración, donde hay un controlador de dominio (Domain Controller), el cual hace la función de servidor donde está alojada la base de datos central en la cual están conectadas todas las máquinas empleado y es la encargada de establecer las configuraciones para cada una de ellas y la información que pueden manejar.

**Ilustración 1** Escenario básico de un entorno empresarial




**Fuente:** Elaboración propia

Aquí se muestra básicamente una estructura de una red distribuida de computadoras en un entorno empresarial donde se usan configuraciones predeterminadas sin alguna forma de protección a su información, y también se logra observar a un atacante o en este caso para esta propuesta sería un pentester, el cuál ejecutará peticiones de la misma forma que lo haría un atacante y aprovechar todas las vulnerabilidades que la red en la que esté penetrando le presente y así concluir que cambios y configuraciones de seguridad hay que realizar en el entorno.

## 2.2. FUNDAMENTACIÓN TEÓRICA DEL ESCENARIO

La situación en la que todos los países del mundo han estado atravesando estos meses ha generado muchos cambios que generalmente en la sociedad eran muy cotidiano, donde ha obligado a que las personas cambiemos algunas costumbres y la tecnología se convirtió en un factor determinante para la interacción personal y también laboral.

### 2.2.1. Hackers

Según [8] es un personaje nacido con la llegada de la cibernética, la tecnología digital e Internet. Esta es una imagen común que se ha naturalizado en los medios.

Sin embargo [9], si definimos qué es un hacker, podemos encontrar referencias en la historia humana que se ajustan al concepto, aunque no se llamen así. De hecho, estamos hablando de una actitud política ante la vida.

El objetivo de los ciberdelincuentes es diagnosticar el valor de los activos de datos en una organización, por lo tanto, los procedimientos deben organizarse e instituirse para los programas de gestión de esa protección y análisis de riesgos.[10]

### 2.2.2. Ciberataques

Los ciberataques tienen elementos comunes necesarios: recopilación de información estratégica, personalización, debilitamiento del despliegue técnico y manipulación selectiva de equipos e información informática. [11]

Podemos definir el cibercrimen como acciones actos ilegales, aprovechando la revolución tecnológica para penetrar las defensas del sistema informático, provocando delitos potenciales de naturaleza delictiva. Afectando la privacidad, los recursos e incluso la actividad del usuario. [12]

### 2.2.3. Ciberespacio

El uso generalizado de Internet junto con la cantidad y el valor de los datos y la información disponibles lo han convertido en un espacio propicio para el desarrollo de nuevas formas delictivas que van más allá del concepto tradicional de derecho penal y desafían sus límites. La reciente pandemia ilustra tanto el potencial como los desafíos que plantea el ciberespacio en términos de seguridad. [13]

### 2.2.4. Redes distribuidas de computadores

Una red de computadoras distribuida se puede definir como un grupo de computadoras interconectadas que comparten diferentes recursos. Este tipo de red implica una conexión entre dispositivos a través de dispositivos específicos que permiten a los portadores de datos enviar y recibir los datos que desean compartir. Así, en una red informática, hay un emisor y un receptor que intercambian mensajes.[14]

Todos estos sistemas interconectados permiten a las empresas u organizaciones aumentar la eficiencia de sus procesos internos y externos para intercambiar información de forma rápida y segura entre sus departamentos. [15]

### 2.2.5. Seguridad de la información

La mayoría de las empresas hoy en día ofrecen servicios en línea a sus clientes, un proceso que conduce a la recopilación de información que debe estar siempre disponible y segura para los usuarios. [16]

Por eso se esfuerzan por tomar decisiones que conduzcan a la integridad de los clientes con su información, y la mayoría de las empresas ahora buscan asesoría experta en seguridad y crean mecanismos de protección para protegerse de cualquier ataque que intente violar la política de información. [17]

Las organizaciones son vulnerables a la piratería de su información, lo que afecta su productividad, enfrentar las demandas de nuevas competencias que permitan la creación de nuevas oportunidades para el beneficio empresarial. [18]

Las principales causas de estos problemas son: hacks, malware, errores de software e inicios de sesión.

### 2.2.6. Ethical Hacking

Es una rama de la seguridad tecnológica que previene, elimina, instala y combate vulnerabilidades de software o hardware. Para ello, debe tener los conocimientos necesarios de redes, administración de servidores y servicios correspondientes, que se tratarán más adelante. La piratería ética es cuando alguien usa sus habilidades informáticas para encontrar errores, lagunas o debilidades. [19]

El objetivo del hacking ético es mejorar la seguridad de la red o del sistema

abordando las vulnerabilidades que aparecen durante el proceso de investigación. Además, las personas que realizan estos estudios utilizan los mismos métodos y herramientas que utilizaron los atacantes reales. [20]

A través de este conjunto de tecnologías es posible determinar el nivel de seguridad que tienen las empresas tanto dentro como fuera de su red por lo que se crea el escenario a través de los mecanismos de la red corporativa y cómo la explotan los ciberdelincuentes. [21]

### 2.2.7. Pentesting

Las empresas necesitan saber el impacto económico que tendrán cuando uno de estos riesgos de TI se acerque, para que puedan capacitarse internamente con el departamento [22]. En toda la infraestructura tecnológica y en general en el entorno de TI, estas pruebas pueden también llevarse a cabo con empresas externas altamente calificadas y empleados experimentados, y a través de estas pruebas esperamos que las empresas hagan una evaluación conjunta y comiencen a priorizar sus objetivos comerciales, y esta evaluación es para resumirlos en los informes de investigación de bajo riesgo y alto riesgo. vulnerabilidades y otras vulnerabilidades que pueden conducir a la explotación por parte de atacantes, tanto externos como internos.[23]

Estas pruebas que se realizan sobre la infraestructura o sobre el entorno de TI se conocen como pruebas de aplastamiento o pruebas de penetración, donde las empresas tienen que conocer sus fallas de seguridad y las consecuencias, además gracias a la aplicación las empresas podrán reducir los riesgos y cómo priorizarlos y cómo tener los controles pertinentes. [24]

Para las actividades y criterios de Pentest, se deben considerar algunas cuestiones, ejemplos, implicaciones legales y tipos de información se accede. A retos abordados en la propuesta de modelado y simulación del ciberespacio. [25]

En la actualidad existen nuevos mecanismos que aseguran información de una forma más eficiente, la conexión de procesos de intercambio de información a través de la red dan iniciativa a el mejoramiento de la seguridad ante ciberataques, dentro de este contexto interviene el tema que se propone dentro de la cuarta revolución industrial como el Blockchain, este tipo de tecnología es capaz de mejorar significativamente los niveles de seguridad en un proceso de intercambio

de información mediante la creación de cadenas de bloques que contienen información específica. [26]

Hay diferentes tipos de pentesting que se determinan según las necesidades del cliente y estas son:

**Tabla 1.** Tipos de pentesting

| | |
|---|---|
| **Caja blanca** | El más completo, el cual se deberá de proporcionar información al pentester sobre la infraestructura de la red. |
| **Caja gris** | En este tipo de testeo el especialista trabaja solo con una información parcial sobre la infraestructura de la red. |
| **Caja negra** | Se acerca más a una prueba simulada, y no se dispone de información sobre la red. |

**Fuente:** [27]

Estos tipos de testeo se determinan según las condiciones que el cliente establezca, mientras menos información se tenga del sistema o red a testear más dificultad tiene el pentester realizar las prueba y el esfuerzo deberá aumentar para así poder lograr el objetivo.

### 2.2.8. Metodología PTES

El Estándar para la Ejecución de Pruebas de Penetración o PTES (Penetration Testing Execution Standard), es un proyecto constituido por diversas organizaciones y empresas. Incluye todo lo relacionado con las pruebas de penetración, desde unas preguntas previas hasta las etapas de recopilación de información y modelado de amenazas en las que los profesionales hacen su trabajo.

Está compuesto por siete fases. [28]

**Tabla 2.** Fases de la metodología PTES

| | |
|---|---|
| **Preacuerdo** | Se define el alcance y los objetivos de la prueba de penetración. |
| **Recopilación de inteligencia** | Se realiza la recolección de información de inteligencia desde fuentes abiertas. |
| **Modelado de amenazas** | Se enuncian las posibles estrategias de penetración. |
| **Análisis de vulnerabilidades** | Se descubren vulnerabilidades que puedan ser explotadas. |
| **Explotación** | Se intentan explotar las vulnerabilidades descubiertas. |
| **Post-explotación** | Los especialistas de seguridad pueden continuar escalando el proceso de explotación. |
| **Reporte** | Se comunica al cliente la información que le permita solucionar las vulnerabilidades encontradas. |

**Fuente:** [28]

## 2.3. OBJETIVOS DEL ESCENARIO

### 2.3.1. Objetivo Principal

Elaborar un escenario de un entorno empresarial mediante un software de virtualización haciendo uso de herramientas de ethical hacking para la ejecución de ataques y corrección de vulnerabilidades empleando el estándar de ejecución de pruebas de penetración.

### 2.3.2. Objetivos Específicos

- Realizar el proceso de instalación y configuración de un entorno empresarial en el software de virtualización VMWare WorkStation.
- Implementación del Parrot OS para su posterior uso de herramientas de ciberseguridad y pentesting.
- Ejecutar los diferentes ataques y pruebas de penetración en las máquinas de la red del entorno mediante las fases que ofrece la metodología PTES para su posteriores correcciones o medidas de seguridad.

## 2.4. DISEÑO DEL ESCENARIO PARA LAS PRUEBAS

El escenario está distribuido por 3 máquinas virtuales, 2 que conformaran parte de la simulación de un entorno empresarial de la vida real, y la máquina sobrante es la que tendrá instalado el Parrot OS que permitirá realizar todas las pruebas de penetración y ataques que comúnmente los cibercriminales ejecutan en redes empresariales.

Iniciando con un equipo que sirve de Domain Controller (DC) y su servicio de Active Directory que gestiona los recursos compartidos en la red de forma centralizada con las demás maquinas conectadas en la red, y más importante aún es la que manejará las credenciales de cada usuario.

Los dos equipos restantes representan a usuarios de la red compartida, conectadas al equipo controlador de dominio, previamente configuradas con sus IPv4, y dirección del DNS, para lograr una conexión exitosa y lograr el funcionamiento del escenario.

### 2.4.1. Virtualización

La virtualización crea un entorno informático virtual o simulado en lugar de uno físico. Esto generalmente incluye versiones de hardware, sistemas operativos, dispositivos de almacenamiento y más. Nacido de la computadora [29].

Esto permite a las organizaciones dividir una sola computadora o servidor físico en varias máquinas virtuales. Cada máquina virtual puede interactuar de forma independiente y ejecutar diferentes sistemas operativos o aplicaciones compartiendo los recursos de un único servidor. [30]

El escenario presentado se realiza en el software de virtualización VMWare WorkStation porque permite a los usuarios ejecutar múltiples sistemas operativos, incluidos Linux, Windows, etc., como máquinas virtuales en una sola PC. Los usuarios pueden clonar entornos de servidor, escritorio y tableta en una sola máquina virtual, para ejecutar aplicaciones simultáneamente en múltiples sistemas operativos sin reiniciar. La estación de trabajo también proporciona un entorno seguro y aislado para evaluar nuevos sistemas operativos como Windows 10 y para probar aplicaciones de software, parches y arquitecturas de referencia. [31]

### 2.4.2. Sistema Operativo

#### 2.4.2.1. Windows Server 2016

Desarrollado por Microsoft, pertenece al grupo de sistemas operativos de clase empresarial diseñados para brindar y compartir servicios entre usuarios, así como administrar completamente el almacenamiento de datos, aplicaciones y redes.

#### 2.4.2.2. Parrot OS

Basada en Debian, esta distribución GNU/Linux fue diseñada para el tema de seguridad y de la privacidad, cuenta con herramientas que dispone de un laboratorio con todo tipo de utilidades de ciberseguridad, partiendo del pentesting, y todo tipo de análisis. [32]

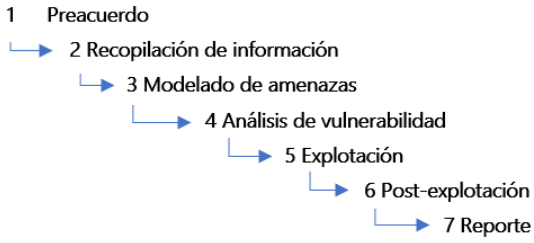
Ofreciendo un arsenal completo de herramientas para la seguridad que se pueden implementar en cualquier dispositivo e incluso en la nube, es un sistema seguro y listo para usarlo en la web para comunicaciones privadas. Con una infraestructura resistente y bien distribuida con CDN dedicados, espejos y puertas de enlace IPFS/PSP permitiendo el acceso a software o información a personas o países donde la conexión a Internet no es estable. [32]

### 2.4.3. Active Directory

Lo que puede hacer este Active Directory es proporcionar un servicio en uno o más servidores que pueden crear objetos como usuarios, computadoras o grupos para administrar la información de inicio de sesión para las computadoras conectadas con la red. Pero esto no es solo porque sí, ya que también podemos administrar todas las políticas de red que utiliza este servidor. [33]

### 2.4.4. Fases de la metodología PTES

**Ilustración 2** Fases de la metodología PTES




**Fuente:** Elaboración Propia

#### 2.4.4.1. Preacuerdo

Según [34] el objetivo de esta sección del PTES es presentar y explicar las herramientas y técnicas disponibles que ayudan en un paso exitoso previo al compromiso de una prueba de penetración. La información dentro de esta sección es el resultado de los muchos años de experiencia combinada de algunos de los probadores de penetración más exitosos del mundo.

Aquí se establecen preguntas puntuales hacia el cliente y establecer los puntos importantes a trabajar con las pruebas de penetración a la red.

Estas preguntas se pueden clasificar dependiendo del tipo de prueba de penetración.

- Pruebas de penetración de red.
- Pruebas de penetración de red inalámbrica
- Pruebas de penetración física.
- Ingeniería social.

Evidentemente para este trabajo se aplicarán las que están direccionadas para pruebas de penetración de red.

1. ¿Por qué se realiza al cliente la prueba de penetración contra su entorno?
2. ¿Se requiere la prueba de penetración para un requisito de cumplimiento específico?
3. ¿Cuándo desea el cliente las partes activas (escaneo, enumeración, explotación, etc.) de la prueba de penetración realizada?
4. ¿Cuántas direcciones IP totales se están probando?
5. ¿Existen dispositivos que puedan afectar los resultados de una prueba de penetración, como un firewall, un sistema de detección/prevención de intrusiones, un firewall de aplicaciones web o un equilibrador de carga?
6. En el caso de que se penetre en un sistema, ¿cómo debe proceder el equipo de pruebas?

#### 2.4.4.2. Recopilación de información

La recopilación de inteligencia implica realizar un reconocimiento de un objetivo para recopilar la mayor cantidad de información posible para penetrar en un objetivo durante la fase de evaluación de explotación y vulnerabilidad. Cuanta más

información recopile durante esta etapa, más vectores de ataque podrá utilizar en el futuro. [35]

#### 2.4.4.3. Modelado de amenazas

El estándar no utiliza un modelo específico, sino que requiere que el modelo utilizado sea consistente en términos de representación de amenazas, capacidades y clasificaciones según la organización que se examina y la capacidad para aplicarlas. Usado varias veces para futuras pruebas con los mismos resultados. [36]

El estándar se centra en dos componentes básicos del modelo de amenazas tradicional: el origen y el atacante (actor de amenazas/comunidad). Cada uno se divide en recursos comerciales, procesos comerciales, comunidades de amenazas y capacidades asociadas, respectivamente. [36]

#### 2.4.4.4. Análisis de vulnerabilidad

- **Ensayos**

Descubrir vulnerabilidades en sistemas y aplicaciones que los atacantes pueden explotar, que pueden ser el resultado de configuraciones deficientes de servidores y servicios o un diseño deficiente de la aplicación. [37]

- **Activo**

Estas pruebas requieren una interacción directa con el componente que se utiliza para detectar cualquier vulnerabilidad. Pueden ser componentes de bajo nivel, como la pila TCP en un dispositivo de red, o pueden ser componentes de nivel superior en la pila, como una interfaz web utilizada para administrar el dispositivo.[37]

- **Pasivo**

Implica analizar metadatos, como documentos de Microsoft Office, que realizarán acciones como enumerar el autor, la empresa o la última vez que se guardó el documento. Estos metadatos se encuentran comúnmente en las redes corporativas, pero se debe tener cuidado antes de publicar esta información.[37]

#### 2.4.4.5. Explotación

Esta etapa sirve para definir el acceso al sistema o sus recursos, evitar sus

limitaciones y luego definir un punto de entrada para lograr metas de alto valor. El principal objetivo es tener cuidado al realizar un ataque al objetivo, cualquier error o alarma pondrá en peligro el éxito de la auditoría. [38]

#### 2.4.4.6. Post-explotación

Las actividades realizadas en esta etapa se centran en recopilar todas las pruebas de abandono del sistema comprometido y mantener el acceso para que persista en el entorno, de modo que se pueda seguir recopilando información o se pueda proporcionar alguna forma de seguimiento. [39]

#### 2.4.4.7. Reporte

La etapa final de esta metodología establece que se deben mantener registros de todos los resultados obtenidos después de todo el proceso de prueba de penetración y la información obtenida.

En general, para la elaboración de este tipo de informes, se recomienda utilizar un mapa de riesgos que contenga el valor que vendrá determinado por la métrica y de esta forma poder crear un informe con todos los resultados y conclusiones.

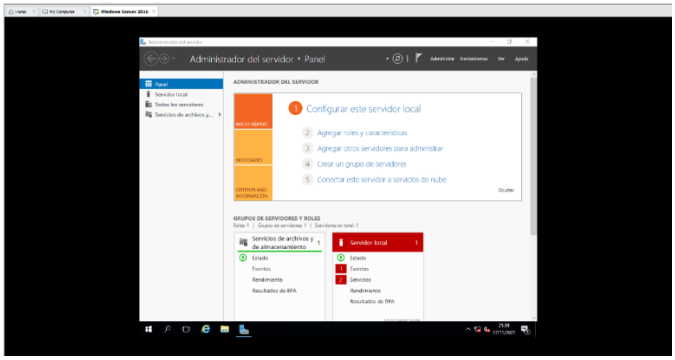
## 2.5. EJECUCIÓN Y/O IMPLEMENTACIÓN DEL ESCENARIO.

### 2.5.1. Creación de máquinas virtuales

Para iniciar el escenario se crea las máquinas virtuales necesarias cada una con su respectivo sistema operativo, las mismas que tomarán el rol que les corresponde en este entorno empresarial controlado.

Empezando por la máquina que tendrá el rol de controlador de dominios (Domain Controller), que soportará el sistema operativo Windows Server versión 2016.

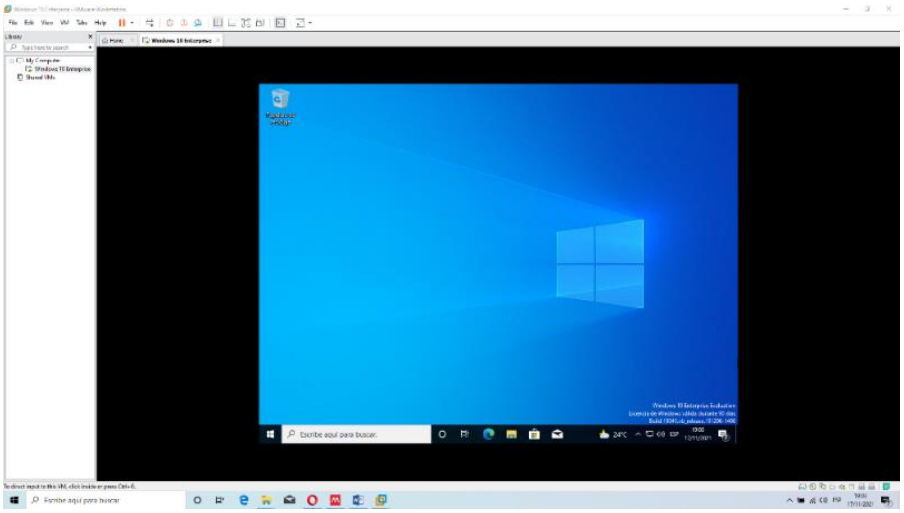
**Ilustración 3** Escritorio de Windows Server 2016




**Fuente:** Elaboración Propia

Continua con la creación e instalación de la máquina que servirá de usuario empleado dentro del entorno empresarial. Este soportará el sistema operativo Windows 10 Enterprise.

**Ilustración 4** Escritorio Windows 10 Enterprise

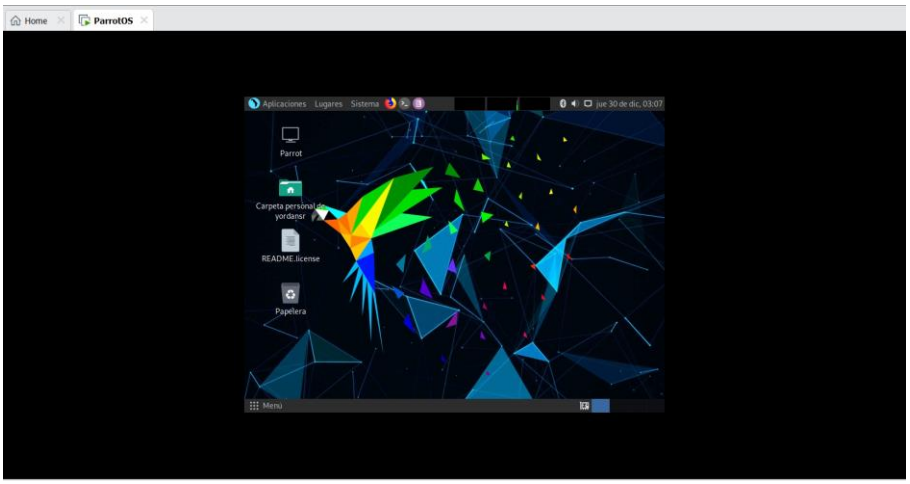


**Fuente:** Elaboración Propia

Representando a las máquinas que son usuarios “empleados” dentro de un entorno empresarial, está conectada a grupo de trabajo la cuál es gestionada por la máquina Domain Controller para tener acceso a los recursos de la red a los cuáles tenga compartido.

Y por último la creación de la máquina que soportará el Parrot OS, que es de donde se logró llevar a cabo todas los ataques y pruebas de penetración hacia el entorno creado.

**Ilustración 5** Escritorio del Parrot OS




**Fuente:** Elaboración Propia

### 2.5.2. Designación de contraseñas

Tanto como la máquina DC y las máquinas “empleados” se les asignó contraseñas.

**Ilustración 6** Contraseñas de las máquinas del escenario

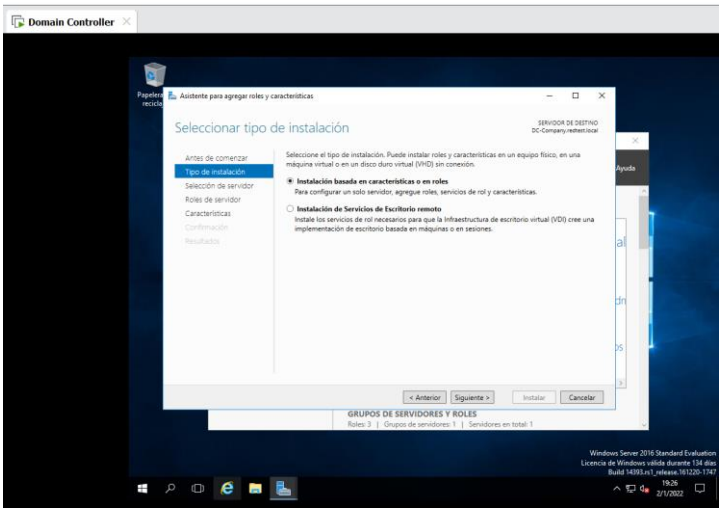
Administrador – P@$$w0rd!
PC-Juan – Password1
PC-María – Password2

**Fuente:** Elaboración Propia

### 2.5.3. Configuración del Domain Controller

Mediante el asistente para configuración de Servicios de dominio de Active Directory se realizaron las debidas instalaciones de servicios y configuraciones para que esta máquina trabaje como con Administrador del Servidor

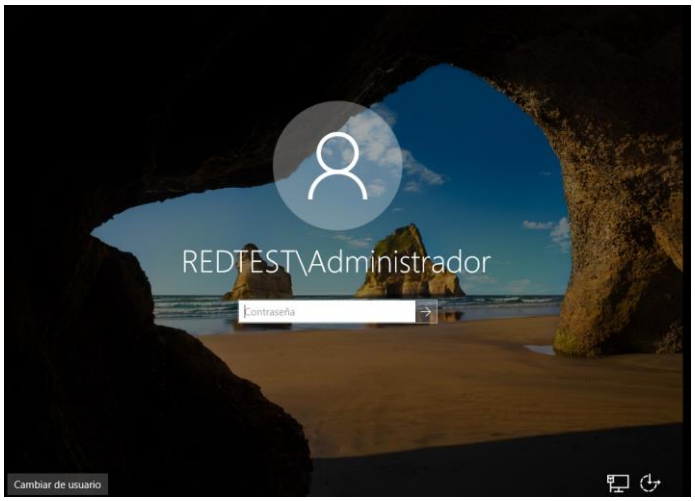
**Ilustración 7** Configuración del Domain Controller




**Fuente:** Elaboración Propia

Luego de haber finalizado con las configuraciones, la máquina pidió reiniciarse para guardar todos los cambios efectuados, y al volver a iniciar solicitó una autentificación a nivel de Administrador del Dominio.

**Ilustración 8** Autentificación en el Domain Controller

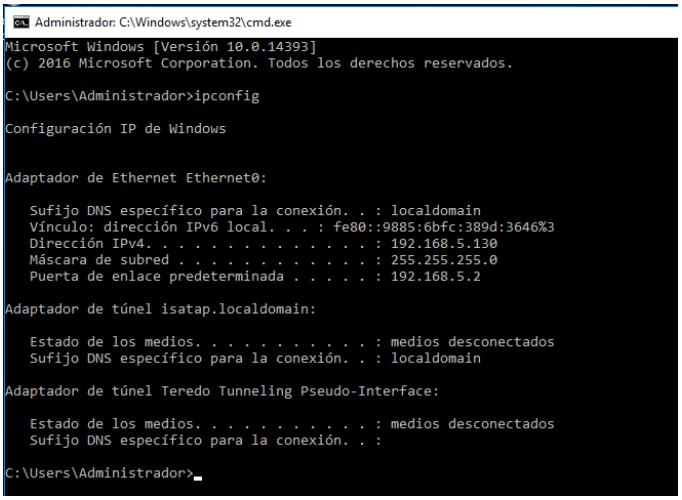



**Fuente:** Elaboración Propia

### 2.5.4. Conexión de usuarios a la red empresarial de trabajo

Para realizar este paso debemos revisar la dirección ipv4 que tiene configurado por defecto la máquina servidor, para poder configurarlos en las máquinas empleados. Para eso ejecutamos el comando ipconfig en el cmd de la máquina Servidor.

**Ilustración 9** Comando ipconfig

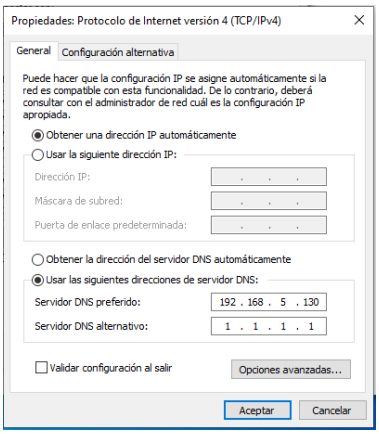



**Fuente:** Elaboración Propia

Ya teniendo la dirección ipv4 del servidor se procedió a crear un grupo de trabajo y poder conectar las dos máquinas “empleados” al dominio.

Primero se configuró la dirección del DNS en cada máquina “empleado” para que así pueda hacer conexión con el servidor.

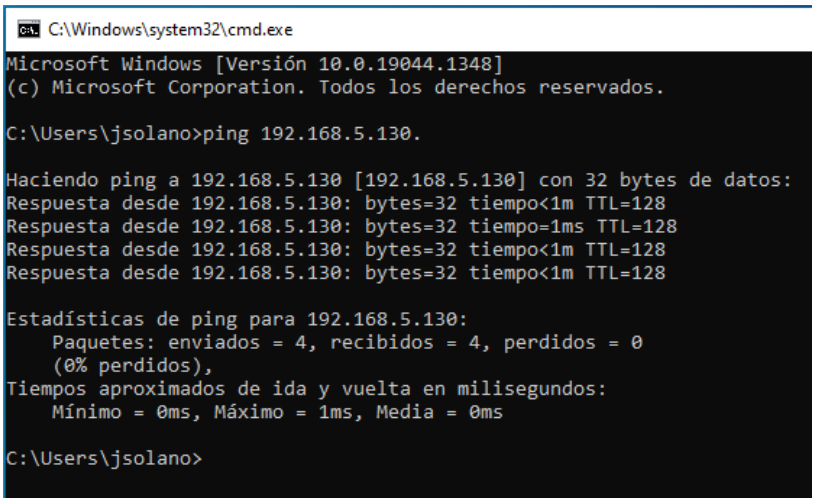
**Ilustración 10** Dirección del servidor DNS




**Fuente:** Elaboración Propia

Se ejecutó el comando ping hacia la dirección ipv4 del servidor y comprobar que exista conexión.

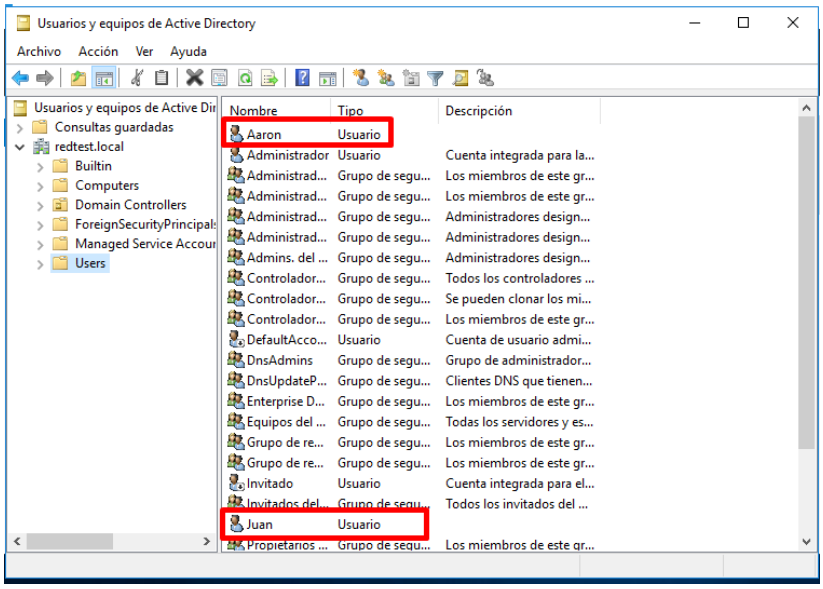
**Ilustración 11** Ping de empleado a servidor




**Fuente:** Elaboración Propia

En este punto las máquinas “empleados” están listas para ser conectadas al dominio, para esto desde el DC crear unos usuarios a nivel de directorio activo (Active Directory), los usuarios serán los mismos que están haciendo el papel de empleados.

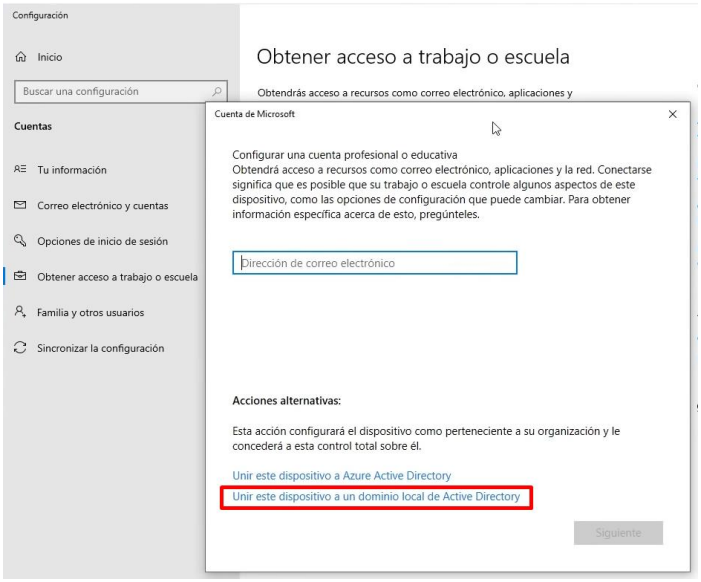
**Ilustración 12** Creación de usuarios de Active Directory




**Fuente:** Elaboración Propia

Luego para que los equipos formen parte del dominio, desde los equipos “empleados” ir a trabajo o escuela y unirse a un dominio local de active directory.

**Ilustración 13** Acceso a trabajo o escuela

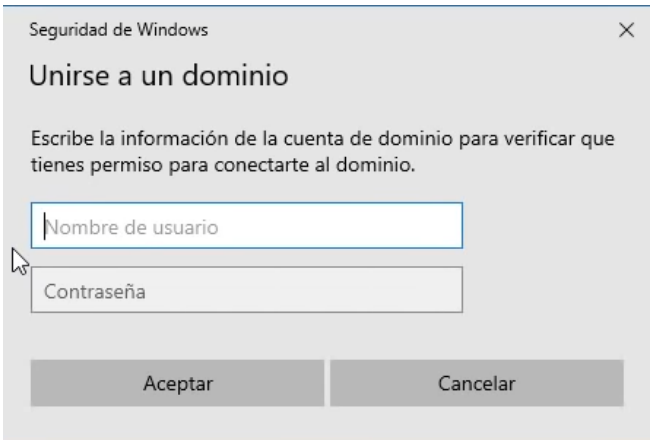



**Fuente:** Elaboración Propia

Allí pedió introducir el nombre del dominio al cuál desean conectarse el cual se le ha denominado previamente como “redtest.local”.

Se visualizó un cuadro de texto pidiendo ya una autentificación a nivel de dominio de la siguiente manera:

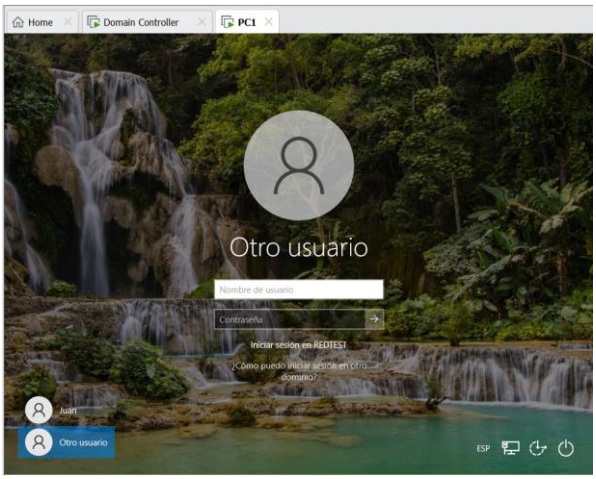
**Ilustración 14** Autentificación a nivel dominio




**Fuente:** Elaboración Propia

Posteriormente la máquina se reinició y permitió un inicio de sesión a nivel de dominio, todo el proceso que se realizó en los pasos anteriores se realizó para la otra máquina “empleado”.

**Ilustración 15** Autentificación al iniciar sesión




**Fuente:** Elaboración Propia

Con todo esto ya estuvo listo el escenario del entorno empresarial y poder ir al siguiente pasó del trabajo que es usar herramientas de hacking ético y ejecutar los diferentes ataques de penetración a esta red como generalmente los atacantes lo hacen en la vida real.

### 2.5.5. Prueba de penetración: Preacuerdo

**1. ¿Por qué se realiza al cliente la prueba de penetración en su entorno?**

Para poner a prueba la red empresarial y así encontrar vulnerabilidades que los atacar podrían explotar al encontrarlas.

**2. ¿Se requiere la prueba de penetración para un requisito de cumplimiento específico?**

Para este trabajo sí, porque se ejecutarán diferentes tipos de ataques y pruebas de penetración para poner a prueba la red empresarial creada.

**3. ¿Cuándo quiere el cliente que se realicen las partes activas (escaneo, enumeración, explotación, etc.) de la prueba de penetración?**

Durante todo el proceso de desarrollo del trabajo de titulación.

**4. ¿Cuántas direcciones IP en total se están probando?**

En total 3, la del servidor y dos equipos empleados.

**5. ¿Existe algún dispositivo que pueda afectar los resultados de una prueba de penetración, como un firewall, un sistema de detección / prevención de intrusiones, un firewall de aplicaciones web o un equilibrador de carga?**

Para este caso no, ya que el escenario está inicialmente configurado como se configura en la vida real cuando no se toman las medidas apropiadas en cuanto a la seguridad de la red empresarial.

Es por ello que se ejecutarán diversos ataques con el fin de exponer las vulnerabilidades y así poder hacer los debidos cambios y medidas de seguridad.

**6. En el caso de que un sistema sea penetrado, ¿cómo debe proceder el equipo de pruebas?**

**1. ¿Realizar una evaluación de vulnerabilidad local en la máquina comprometida?**

Sí.

**2. ¿Intentó obtener los privilegios más altos (root en máquinas Unix, SYSTEM o Administrador en máquinas Windows) en la máquina comprometida?**

Sí.

**3. ¿Realizar ataques de contraseña mínimos, mínimos, de diccionario o exhaustivos contra los hashes de contraseñas locales obtenidos (por ejemplo, / etc / shadow en máquinas Unix)?**

Sí, en este caso son máquinas con Windows SO.

### 2.5.6. Prueba de penetración: Recolección de Información

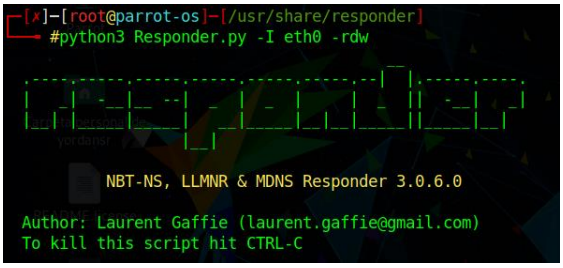
#### 2.5.6.1. Ataque SMB Relay por IPv4

Este tipo de ataque se realiza para acceder al equipo comprometido, lo que hace es conseguir la conexión del servidor al usuario entre los puertos que se utilizan para intercambiar paquetes y mediante este intercambio se obtienen las credenciales de acceso al servidor[40]

Generalmente las empresas usan una configuración por defecto que hace que la samba no esté firmada, esto quiere decir que cuando haya una comunicación los hashes no coincidirán, lo que hace la firma es que se confirmen las identidades tanto del remitente como del receptor.

Para empezar, usaremos un smb relay típico, y desde la máquina que soporte el Parrot OS, se usó una herramienta llamada Responder.py, él cual es un envenenador de tráfico que responde a consultas dando su propia dirección IP para cualquier nombre de host que hayan solicitado.

**Ilustración 16** Ejecución del Responder.py

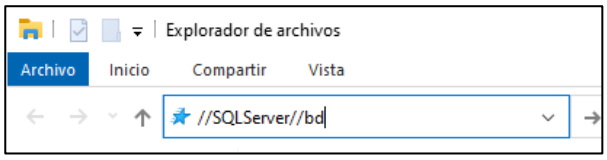



**Fuente:** Elaboración Propia

Cabe mencionar que el Responder.py captura datos (credenciales, ip, hashes) a solicitudes sobre recursos de red compartidos no existentes**.**

Entonces desde el equipo con el usuario “jsolano”, se intenta acceder a un recurso compartido no existente.

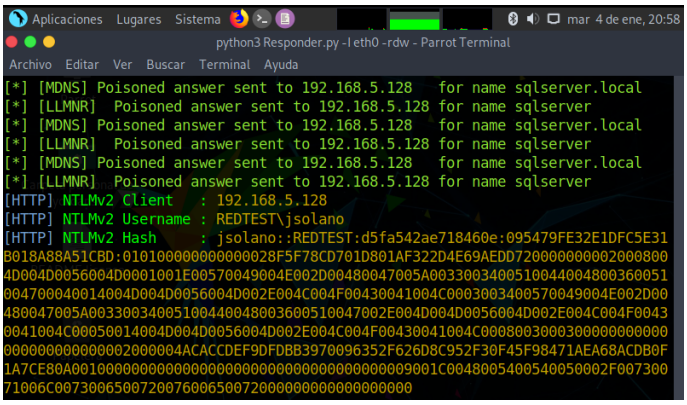
**Ilustración 17** Solicitud a recurso no existente




**Fuente:** Elaboración Propia

Al solicitar ese recurso no existente, el Responder.py automáticamente se autentifica contra el equipo solicitante y capturará los datos como se podrá ver a continuación:

**Ilustración 18** Captura de datos por el Responder.py




**Fuente:** Elaboración Propia

Como se puede apreciar el envenador capturó inmediatamente datos del solicitante como: la dirección ipv4, el username del equipo, y el hash NTLMv2.

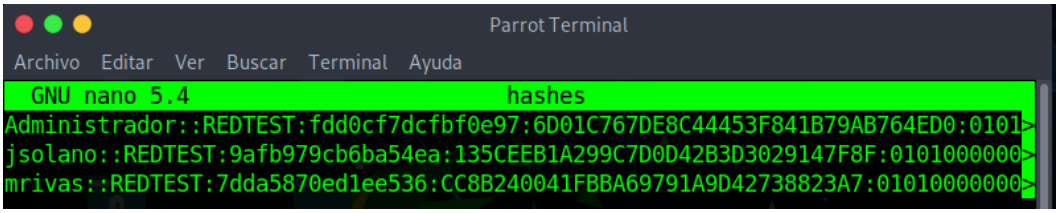
Estos datos o credenciales capturados, no sirven para hacer un Pass the hash, pero sí sirven para luego tratar de crackearlo de forma offline.

### 2.5.7. Prueba de penetración: Modelado de Amenazas

Una vez de haber conseguido estos datos, lo que se realizó es ejecutar una herramienta que pueda hacer uso de estos hashes y así intentar desencriptarlos a texto plano si es que las contraseñas son débiles.

Para eso se copió los datos capturados, y se almacenó en un archivo nuevo que será llamado ‘hashes’, que luego de escribir la siguiente línea devolvió las contraseñas de los equipos que se obtuvo gracias al envenenador de tráfico Responder.py.

**Ilustración 19** Archivo Hashes



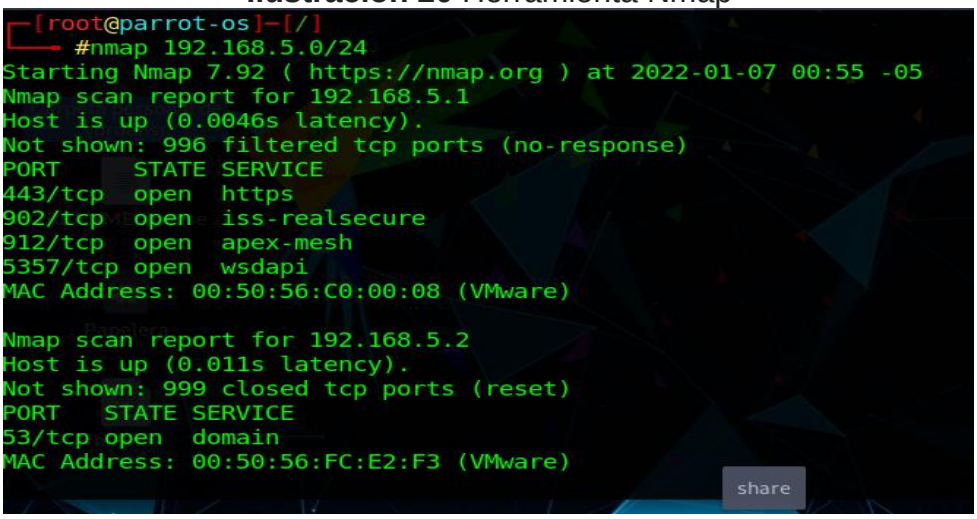

**Fuente:** Elaboración Propia

### 2.5.8. Prueba de penetración: Análisis de vulnerabilidades

Una herramienta que se puede usar en esta fase es el nmap que realizar un escaneo en una red o en puertos, como también que hosts están o no levantados, es una utilidad completamente gratis y opensource. [41]

De esta forma se puede ver los hosts en una red local y ver cuales están conectados en ese momento a internet o localmente. Se puede saber qué servicios están siendo usados en dichos hosts y también los estados de los puertos.

**Ilustración 20** Herramienta Nmap




**Fuente:** Elaboración Propia

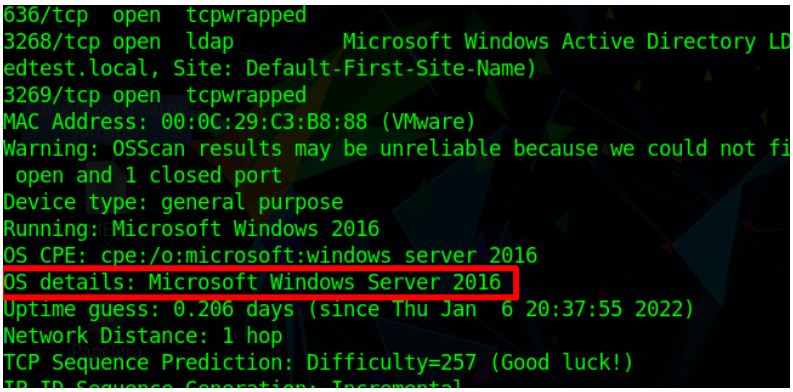
Otra cosa más que se puede realizar gracias a esta herramienta es detectar que sistema operativo están usando algún host en específico y también obtener mucha más información detallada del host usando el siguiente comando: nmpa -A -v *ip del host*.

**Ilustración 21** Nmap sobre DC


**Fuente:** Elaboración Propia

Como se puede apreciar en la siguiente ilustración se obtiene información del sistema operativo que usa el host, y más información como el nombre de equipo, grupos a los que pertenece, dirección mac, puertos y servicios que está usando, dominio al que pertenece, etc.

**Ilustración 22** Sistema operativo del host DC




**Fuente:** Elaboración Propia

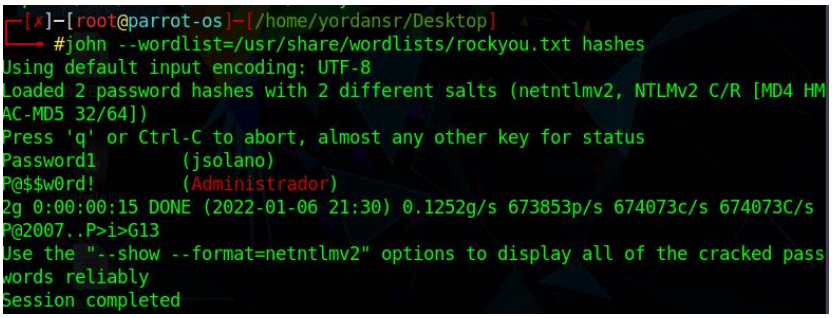
### 2.5.9. Prueba de penetración: Explotación

#### 2.5.9.1. John the Ripper

Es una herramienta de recuperación de contraseñas de código abierto que se pueden usar en diferentes sistemas operativos, admitiendo cientos de cifrados y hash. Desencripta contraseñas por fuerza bruta, estas deben ser de acceso débil, también puede ser usada en ocasiones donde el usuario haya olvidado la contraseña. [42]

Entonces con el archivo “hashes” previamente creado que contiene los hashes y usuarios capturados se procedió a ejecutar la siguiente línea con la herramienta john.

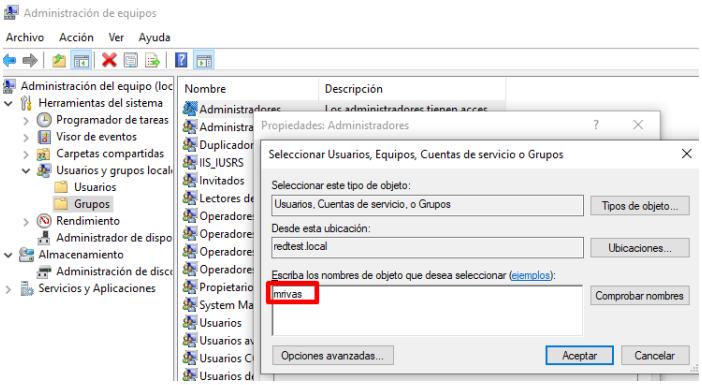
**Ilustración 23** Crackeado de contraseñas




**Fuente:** Elaboración Propia

Hay ocasiones donde existen equipos que tienen privilegios sobre otros, y simular un escenario así, se realizó la siguiente acción: desde el equipo PC-Juan ir a Administrador de Equipos, y clonar al equipo DC y poner al equipo PC-María con privilegios sobre este equipo.

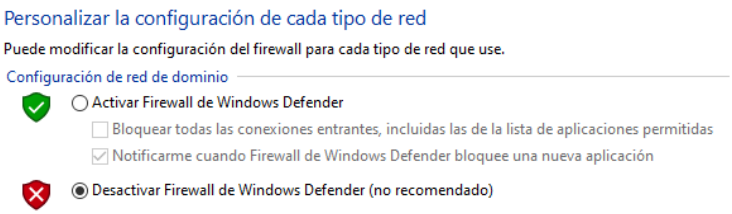
**Ilustración 24** Otorgando privilegios a un equipo




**Fuente:** Elaboración Propia

Previamente se revisó el estado del Firewall de Windows Defender, para proceder a ejecutar el siguiente ataque o herramienta de post explotación.

**Ilustración 25** Firewall de Windows Defender




**Fuente:** Elaboración Propia

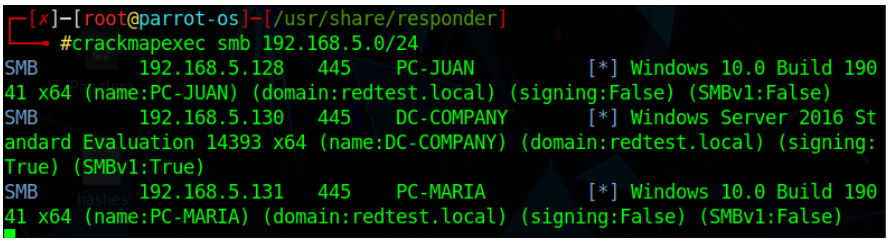
### 2.5.9.2. Crackmapecex

Es una herramienta muy conocida, escrita en Python, fue diseñada para la explotación en entornos con Windows, cuya función principal es realizar movimientos de forma lateral en una red obteniendo credenciales. [43]

Puede usar 5 diferentes protocolos como: smb, winrm, ssh, mssql o http.

Entonces usando crackmapexec bajo el protocolo samba en el segmento de red que está usando el entorno empresarial simulado se ejecutó la siguiente línea.

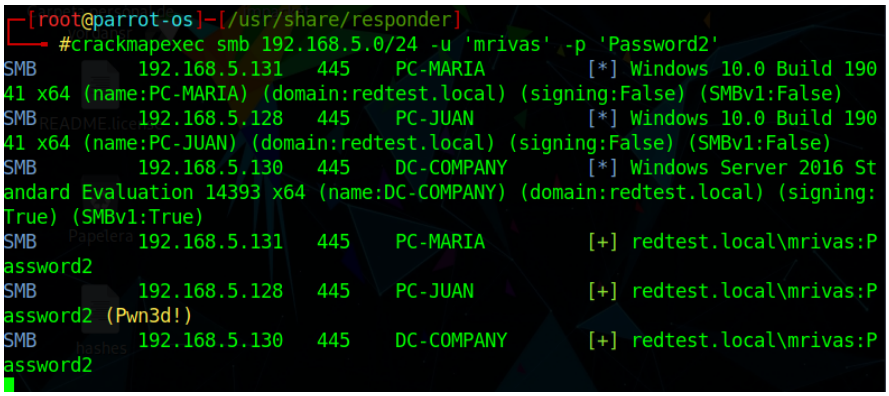
**Ilustración 26** Ejecución del crackmapexec




**Fuente:** Elaboración Propia

Ahora también se realizó un password spraying, un ataque típico donde sabiendo la contraseña de un determinado equipo se puede acceder a dicho equipo o a servicios, y gracias a esto se puede apreciar que en el equipo PC-Juan marcará con (Pwn3d!) porque el equipo PC-María es privilegiado sobre este.

**Ilustración 27** Crackmapexec con equipo privilegiado




**Fuente:** Elaboración Propia

### 2.5.10. Prueba de penetración: Post-explotación

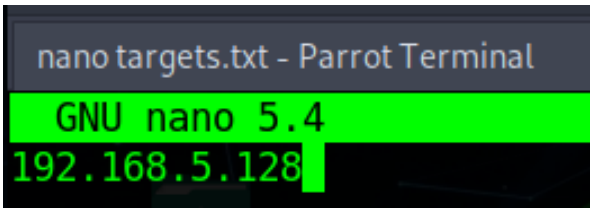
#### 2.5.10.1. NTLM Relay

Es una técnica que realiza acciones en un servidor mientras finge ser un cliente, se la puede usar para tomar el control de algún dominio de directorio activo sin necesidad de tener credenciales, se basa en la autentificación NTLM, un protocolo que sirve para autenticar un cliente en un servidor. [44]

Se continuó con los ataques smb relay, y se cambió la configuración del archivo responder.conf cambiando los valores de smb y http de on a off.

Y ahora desde el escritorio se definió un archivo de target para comprometer el equipo Pc-Juan.

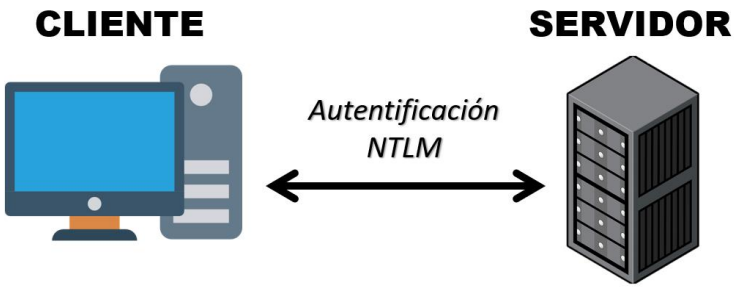
**Ilustración 28** Target




**Fuente:** Elaboración propia

Entonces en el archivo target se añadió la dirección ip ya conocida del equipo PC-Juan y se procedió a usar la herramienta NTLM Relay.

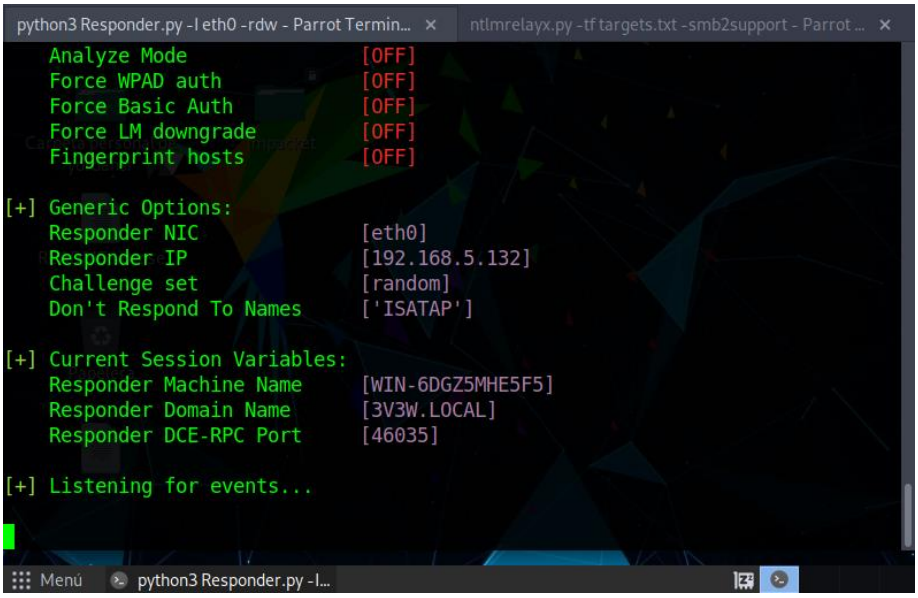
**Ilustración 29** Autentificación NTLM




**Fuente:** Elaboración Propia

Antes de ejecutar el ntlm relay, se procedió a lanzar el responder.py para envenenar la red, para que desde el otro equipo Pc-Maria, intentar acceder a un recurso compartido a nivel de red que existe atrapar esa conexión mientras no se logra validar la legitimidad del origen.

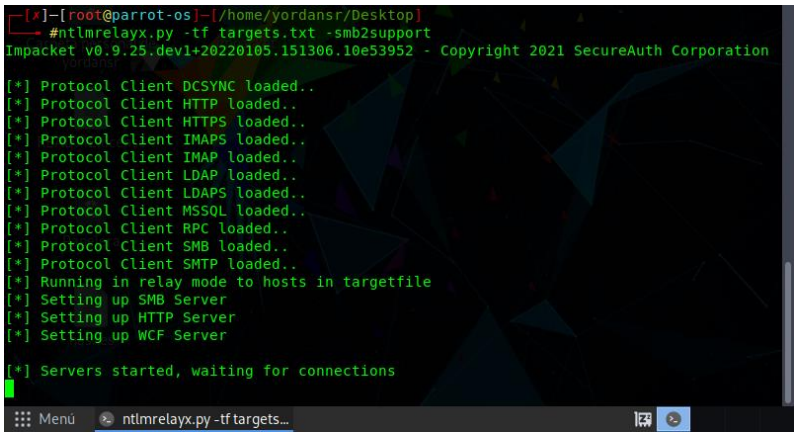
**Ilustración 30** Ejecución del responder.py




**Fuente:** Elaboración propia

Ya lanzado el responder se procedió a ejecutar el ntlm relay especificando el archivo de target con la ip del equipo que se desea comprometer y dándole soporte a la versión 2 de smb ya que se está trabajando con un equipo con sistema operativo Windows 10.

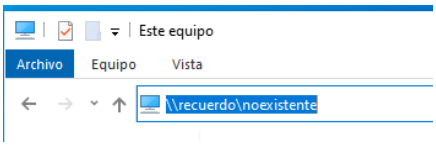
**Ilustración 31** Ejecución del ntlmrelayx.py




**Fuente:** Elaboración propia

Ahora desde el equipo Pc-María el cuál es administrador sobre el equipo de PC-Juan se intentó acceder a un recurso compartido que no existe.

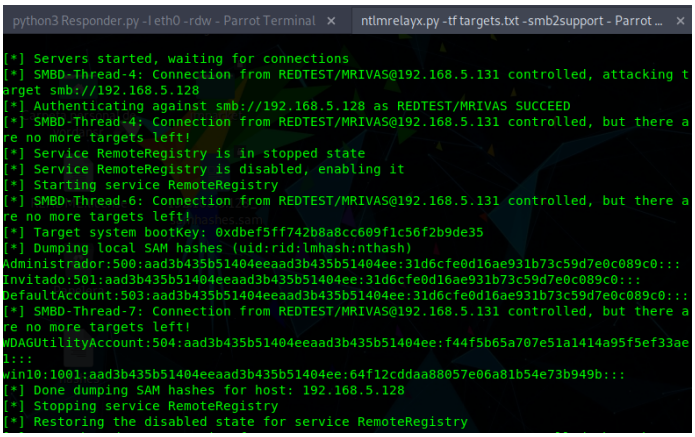
**Ilustración 32** Intento de acceso a recurso no existente




**Fuente:** Elaboración propia

Inmediatamente el responder y el ntlmrelay hacen su trabajo y capturaron la conexión, y gracias a que no se logró validar el origen, entonces el ntlm hace que se autentique con él y que aproveche las credenciales que identificó como privilegiadas sobre el equipo definido en el archivo target y así redirigió el flujo de esa autentificación sobre el equipo víctima para así con el ntlm relay dumpear la smb del equipo.

**Ilustración 33** Dumpeando la smb del equipo




**Fuente:** Elaboración propia

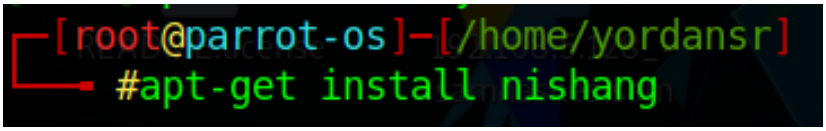
Una vez logrado esto una de las cosas que se pueden hacer es ejecutar comandos en el propio sistema, y para eso se realizó otro procedimiento similar, pero usando otro parámetro en la línea del ntlm relay.

Este proceso fue acompañado del uso de una script de otra herramienta de penetración que se detallará a continuación.

#### 2.5.10.2. Nishang

Nishang es un framework que contiene una colección de scripts y payloads que permiten ejecutar diferentes ataques y acciones post explotación, es una herramienta de pruebas de penetración basada en PowerShell, secuencia de comandos, DNS, y más scripts que son ampliamente usados en diferentes fases de pruebas. [45]

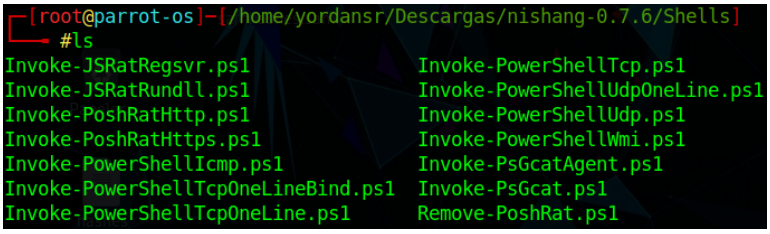
**Ilustración 34** Instalación de Nishang




**Fuente:** Elaboración Propia

Ya instalado ser puede ver los diversos scripts que contiene y esta vez se usó uno llamado Invoke-PowerShellTcp.ps1

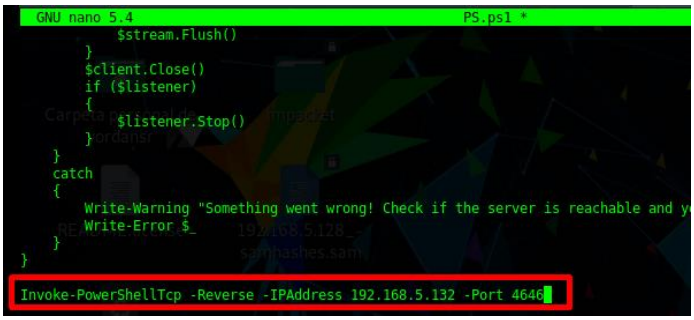
**Ilustración 35** Colección de scripts para PowerShell




**Fuente:** Elaboración propia

Se usó ese script, pero con una modificación y es por eso que para no afectar al archivo original se procedió a hacer una copia del script.

**Ilustración 36** Creación de la copia PS.ps1

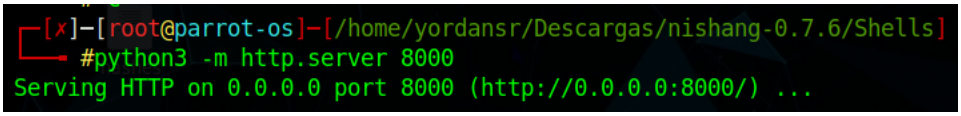



**Fuente:** Elaboración propia

Lo que hace esa línea es que se logre recibir un reserve Shell por power Shell tcp al equipo atacante por el puerto 4646.

Entonces lo que sucedió fue que al compartir un servidor http con Python por el puerto 8000 por defecto.

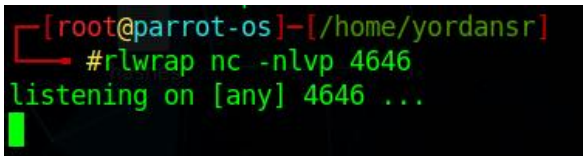
**Ilustración 37** Puerto http




**Fuente:** Elaboración Propia

El puerto 4646 se lo estableció en acción de escucha.

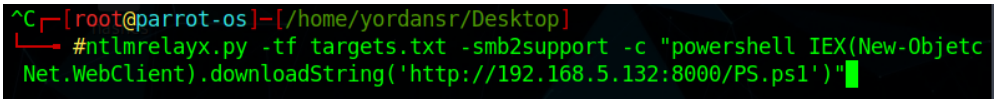
**Ilustración 38** Puerto 4646 en escucha




**Fuente:** Elaboración propia

Finalmente, con el ntlm relay ya no se dumpeó la smb si no mediante otros parámetros se logró interpretar un código malicioso que se preparó anteriormente de Nishang y nuevamente se lanzó el responder.py y el ntlmrelay.

**Ilustración 39** Ejecución del ntlmrelay con nishang




**Fuente:** Elaboración propia

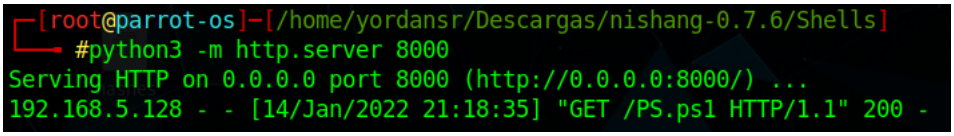
Nuevamente se ejecuta un intentó de acceso a un recurso compartido no existente desde el equipo PC-María, y esto ocurrió.

**Ilustración 40** Autentificación existosa por smb


**Fuente:** Elaboración propia

Como se logra visualizar el ntlm relay se ejecutó correctamente al igual que se logró visualizar que se realizó el GET e inyectó el comando a nivel de sistema.

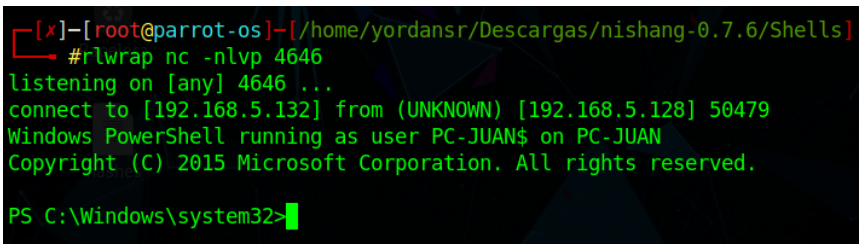
**Ilustración 41** Resultado del puerto 8000




**Fuente:** Elaboración propia

De forma que se logró acceder a la máquina PC-Juan con éxito.

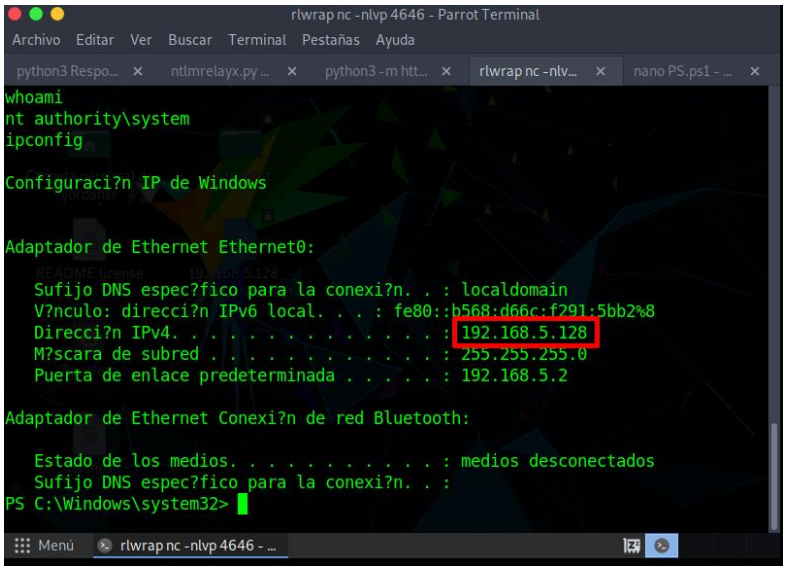
**Ilustración 42** Acceso exitoso a Pc-Juan




**Fuente:** Elaboración propia

Para comprobar que está en ese equipo se ejecutó un ipcofig y se logró visualizar que muestra la ip de PC-Juan.

**Ilustración 43** Ejecución de un ipconfig




**Fuente:** Elaboración propia

Es por ello la importancia de cuando el samba no está firmado en los todos los equipos de una red se exponen a que un atacante se aproveche de estas vulnerabilidades.

### 2.5.11. Reporte

En esta etapa se elabora un informe tipo ejecutivo dirigido a la directiva de la empresa, sin embargo no se realizará dicho informe porque no se está trabajando con ninguna empresa en específico, es por ello que se realizará un reporte técnico como se muestra a continuación.

**Tabla 3** Reporte

| **Informe N001** | **Test de penetración en Red Empresarial “RedTest”** |
|---|---|
| **Recolección de información** | • Se utilizó el envenenador Responder.py para capturar datos de los equipos de la red como el usuario, el nombre de la red, y hashes ntlmv2.<br>• Estos datos sirvieron para seguir el desarrollo de las siguientes fases de la metodología empleada. |

| | |
|---|---|
| **Modelado de Amenazas** | • Se recopiló datos de equipos pertenecientes a la red, que pueden ser usados para ataques de penetración y vulnerar información que compartan. |
| **Análisis de Vulnerabilidades** | • Haciendo uso de la herramiento nmap se logró escanear los puetos de la red en general, y detectar los hosts que se encuentran activos y detertar sus servicios como tambien sus versiones.<br>• Tambien se logra obtener datos en algún equipo en específico que un atacante o pentesting desee saber, como el sistema opoerativo que ocupa el equipo, direccion mac, servicios, etc. |
| **Explotación** | • Para esta fase se realizo dos tipos de herramientas, empezando por el john the rinner el cuál permitió desencriptar las contraseñas de los equipos de la red que se habían capturado antes, esto sucede cuando las claves en una red son demasiado débiles haciendo muy fácil el trabajo para estas herramientas y el atacante.<br>• Luego gracias al uso de la herramienta crackmapecex, que logró obtener más credenciales de tales equipos, esta herramienta logra ejecutarse aun así el windows defender de los equipos esté o no activado.<br>• Se logra obtener más datos como el dominio, estado de la firma del smb que es muy importante para los atacantes para con que equipo puede desplegar muchoos |

| | |
|---|---|
| | más ataques. |
| **Post-Explotación** | • Y por último en esta fase de las pruebas, mediante el uso de NTLM Relay y scripts de Nishang, se logró comprometer el equipo deseado por este caso el pentester, consiguiendo así acceso desde la máquina atacante y poder ejecutar comandos a nivel de sistema. |

**Fuente:** Elaboración propia

# 3. CAPÍTULO III. EVALUACIÓN DEL ESCENARIO

## 3.1. PLAN DE EVALUACIÓN

Como en el trabajo se simuló un entorno empresarial controlado donde se lo dejó vulnerable para desplegar los diferentes ataques, se propone evaluar la red mediante los debidos cambios y configuraciones que una empresa debería de realizar para proteger a los equipos de su red y su información.

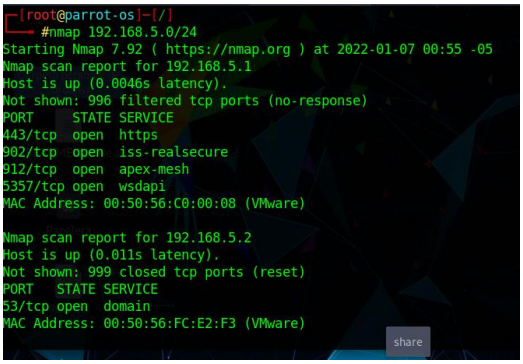
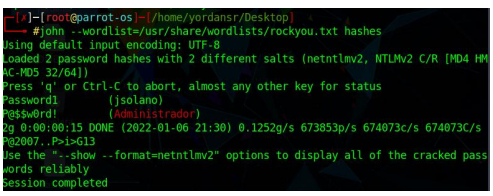
El plan consiste en ejecutar una vez más los ataques de penetración y constatar como reacciona cuando la red ya está configurada, y evidenciar los resultados que dejan cuando las empresas toman medidas correctas para la seguridad de su red.

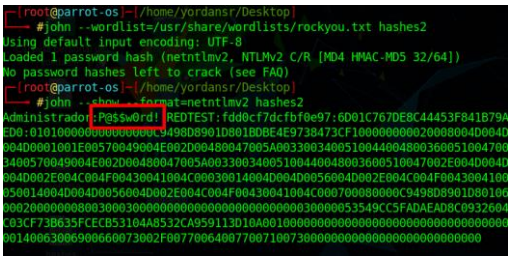
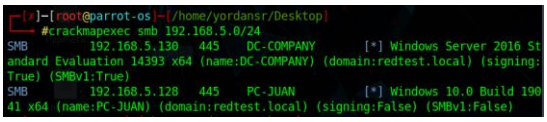
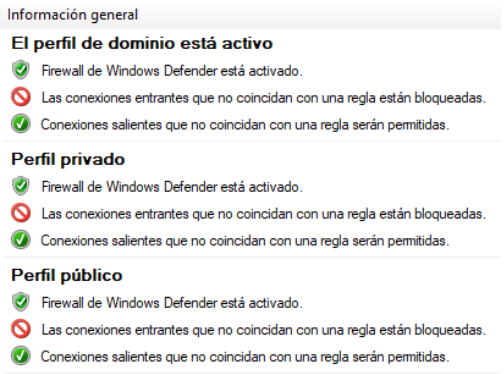
## 3.2. RESULTADOS DE LA EVALUACIÓN

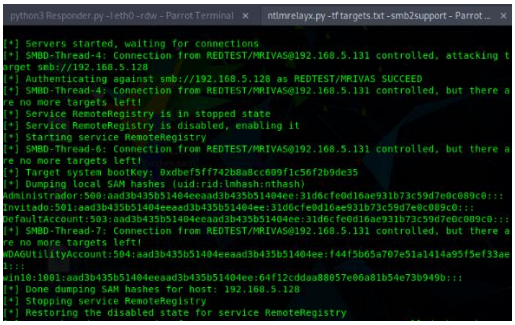
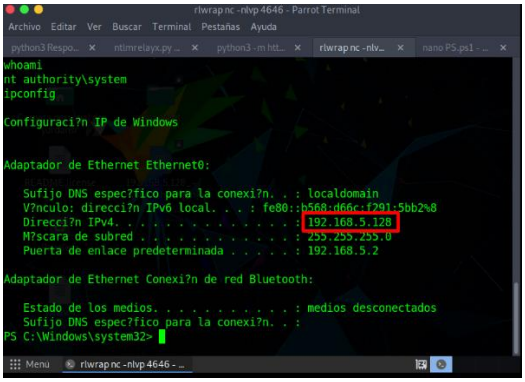
Para mostrar los resultados de la evaluación se elaboró una tabla donde se indica el nombre del ataque desplegado conjuntamente con el resultado obtenido en la red empresarial vulnerable y a lado las correciones que se hicieron o detallar las medidas que se pueden llevar a cabo para defenderse ante tales ataques desplegados.

Lo cual ayudó para poder sacar las conclusiones sobre la importancia en la actualidad sobre el emplear el ethical hacking para la seguridad en las redes empresariales.

**Tabla 4** Resultados de la evaluación

<table>
<tr><th colspan="2">Ataque desplegado: nmap</th></tr>
<tr><th>Resultados</th><th>Correciones/Medidas</th></tr>
<tr><td>El nmap se ejecuta con éxito obteniendo los hosts activos en la red, sus servicios disponibles y sus versiones, sistema operativo, etc.<br> 
</td><td>• Conociendo lo que este ataque obtiene, se puede esconder los servicios, nmap obtiene una lista de los 1000 puertos más usados, por eso es bueno cambiar el puerto de escucha de algun servicio por uno que no sea muy usual, y así librarse del escaneo rápido de esta herramienta.<br><br>• Otra medida puede ser confundir la detección del sistema operativo y esto se lograría modificando el valor por defecto del TTL por un valor inusual.</td></tr>
<tr><th colspan="2">Ataque desplegado: John the Ripper</th></tr>
<tr><th>Resultados</th><th>Correciones/Medidas</th></tr>
<tr><td>La herramienta john se ejecutó y logró crackear las contraseñas de los equipos obtenidos durante el trafico originado por el envenador sin problema alguno debido a la póca dificultad que tienen estas.<br> 
</td><td>• En este caso se cambio la contraseña del equipo Domain Controller la cual tenia: P@$$w0rd!, a una mucho más difícil de desencriptar, esta P@$$w0rd!ZxCvBnM@!#%, y estos fueron los resultos obtenidos luego de volver a intentar ejecutar el comando john.</td></tr>
</table>

| | |
|---|---|
|  | • Se carga el hash del equipo pero ahora ya no arrojó ningún resultado de contraseña crackeada, se uso un comando para visualizar la lista de contraseñas crackeadas según el arcvhico hashes2 y tapoco mostró resultados. |
| **Ataque desplegado:** crackmapecex | |
| **Resultados** | **Correciones/Medidas** |
| Se ejecutó el crackmapecex para un escaneo rápido de las máquinas activas en la red según la subred especificada y bajo el protocolo smb.<br>  | • Una medida para contrarrestar este ataque es asegurarse de tener siempre activados el Firewall de Windows Defender.<br>  <br>• En este caso se dejo al equipo DC con el firewall desactivado y al equipo Pc-Juan con los firewalls activado y al momento de ejecutar el crackmapecex ya no logró capturar al equipo PC-Juan. |

| **Ataque desplegado:** ntlmrelay y scripts de nishang | |
|---|---|
| **Resultados** | **Correcciones/Medidas** |
| Logra dumpear la smb del equipo comprometido sin nigún problema.<br>  <br>Así tambíen se logró ejecutar comandos a nivel de sistema ya habiendo conseguido acceder a la máquina comprometida.<br>  | • Una medida sería desahbilitar la detección automatizada de la red interna y asegurarse de que los navegadores se autentifiquen solamente en sitios confiables.<br>• Desactivar la detección del proxy automatica de Windows.<br>• Y una medida más sería deshabilitar los protocolos LLMNR y NBNS los cuáles no suelen ser necesarios para un red que se encuentre bien configurada. Esto ayudará a que al atancate se le dificulte la falsificación de resolución de nombres y así evitar que pueda las máquinas comprometida se conecten a la máquina o servidor del atacante. |

**Fuente:** Elaboración propia

## 3.3. CONCLUSIONES

- Se realizó una red de entorno empresarial mediante un software de virtualización que permitió interactuar sin problemas con los equipos creados y designarle sus roles correspondientes.

- El sistema operativo Parrot resultó de mucha utilidad en el desarrollo de este trabajo, muy conocida dentro del mundo de la ciberseguridad y comunidades grandes de hackers, resulto ser una herramienta muy útil y completa para poder desplegar los ataques de penetración hacia la red virtualizada.

- La metodología PTES, ofrece varias opción según el tipo de pruebas y entornos a los que se quieran dirigir, es por ello que se utilizó las fases para pruebas dirigidas a una red, que resultó ser muy completa y entendible para corregir vulnerabilidades que presentaba la red, y gracias a la investigación realizada sobre configuraciones que las empresas deben ejecutar al momento de armar toda la infraestructura informática.

## 3.4. RECOMENDACIONES

- Para el desarrollo de este trabajo fue importante estar al tanto de las especificaciones del equipo donde se elaboró la virtualización del entorno empresarial, y así poder determinar la magnitud del prototipo y desarrollar sin problema alguno cada una de las actividades propuestas.

- Parrot OS es una excelente distribución para personas principiantes y profesionales, viene acompañada con mas de 500 herramientas enfocadas a la seguridad, se recomienda que si se quiere usarla como un sistema operativo principal probar antes instalandola en una máquina virtual y ver el comportamientes, y así detectar cualquier fallo o error, luego de eso si ya se podría probar en una partición física.

- Es importante ser cuidadoso en cumplir con el alcance que se espicificó en la metodología, porque algún error puede ocasionar incovenientes con la empresada que haya solicitado el pentesting, aunque en este caso no se trabajó con alguna empresa en específico.

- Procurar consultar con un especialista en el tema antes de llevar a cabo algun actividad sobre ciberseguridad, y estar seguro de que sistema operativo se enfoque más al caso en cuestión.

- Realizar las debidas configuraciones de seguridad para prevenir estos tipos de ataques que intentar encontrar vulnerabilidades y comprometer lo más importante que tienen la mayoría de empresas del mundo que es la información.

## REFERENCIAS BIBLIOGRÁFICAS


[1] E. Zhuma Mera, O. J. Brito Casanova, J. T. Vergara, and B. Oviedo Bayas, “DYNAMIC ANALYSIS OF MALWARE IN A VIRTUALIZED NETWORK ENVIRONMENT,” *CONRADO*, vol. 17, no. 0, pp. 114–120, Jan. 2021.

[2] “CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE ,” 2020.

[3] S. Morgan, “Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021,” 2019.

[4] H. Muñoz Hernández, L. G. Zapata Cantero, and D. M. Requena Vidal, “Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia,” *Revista Venezolana de Gerencia*, vol. 2, no. 0, pp. 528–541, 2019.

[5] D. Ramírez Bermúdez, “Criptografía y seguridad informática,” *Revista de Ciencias de la Universidad Pablo de Olavide*, no. 0, pp. 64–67, Oct. 2020.

[6] C. Astudillo, F. Carvajal, J. P. Carvallo, E. Crespo-Martínez, M. Orellana, and R. Vintimilla, “Attacking an ERP with Open Source Software,” *Enfoque UTE*, vol. 9, no. 0, pp. 138–148, Mar. 2018.

[7] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, “Web attacks: defeating monetisation attempts,” *Network Security*, vol. 2019, no. 5, pp. 11–19, May 2019, doi: 10.1016/S1353-4858(19)30061-3.

[8] E. Foglia, “Mundo ‘hacker’ y diseño (I): el ‘hacker’ como sujeto político,” *COMeIN*, vol. 111, no. 0, Jun. 2021.

[9] R. O. Andrade, I. Ortiz-Garces, and M. Cazares, “Cybersecurity Attacks on Smart Home During Covid-19 Pandemic,” in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, Jul. 2020, pp. 398–404. doi: 10.1109/WorldS450073.2020.9210363.

[10] M. Silic and P. B. Lowry, “Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes,” *Information Systems Frontiers*, vol. 23, no. 2, pp. 329–341, Apr. 2021, doi: 10.1007/s10796-019-09949-3.

[11] G. Martínez Atienza, “Ataques en el Ciberespacio,” *Experiencia*, vol. 0, no. 0, 2020, Accessed: Dec. 16, 2021. [Online]. Available: https://dialnet.unirioja.es/servlet/libro?codigo=789379

[12] J. F. Espinosa Sánchez, “Ciberdelincuencia. Aproximación criminológica de los delitos en la red.,” *Revista hispanoamericana de Historia de las Ideas*, no. 44, pp. 153–173, 2019.

[13] S. Arrazola Ruiz, “Cybercrimes as a juridical phenomenon. A procedural approach.,” *Revista Aequitas*, no. 18, pp. 371–402, 2021.

[14] V. P. Tintín-Perdomo, J. R. Caiza-Caizabuano, and F. S. Caicedo-Altamirano, “Architecture of information networks. Principles and concepts.,” vol. 4, no. 2, pp. 103–122, 2018, doi: 10.23857/dom.cien.pocaip.2017.4.núm.2.abril.103-122.

[15] D. Dias Rodrigues and C. de C. Sander, “Informatização empresarial: fatores, dificuldades e desafios,” *Research Society and Development*, vol. 8, no. 5, p. e885764, Feb. 2019, doi: 10.33448/rsd-v8i5.764.

[16] M. S. Aliero, I. Ghani, K. N. Qureshi, and M. F. Rohani, “An algorithm for detecting SQL injection vulnerability using black-box testing,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 1, pp. 249–266, Jan. 2020, doi: 10.1007/s12652-019-01235-z.

[17] O. Cárdenas, J. Molina, and J. Armijos, “LA SEGURIDAD INFORMÁTICA EN LA PREVENCIÓN DE VULNERABILIDADES DE LOS DISPOSITIVOS MÓVILES,” *Centro de Investigación y Desarrollo Profesiona*, vol. 1, pp. 219–230, 2017.

[18] J. E. Ortiz-Lazo and J. K. Vizñay-Duran, “Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel,” *Polo del Conocimiento*, vol. 4, no. 7, p. 174, Jul. 2019, doi: 10.23857/pc.v4i7.1029.

[19] A. E. Rodríguez Llerena, “Fundamental Tools for Ethical Hacking,” *Revista Cubana de Informática Médica*, vol. 12, no. 1, pp. 116–131, 2020, [Online]. Available: http://scielo.sld.cu

[20] A. Etxeberria, I. Goirizelaia, J. J. Uncilla, J. Astorga, and M. Uharte, “Zibererasoetatik babesteko, hacking etikoaren balioa,” *EKAIA Euskal Herriko Unibertsitateko Zientzia eta Teknologia Aldizkaria*, no. 39, pp. 313–326, Apr. 2021, doi: 10.1387/ekaia.21939.
[21] John Jackson, “Principle Ethical Hacking & Considerations,” *Actuarios*, vol. 48, pp. 28–29, 2021.
[22] F. R. Muñoz, E. A. Armas Vega, and L. J. G. Villalba, “Analyzing the traffic of penetration testing tools with an IDS,” *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6454–6469, Dec. 2018, doi: 10.1007/s11227-016-1920-7.
[23] A. Y. Vanegas Romero, “Pentesting, ¿Porque es importante para las empresas?,” *Universidad Piloto de Colombia*, 2019, Accessed: Dec. 14, 2021. [Online]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6286/00005220.pdf?sequence=1
[24] J. J. Santacruz Espinoza, C. R. Vega Abad, L. F. Pinos Castillo, and O. E. Cárdenas Villavicencio, “Sistema cobit en los procesos de auditorías de los de sistemas informáticos,” *Journal of Science and Research: Revista Ciencia e Investigación*, vol. 2, no. 8, p. 65, Dec. 2017, doi: 10.26910/issn.2528-8083vol2iss8.2017pp65-68.
[25] M. Shakibazad, “A Framework to Create a Virtual Cyber Battlefield for Cyber Maneuvers and Impact Assessment,” *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 3, pp. 615–625, Sep. 2019, doi: 10.1007/s40998-018-00172-5.
[26] B. García, M. A. Sánchez, and J. Abadía, “Herramienta web con tecnología de cadena de bloques para un sistema de facturación electrónica en Colombia,” *Información tecnológica*, vol. 32, no. 3, pp. 15–24, Jun. 2021, doi: 10.4067/S0718-07642021000300015.
[27] C. G. Erazo Bastidas, “IDENTIFICACIÓN DE VULNERABILIDADES DE LOS SERVICIOS TECNOLÓGICOS DE LA UNIÓN DE COOPERATIVAS DE AHORRO Y CRÉDITO DEL NORTE APLICANDO LA PRÁCTICA DE PENTESTING.,” Ibarra, 2017. Accessed: Dec. 15, 2021. [Online]. Available: http://repositorio.utn.edu.ec/bitstream/123456789/7396/1/04%20ISC%20447%20TRABAJO%20DE%20GRADO.pdf
[28] H. R. González Brito and R. Montesino Perurena, “Capabilities of penetration test methodologies to detect frequent vulnerabilities of web applications,” *Revista Cubana de Ciencias Informáticas* , vol. 12, no. 0, pp. 52–65, Sep. 2018, Accessed: Dec. 15, 2021. [Online]. Available: http://scielo.sld.cu/pdf/rcci/v12n4/rcci05418.pdf
[29] V. D. Cordoví Hernández, M. E. Pardo Gómez, E. López Hung, and I. Martínez Ramírez, “Virtualization of the training contents: a didactic alternative in the Nursing-Technology Faculty in Santiago de Cuba,” *MEDISAN*, vol. 23, no. 1, 2019.
[30] R. Perdigón Llanes and R. Ramírez Alonso, “Plataformas de software libre para la virtualización de servidores en pequeñas y medianas empresas cubanas,” *Revista Cubana de Ciencias Informáticas*, vol. 14, no. 1, pp. 40–57, 2020.
[31] Vmware, “Workstation para Windows,” Dec. 24, 2021. https://www.vmware.com/content/vmware/vmware-published-sites/latam/products/workstation.html (accessed Dec. 27, 2021).
[32] L. Faletra, “Parrot Security,” 2020. https://www.parrotsec.org (accessed Feb. 12, 2022).
[33] I. Nalini C, K. Anil M., and Heera G. Wali, “Implementation of Active Directory for efficient management of networks,” *Procedia Computer Science*, vol. 172, pp. 112–114, 2020, doi: 10.1016/j.procs.2020.05.016.
[34] “Directrices técnicas de PTES.” http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (accessed Dec. 27, 2021).
[35] “Recopilación de inteligencia.” http://www.pentest-standard.org/index.php/Intelligence_Gathering#Level_1_Information_Gathering (accessed Dec. 27, 2021).
[36] “Modelado de amenazas.” http://www.pentest-standard.org/index.php/Threat_Modeling (accessed Dec. 27, 2021).

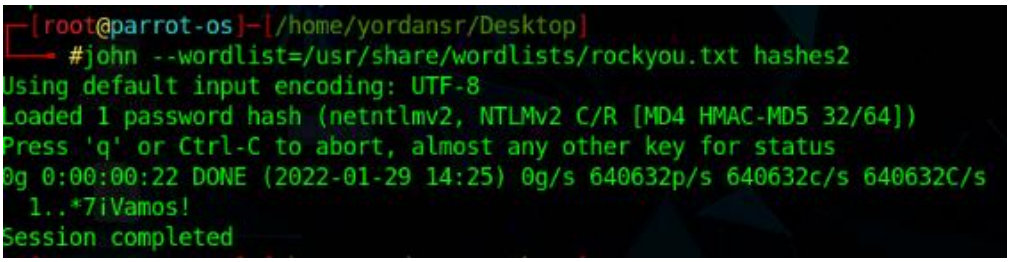
[37] “Análisis de vulnerabilidades.” http://www.pentest-standard.org/index.php/Vulnerability_Analysis (accessed Dec. 27, 2021).
[38] “Explotación.” https://www-pentest--standard-org.translate.goog/index.php/Exploitation (accessed Dec. 28, 2021).
[39] “Post-explotación.” http://www.pentest-standard.org/index.php/Post_Exploitation (accessed Dec. 28, 2021).
[40] M. A. Leguizamón Páez, M. A. Bonilla-Díaz, and C. A. León-Cuervo, “Analysis of computer attacks through Honeypots in the District University Francisco José de Caldas,” *INGENIERÍA Y COMPETITIVIDAD*, vol. 22, no. 2, pp. 1–13, May 2020, doi: 10.25100/iyc.v22i2.8483.
[41] D. S. Gordón Revelo and R. Pacheco Villamar, “Analysis of Strategies of Computer Security Management Based on the Open Source Security Testing Manual Methodology (OSSTMM) for the Intranet of a Higher Education Institution,” *ReCIBE*, vol. 7, no. 1, pp. 1–21, Feb. 2018, Accessed: Jan. 06, 2022. [Online]. Available: https://www.redalyc.org/journal/5122/512255650001/
[42] Openwall, “John the Ripper password cracker.” https://www.openwall.com/john/ (accessed Feb. 12, 2022).
[43] NGI, “CrackMapExec: post-explotación para entornos Active Directory,” 2020. https://www.ngi.es/crackmapexec-post-explotacion-entornos-active-directory/ (accessed Feb. 12, 2022).
[44] I. M. Torres Moreno and A. Hidalgo Guerrero, “Content Management System and appropriation of urban heritage,” *Trilogía Ciencia Tecnología Sociedad*, vol. 9, no. 17, pp. 161–174, Dec. 2017, Accessed: Jan. 07, 2022. [Online]. Available: https://www.redalyc.org/articulo.oa?id=534367006007
[45] Kali, “Nishang,” 2020. https://www.kali.org/tools/nishang/ (accessed Feb. 12, 2022).

## ANEXOS

Resultado luego de la corrección.

### John the ripper

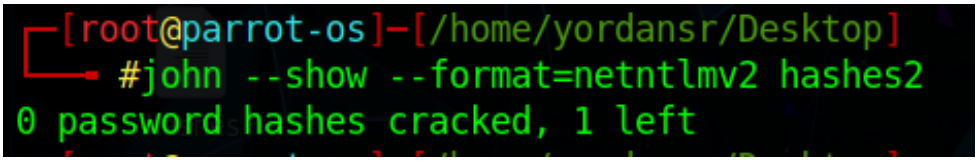
**Ilustración 44** Prueba de corrección John the ripper




**Fuente:** Elaboración propia

Al momento de visualizar las contraseñas crackeadas no se obtuvo resultados con una contraseña mucho más complicada.

**Ilustración 45** Visualización de contraseñas crackeadas

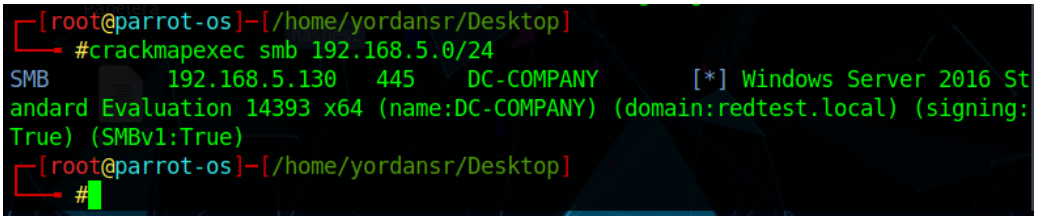



**Fuente:** Elaboración propia

Resultado luego de la corrección.

**Crackmapecex**

**Ilustración 46** Prueba de corrección Crackmapecex

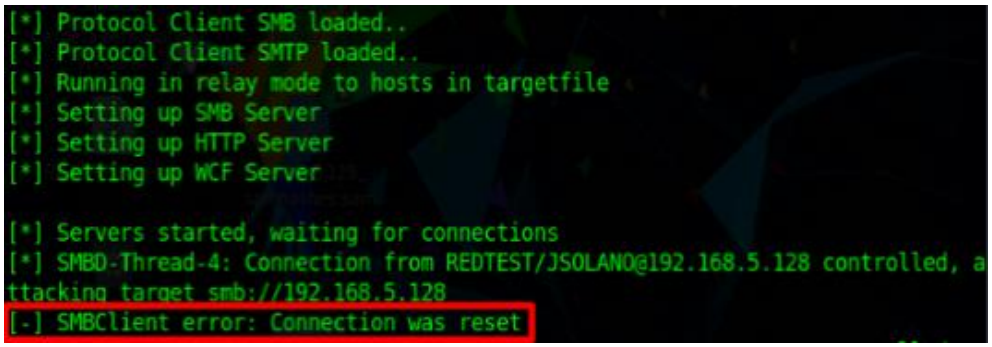



**Fuente:** Elaboración propia

Resultado luego de la corrección.

**Ntlmrelay**

**Ilustración 47** Prueba de corrección Ntlmrelay




**Fuente:** Elaboración propia