LABORATORIO DE PENTESTING CON IMPACKET.

PENTESTING ÉTICO: KALI LINUX → WINDOWS 10

Objetivo: Aprendizaje de técnicas de penetración ética.

Enfoque: Explotación de servicios Windows con Impacket.

Modalidad: Laboratorio controlado y educativo.

>> **ADVERTENCIA**: Solo para fines educativos y éticos

- DESCRIPCIÓN DEL TRABAJO

Este laboratorio simula un escenario real de pentesting donde un profesional de ciberseguridad evalúa la seguridad de sistemas Windows desde una estación Kali Linux, utilizando herramientas Impacket.

COMPETENCIAS A DESARROLLAR:

✅ Reconocimiento y mapeo de red (Nmap, ping)

✅ Explotación de servicios SMB para acceso a recursos

✅ Ejecución remota de comandos (PSExec/WMI shells).

✅ Extracción y análisis de credenciales del sistema.

✅ Aplicación de técnicas de post-explotación.

✅ Implementación de contramedidas defensivas.

ENTORNO: Laboratorio aislado con sistemas virtuales controlados.

- **IMPACKET**: SUITE ESPECIALIZADA EN PROTOCOLOS WINDOWS.

JUSTIFICACIÓN DE LA ELECCIÓN:

Impacket es el estándar de facto para pentesting de entornos Windows debido a su capacidad nativa para manejar protocolos Microsoft sin requerir instalación de software adicional en el objetivo.

COMPONENTES UTILIZADOS:

>> smbclient.py - ACCESO A RECURSOS COMPARTIDOS.

Navegación en sistema de archivos remoto.

Descarga/subida de archivos sensibles.

>> psexec.py - SHELL REMOTO PRINCIPAL.

Ejecución de comandos con privilegios SYSTEM.

Técnica ampliamente conocida por administradores.

>> wmiexec.py - SHELL ALTERNATIVO SIGILOSO

Ejecución vía WMI sin escritura de archivos.

Menor detección por sistemas de monitoreo.

>> secretsdump.py - EXTRACCIÓN DE CREDENCIALES

Volcado de hashes SAM y LSA.

Base para técnicas de escalamiento de privilegios.

REQUISITOS ESPECÍFICOS PARA VIRTUALIZACIÓN

REQUISITOS DEL HOST FÍSICO (PC CON VIRTUALBOX):

- Procesador: Intel Core i5 o AMD Ryzen 5 (mínimo 4 núcleos)
- RAM: 16GB mínimo, 32GB recomendado
- Sistema Operativo Host: Windows 10/11, Ubuntu 20.04+ o macOS 10.15+
- VirtualBox 6.1+ o VMware Workstation Pro 16+

RECURSOS PARA VMs:

Kali Linux VM:

- RAM: 4GB asignados (8GB recomendado).
- CPU: 2 núcleos virtuales (4 recomendado).
- Red: Adaptador puente o red interna.

Windows 10 VM:

- RAM: 4GB asignados (8GB recomendado)
- CPU: 2 núcleos virtuales (4 recomendado)
- Red: Misma configuración que Kali

CONFIGURACIÓN DE KALI LINUX (64-bit):

- Distribución: Kali Linux 2023.1+ (imagen oficial)
- Python: 3.9+ preinstalado
- Usuario: kali con privilegios sudo
- Herramientas: nmap, netdiscover preinstaladas.

CONFIGURACIÓN DE WINDOWS 10 (64-bit):

- Versión: Windows 10 (64-bit).
- Usuario Administrador: Propiedades de la cuenta debe estar deshabilitada
- Firewall: Totalmente desactivado.
- Windows Defender: Totalmente desactivado.

CONFIGURACIÓN DE RED REQUERIDA:

- Ambas VMs en la misma red virtual (Adaptador Puente=192.168.x.x).
- Conectividad IP bidireccional confirmada.
- Puerto 445 (SMB) abierto en Windows.

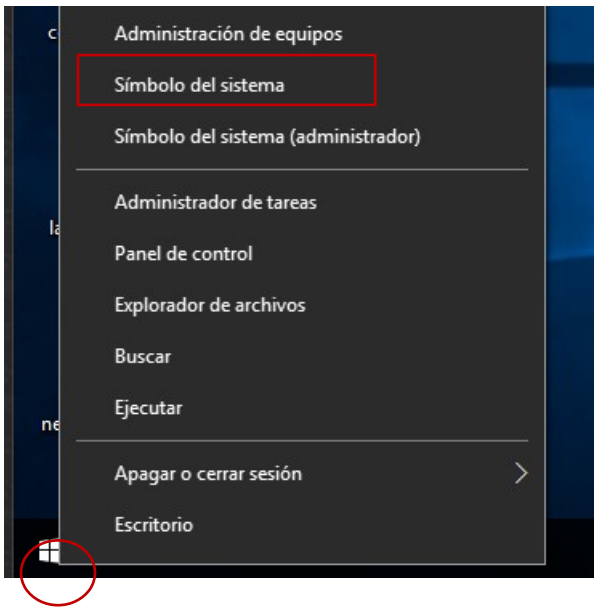
VALIDACIONES MÍNIMAS ANTES DE EJECUTAR:

- Ping exitoso entre ambas máquinas
- nmap -p 445 [IP_Windows] debe mostrar puerto abierto
- Credenciales de administrador Windows confirmadas
- Python 3 funcional en Kali con permisos sudo.

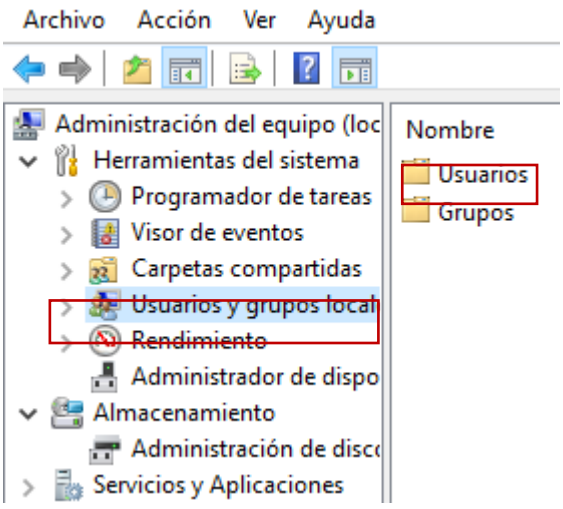
PROCESO: INSTALACION Y PREPARACION:

VMS: WINDOWS 10 64 Bits

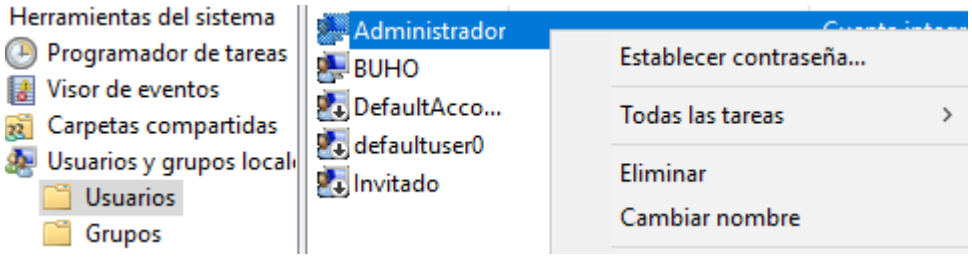
1. Iniciaremos con Windows pues será el punto objetico de ataque:
2. Presionaremos click derecho **>** sobre el símbolo de Windows **>** he iremos a **Administrador de equipos**:



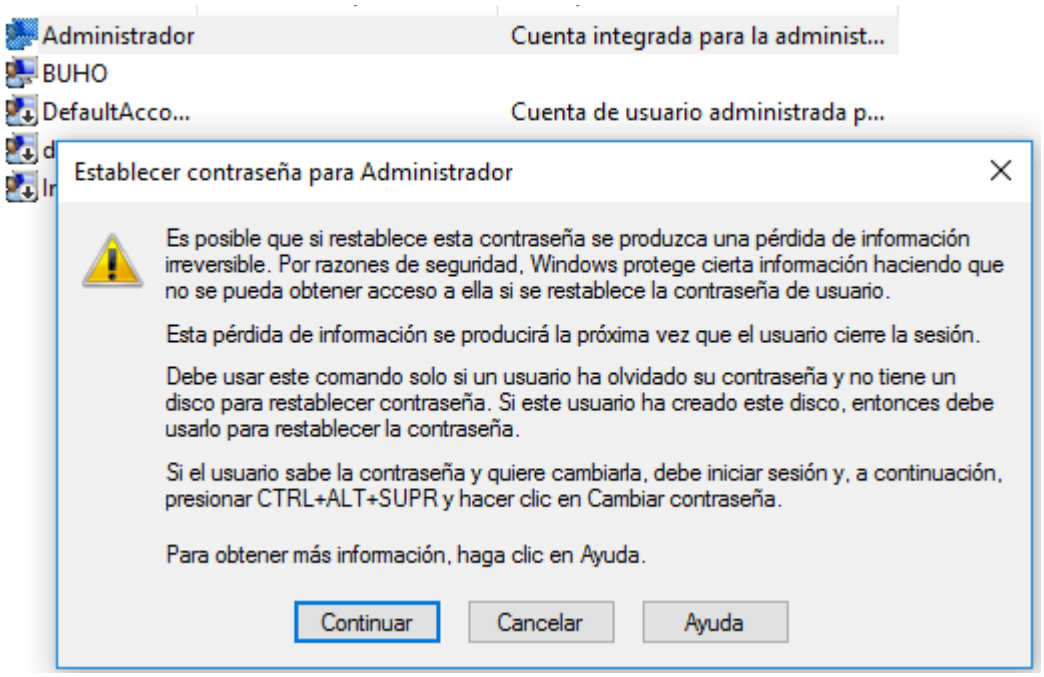
3. Una vez estando en administrador de equipos nos dirigiremos a > Usuarios y Grupos Locales > Carpeta Usuarios:



4. Estableceremos una contraseña al usuario administrador (o nueva contraseña si ya le han asignado una) y le daremos **guardar.**
   Nota: Si el usuario Administrador no existe seleccionaremos el usuario que posea permisos de Administrador, probablemente sea el usuario que se creo al iniciar la instalación de Windows.

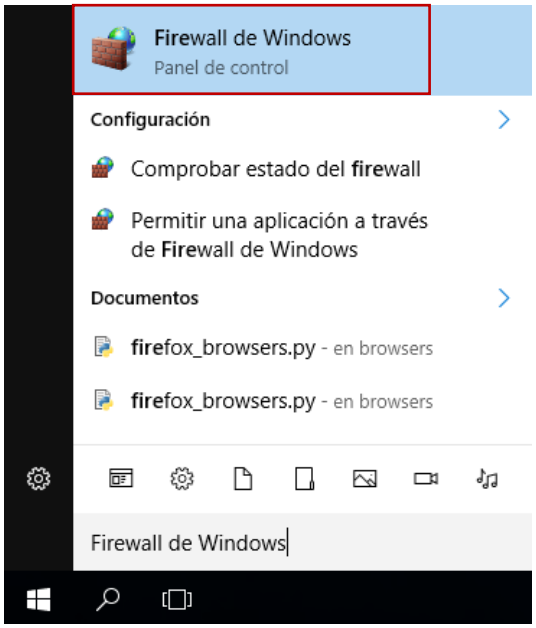


- Es probable que al presionar Establecer contraseña se habrá una ventana emergente, pero esta solo una advertencia de que la contraseña va a ser restablecida mas no afectara el funcionamiento de nuestra VMS.



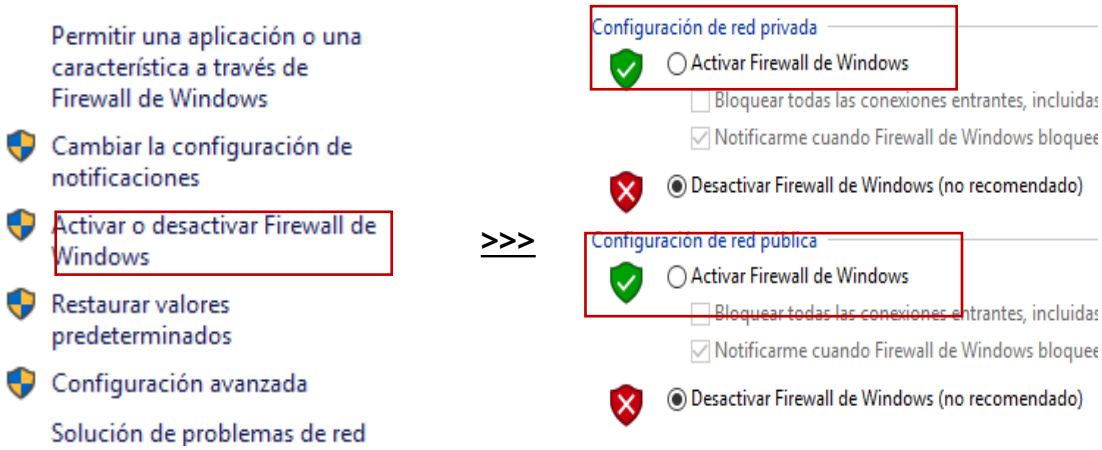
5. Ahora se desactivará el firewall de Windows con la intensión de que este no bloquee los puertos smb (SAMBA), usando el buscador de Windows buscaremos FIREWALL WINDOWS.

   NOTA: Dependiendo de la versión de Windows este puede tener otro nombre y se deberá usar acceder al panel de control, el ejercicio de laboratorio se está mostrando en base Windows 10 64 bit.



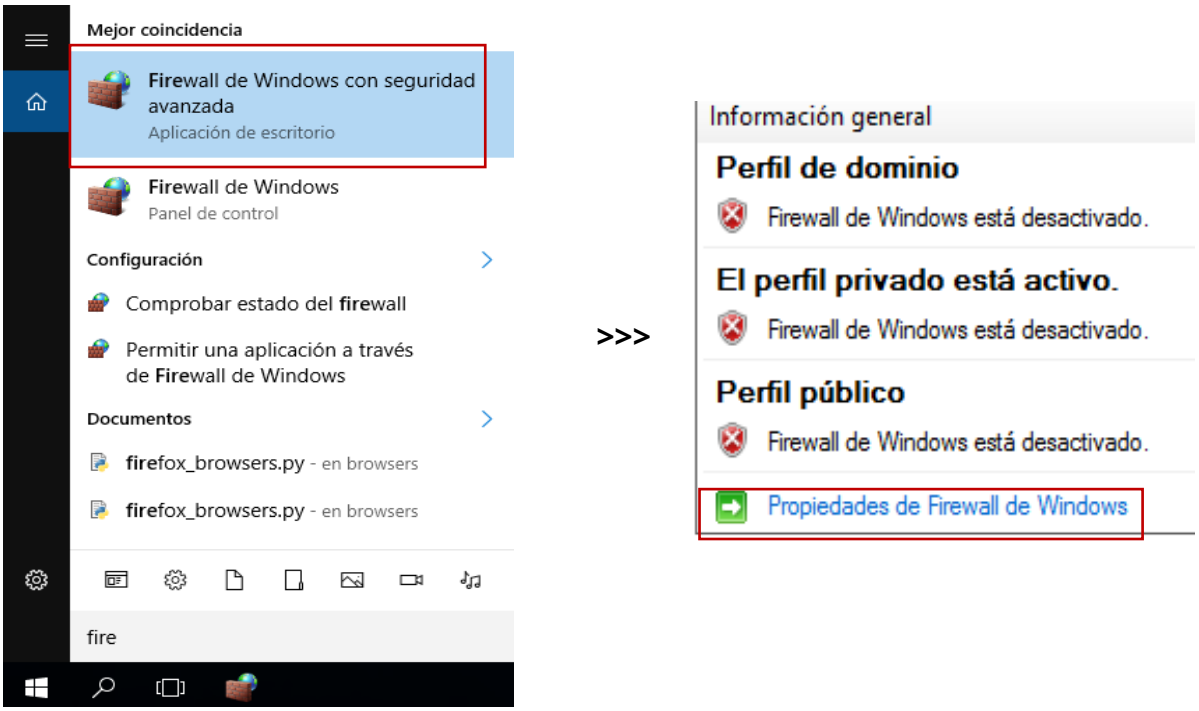
- Una vez en el firewall editaremos la opción > **Activar o Desactivar Firewall >**

  En ella **Desactivaremos** las casillas de configuración de red **privada y Pública.**

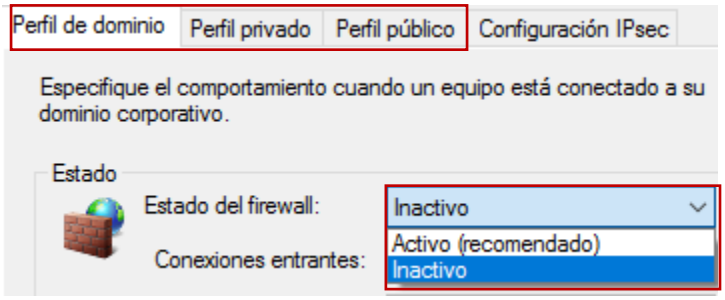


6. Por último, en el buscador de Windows buscaremos firewall, pero seleccionaremos la aplicación > **Firewall de Windows con seguridad avanzada.**

- Dentro de esa aplicación veremos varias configuraciones de firewall de Windows, pero nos ubicaremos en la sección de > **Propiedades de Firewall Windows.**



- Dentro del apartado de propiedades veremos el Perfil de Dominio el cual estará activo y por ello lo desactivaremos, es probable que los perfiles Privados y Públicos este igual activos así que también deben ser desactivados.



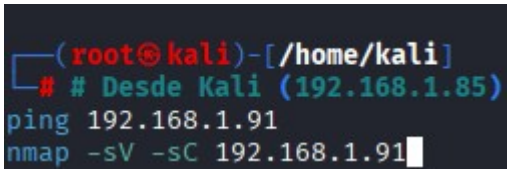
NOTA: Esto finalizaría la configuración de Windows 10 para la ejecución de la herramienta de impacket y evitar algún tipo de bloqueo por parte de Windows.

PROCESO: INSTALACION Y PREPARACION:

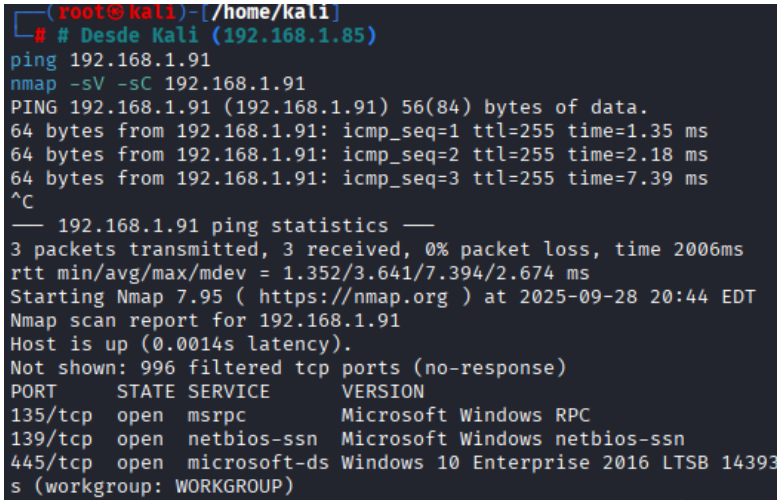
VMS: Kali Linux 64 Bits

1. Estando en Kali Linux abriremos una termina y accederemos como usuario **root** con el comando **sudo su** > Digitaremos nuestra contraseña este caso será **kali**

- Una vez como usuarios root haremos una prueba ping y mapeo usando la ip de Windows – esto nos hará saber si hay respuesta entre redes con ambas maquina y también saber si el puerto smb esta activo o no:

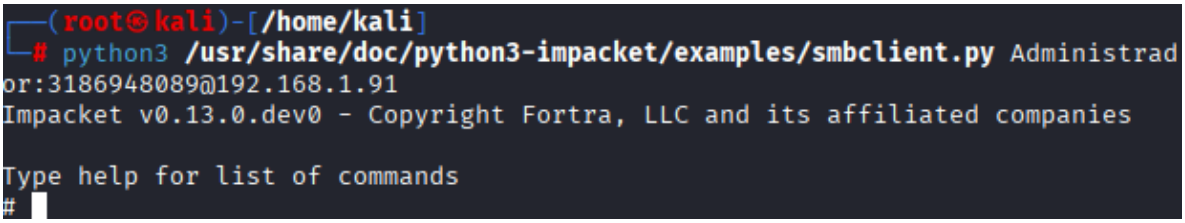


- Los comandos empezaremos ejecutar, si el ping es correcto detendremos el proceso con las teclas **Ctrl + C**, eso ara que el mapeo de la ip empiece lo cual puede tardar un par de minutos, si la respuesta se mostrara una serie de código igual a la siguiente imagen:

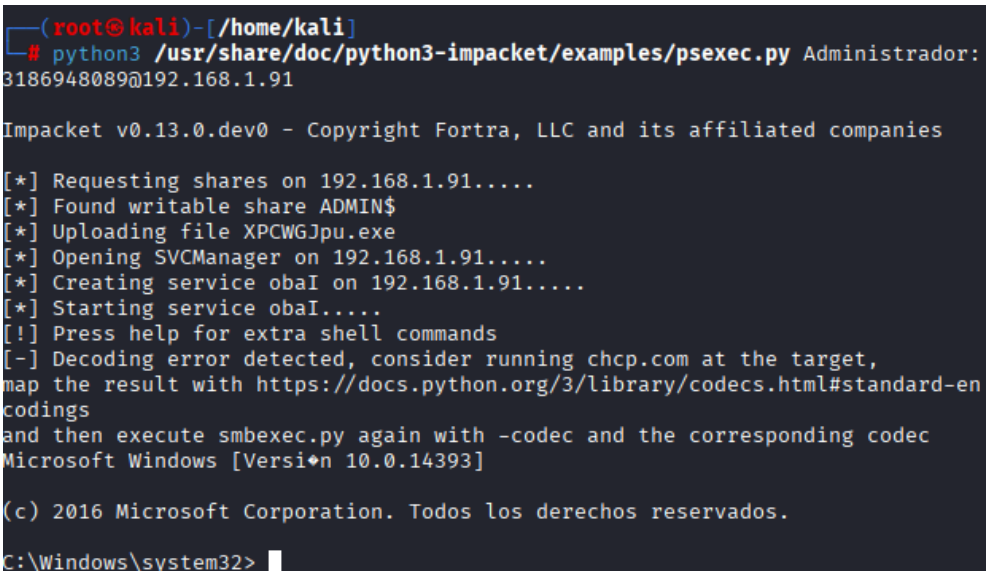


2. Para verificar el acceso SMB hacia Windows con el siguiente código deberemos tener Usuario **Administrador** de Windows > **Contraseña** del usuario y la **ip** del Windows:
python3 /usr/share/doc/python3-impacket/examples/smbclient.py Administrador:3186948089@192.168.1.91

- Si el resultado es correcto se mostrará el siguiente resultado de mostrar una respuesta errónea se debe verificar el proceso de Windows dado en la pagina 5:

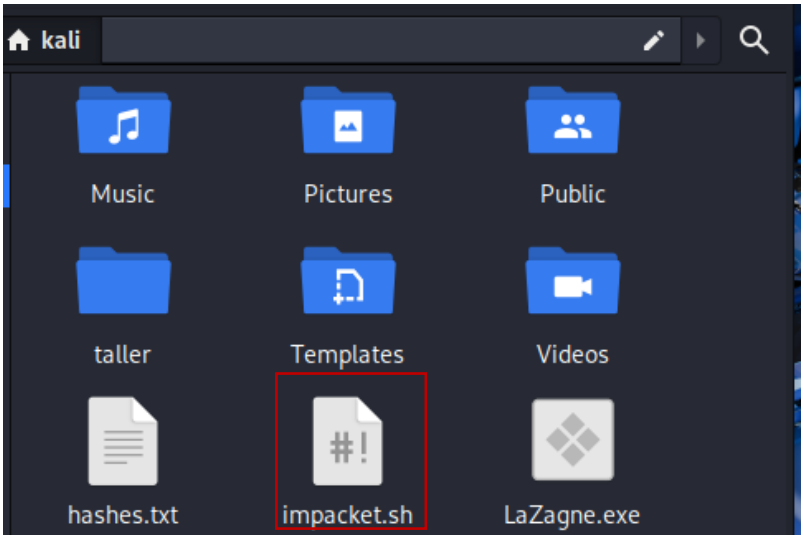


3. Si el comando anterior funciono correctamente presionaremos Ctrl + C para salir de el y usaremos en siguiente comando el cual nos dará acceso remoto a Windows de manera remota.
   python3 /usr/share/doc/python3-impacket/examples/psexec.py Administrador:3186948089@192.168.1.91



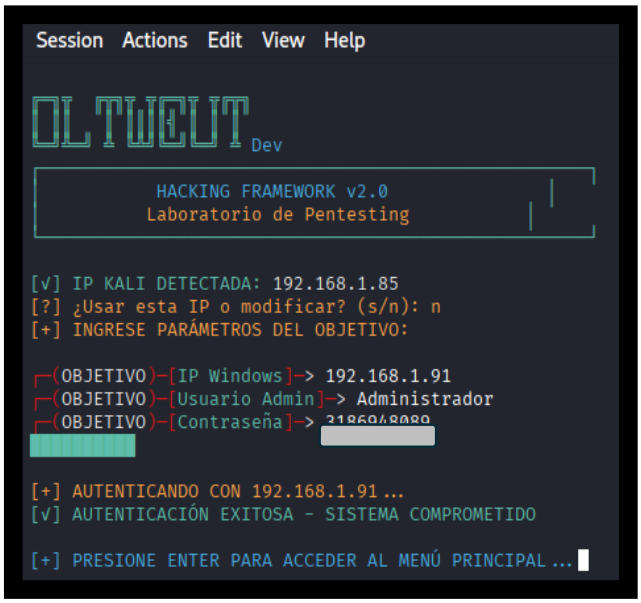
- En este punto se puede usar una cantidad muy variada de comandos de impacket que permiten extraer la información de Windows de manera remota, pero sería muy tardada por ello se ha desarrollado un menú interactivo.

4. Del anterior comando saldremos de el con Ctrl + C y dejaremos la terminal un momento, ahora pegaremos en la carpeta **home** el archivo **impacket.sh** que se encuentra en el repositorio donde se encuentra este mismo documento:



5. En la terminal ejecutaremos los comandos > **chmod +x impacket.sh** > **sudo ./impacket.sh** los cuales nos llevaran al menú interactivo impacket con funciones principales de extracción de información.

- NOTA: Para usar el menú interactivo se deberá tener el usuario **Admin** y **Contraseña** de Windows además de la **Ip** de la misma



>>>

CONCLUSION:

Este menú mejorar la experiencia de uso de la herramienta impacket además de una alta facilidad de uso de comandos y un entendimiento sobre las opciones mostradas en el menú.