

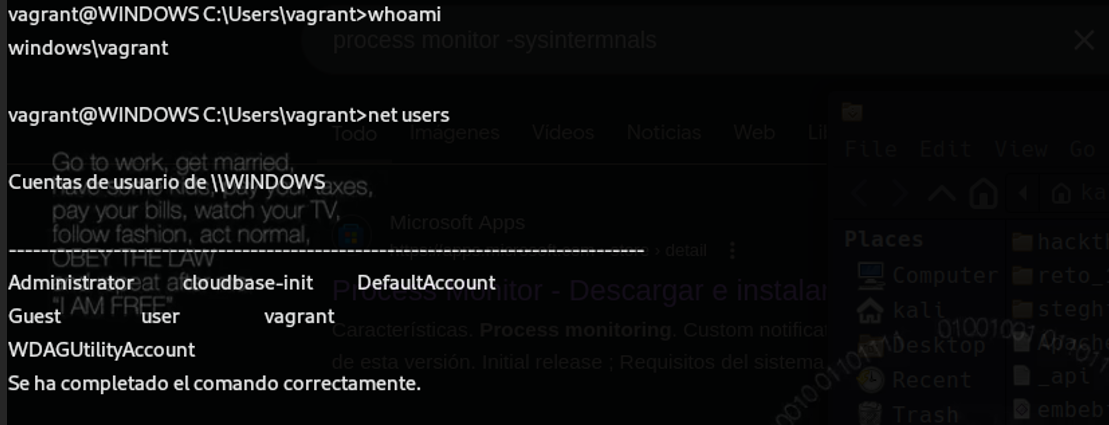
SPRING 16

EJERCICIO UNIDAD 1 – HIGH PRIVILEGE WINDOWS

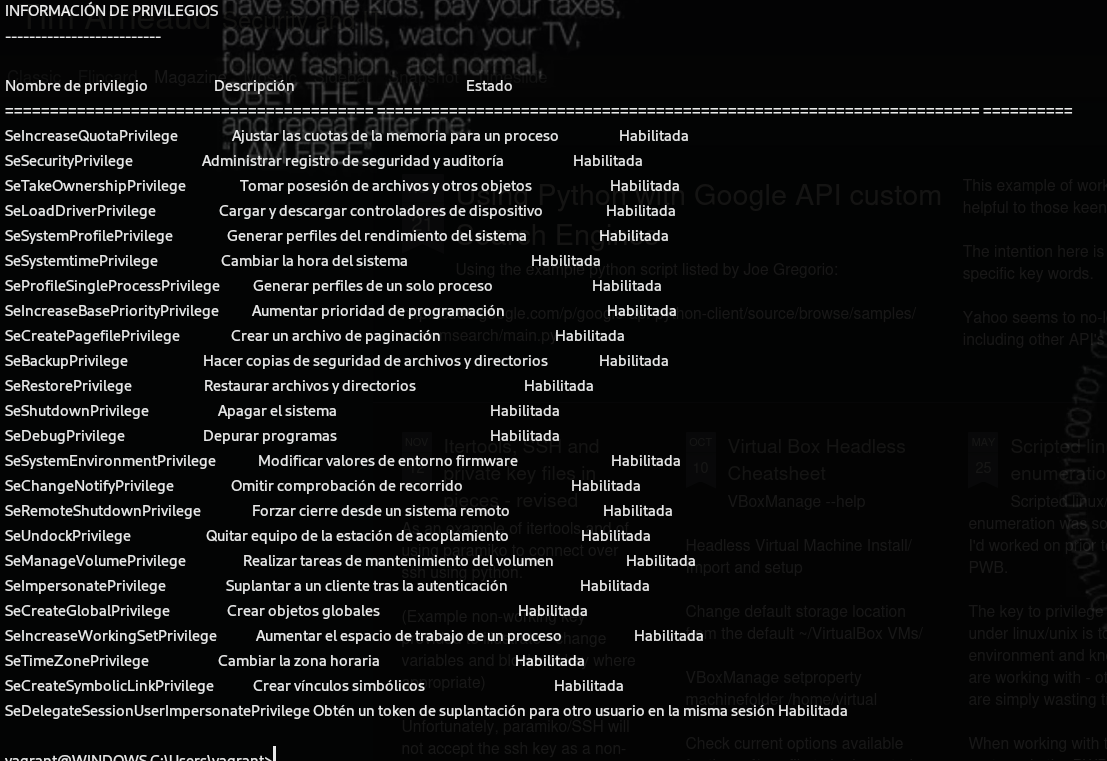
DLL HIJAKIING Y PHANTOM DLL

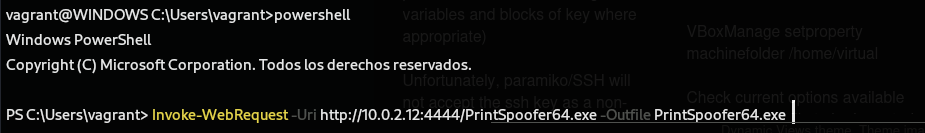
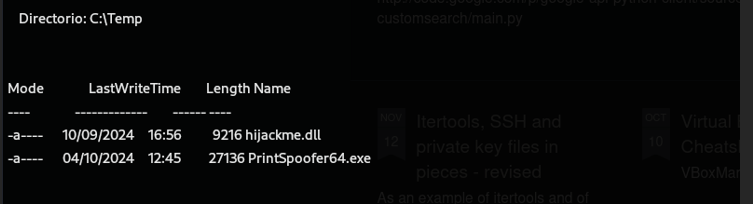
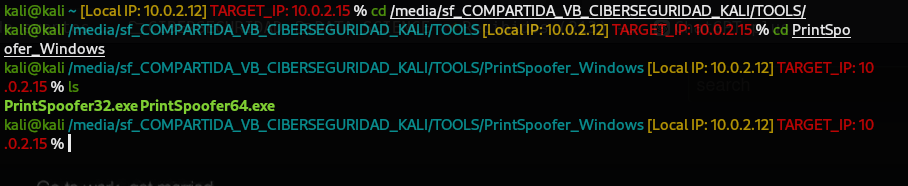
EJERCICIO 1.- EXPLOTACIÓN MÁQUINA WINDOWS CON EL MÉTODO “*PRINTSPOOFER”.*

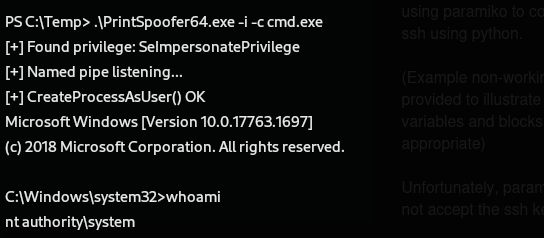
* Una vez instalada y conectada en el mismo rango de red que mi maquina Kali, procedemos a realizar un netdiscover para conocer la dirección IP del objetivo siendo esta 10.0.2.15.
* Ahora, dado que tenemos usuario y contraseña del usuario *“vagrant”,* procedemos a conectarnos a la maquina Windows a través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



Para ver la información de los privilegios del sistema que tenemos con nuestro usuario ejecutamos: ***whoami /priv***



* Como podemos observar tenemos muchos servicios habilitados, algunos con un alto nivel de poder sobre el sistema (“*SeDebugPrivilege”, “SeImpersonatePrivilege” o “SeTakeOwnershipPrivilege”*), siendo explotable únicamente por el método PrintSpoofer el servicio ***“SeImpersonatePrivilege***”. No obstante, un atacante que tenga acceso a alguno de los otros dos privilegios, podría combinar técnicas para escalar privilegios en el sistema.
* El servicio “***“SeImpersonatePrivilege”,*** normalmente, está habilitado para cuentas de servicio o que formen parte del grupo del administrador permite que un proceso suplante la identidad de otro usuario después de la autenticación, es decir, que si un atacante o un proceso con este privilegio, puede suplantar el token de un proceso con mayores privilegios (System), pudiendo ejecutar acciones en su nombre ( algo similar a los Bit SUID en Linux).
* Una vez verificado que tenemos este servicio habilitado, enviamos el fichero “PrintSpoofer64.exe” , previamente bajado desde la maquina Kali, abriendo un servidor python en esta máquina, ejecutando en la máquina objetivo una shell de “*PowerShel*l”, y una vez en ella, ejecutamos el comando “*Invoke-Web”* junto a sus parámetros, consiguiendo tener en el directorio *C:\Temp* el archivo malicioso.
* Finalmente, ejecutamos el archivo malicioso de manera interactiva (-i) para que, una vez conseguido el token privilegiado, ejecute el comando (-c cmd.exe), donde abrirá la shell con los permisos elevados, concretamente, con el usuario ***“nt authority”.***



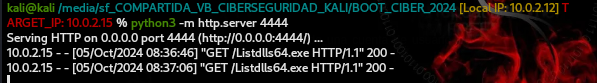
EJERCICIO 2.- ELEVACION DE PRIVILEGIOS MEDIANTE EL METODO *“PHANTOM DLL”*

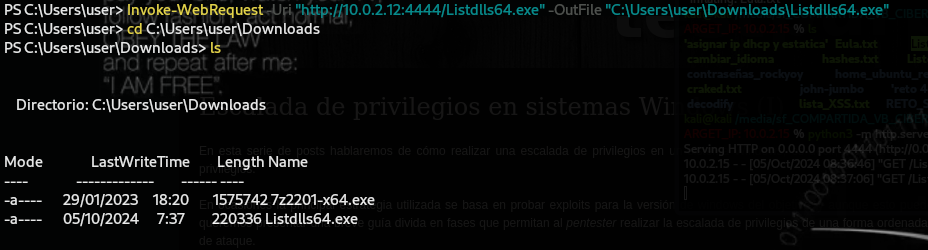
* Una vez instalada y conectada en el mismo rango de red que mi maquina Kali, procedemos a realizar un netdiscover para conocer la dirección IP del objetivo siendo esta 10.0.2.15.
* Ahora, dado que tenemos usuario y contraseña del usuario *“user”,* procedemos a conectarnos a la maquina Windows a través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



* En este caso, los servicios habilitados están muy limitados, por un lado, está el servicio **“SeChangeNotifyPrivilege”,** el cual, permite que el proceso monitorice, únicamente, los cambios en archivos y directorios y, por otro lado, ***“SeIncreaseWorkingSetPrivilege”,*** que permite a los procesos aumentar su espacio de trabajo, es decir, que puede influir en la cantidad de memoria que utiliza un proceso en el sistema.

Aunque no es permite la inyección de una DLL de manera directa, si puede proporcionar un ámbito que permita aprovechar esos procesos de ampliación de memoria para modificar, inyectar o abusar de un proceso de carga en la memoria del sistema.





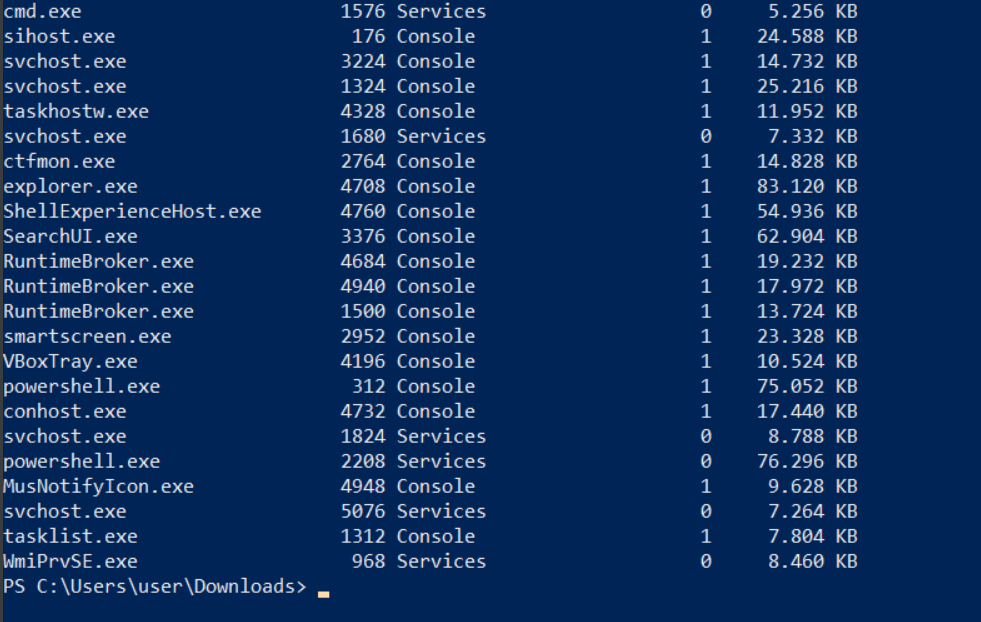


El privilegio **SeIncreaseWorkingSetPrivilege** te permite modificar la cantidad de memoria asignada a los procesos en ejecución, lo cual podría ser útil si logras manipular un proceso con más privilegios (por ejemplo, un proceso del sistema o uno ejecutado como **SYSTEM**).

Dado que no puedes inyectar directamente una DLL o código malicioso en estos procesos, una opción viable sería aprovechar la **manipulación de la memoria** para alterar el comportamiento de un proceso o forzar la ejecución de código que puedas controlar.

PS C:\Users\user\Downloads> tasklist





Nombre de imagen PID Nombre de sesión Núm. de ses Uso de memor

========================= ======== ================ =========== ============

System Idle Process 0 Services 0 8 KB

System 4 Services 0 160 KB

Registry 88 Services 0 73.332 KB

smss.exe 280 Services 0 1.148 KB

csrss.exe 368 Services 0 5.480 KB

wininit.exe 444 Services 0 6.948 KB

csrss.exe 452 Console 1 5.324 KB

winlogon.exe 504 Console 1 13.560 KB

services.exe 580 Services 0 9.952 KB

lsass.exe 600 Services 0 16.524 KB

svchost.exe 708 Services 0 3.844 KB

fontdrvhost.exe 728 Console 1 5.296 KB

fontdrvhost.exe 736 Services 0 4.448 KB

svchost.exe 744 Services 0 26.348 KB

svchost.exe 840 Services 0 10.944 KB

svchost.exe 888 Services 0 9.848 KB

dwm.exe 972 Console 1 46.516 KB

svchost.exe 308 Services 0 12.820 KB

svchost.exe 456 Services 0 9.900 KB

svchost.exe 624 Services 0 5.780 KB

svchost.exe 556 Services 0 11.688 KB

svchost.exe 1136 Services 0 14.396 KB

svchost.exe 1160 Services 0 7.396 KB

VBoxService.exe 1240 Services 0 7.800 KB

svchost.exe 1300 Services 0 7.404 KB

svchost.exe 1316 Services 0 6.676 KB

svchost.exe 1344 Services 0 7.268 KB

svchost.exe 1384 Services 0 9.936 KB

svchost.exe 1432 Services 0 11.328 KB

svchost.exe 1440 Services 0 7.584 KB

svchost.exe 1464 Services 0 5.632 KB

svchost.exe 1540 Services 0 11.552 KB

svchost.exe 1636 Services 0 8.032 KB

svchost.exe 1648 Services 0 14.352 KB

svchost.exe 1660 Services 0 6.776 KB

svchost.exe 1716 Services 0 7.968 KB

svchost.exe 1724 Services 0 8.768 KB

svchost.exe 1776 Services 0 8.148 KB

svchost.exe 1812 Services 0 8.232 KB

svchost.exe 1976 Services 0 11.848 KB

svchost.exe 1036 Services 0 9.320 KB

svchost.exe 1228 Services 0 16.288 KB

svchost.exe 2180 Services 0 9.836 KB

svchost.exe 2324 Services 0 7.800 KB

svchost.exe 2332 Services 0 7.128 KB

svchost.exe 2352 Services 0 8.180 KB

spoolsv.exe 2400 Services 0 16.584 KB

svchost.exe 2528 Services 0 13.632 KB

svchost.exe 2544 Services 0 17.264 KB

svchost.exe 2552 Services 0 34.148 KB

svchost.exe 2688 Services 0 7.996 KB

svchost.exe 2700 Services 0 6.984 KB

svchost.exe 2752 Services 0 6.556 KB

svchost.exe 2804 Services 0 11.492 KB

sshd.exe 2816 Services 0 7.336 KB

svchost.exe 2836 Services 0 5.436 KB

svchost.exe 2844 Services 0 7.532 KB

svchost.exe 2856 Services 0 6.280 KB

svchost.exe 2920 Services 0 19.960 KB

svchost.exe 3296 Services 0 12.020 KB

svchost.exe 3648 Services 0 5.404 KB

svchost.exe 5024 Services 0 13.784 KB

svchost.exe 5092 Services 0 7.560 KB

msdtc.exe 4232 Services 0 10.012 KB

sppsvc.exe 4364 Services 0 17.836 KB

svchost.exe 3956 Services 0 15.408 KB

SppExtComObj.Exe 4280 Services 0 8.384 KB

svchost.exe 3292 Services 0 18.152 KB

svchost.exe 2304 Services 0 12.064 KB

svchost.exe 4412 Services 0 11.276 KB

svchost.exe 4424 Services 0 22.332 KB

svchost.exe 4432 Services 0 10.920 KB

conhost.exe 1476 Services 0 5.852 KB

cmd.exe 1576 Services 0 5.256 KB

sihost.exe 176 Console 1 24.588 KB

svchost.exe 3224 Console 1 14.732 KB

svchost.exe 1324 Console 1 25.216 KB

taskhostw.exe 4328 Console 1 11.952 KB

svchost.exe 1680 Services 0 7.332 KB

ctfmon.exe 2764 Console 1 14.828 KB

explorer.exe 4708 Console 1 83.120 KB

ShellExperienceHost.exe 4760 Console 1 54.936 KB

SearchUI.exe 3376 Console 1 62.904 KB

RuntimeBroker.exe 4684 Console 1 19.232 KB

RuntimeBroker.exe 4940 Console 1 17.972 KB

RuntimeBroker.exe 1500 Console 1 13.724 KB

smartscreen.exe 2952 Console 1 23.328 KB

VBoxTray.exe 4196 Console 1 10.524 KB

powershell.exe 312 Console 1 75.052 KB

conhost.exe 4732 Console 1 17.440 KB

svchost.exe 1824 Services 0 8.788 KB

powershell.exe 2208 Services 0 76.296 KB

MusNotifyIcon.exe 4948 Console 1 9.628 KB

svchost.exe 5076 Services 0 7.264 KB

tasklist.exe 1312 Console 1 7.804 KB

WmiPrvSE.exe 968 Services 0 8.460 KB

PS C:\Users\user\Downloads>