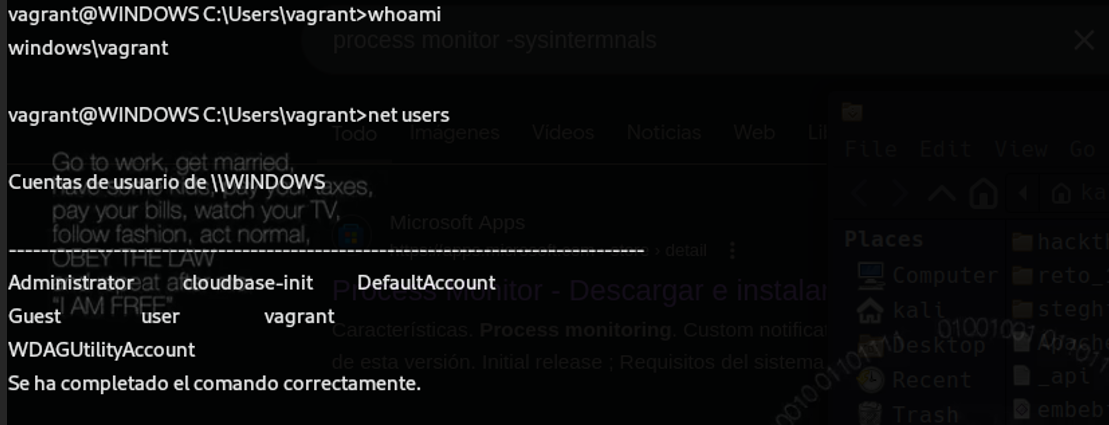
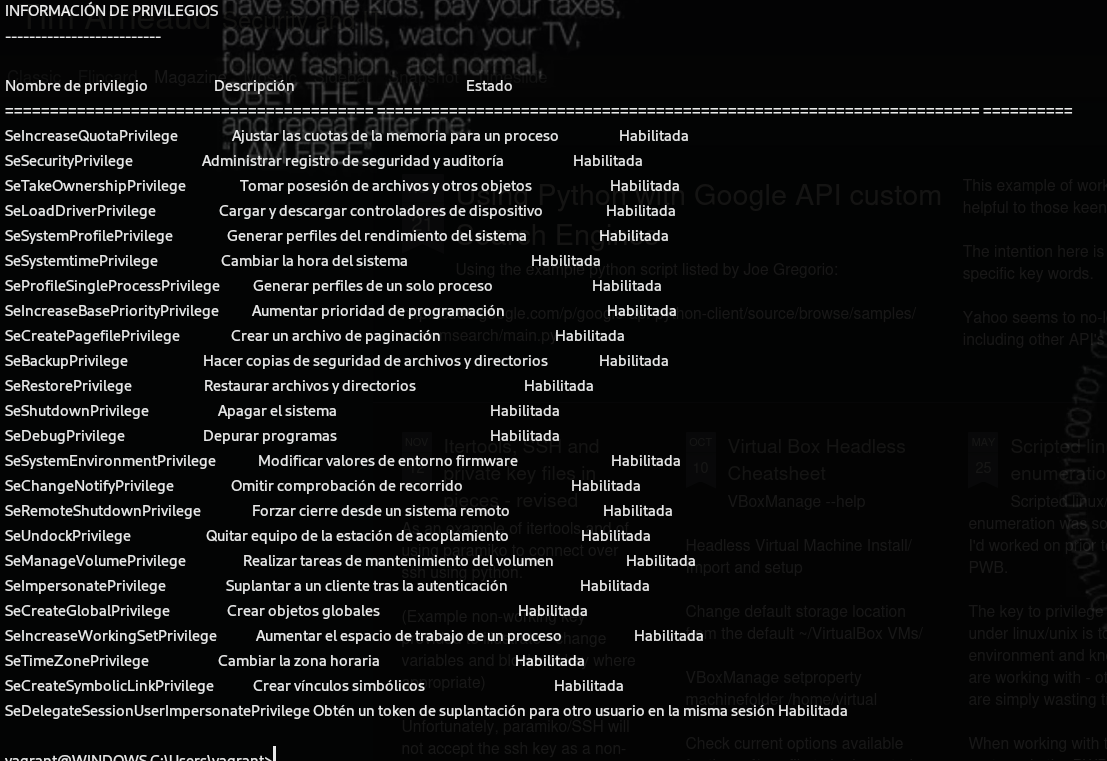
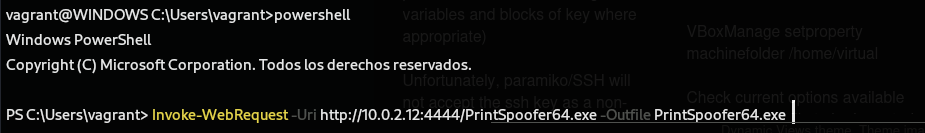
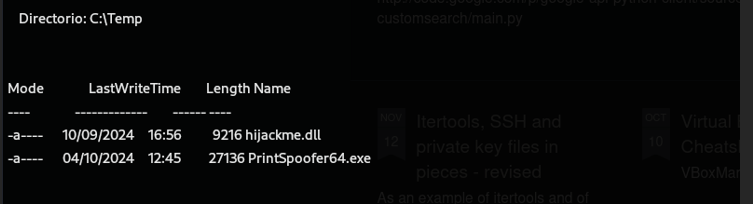
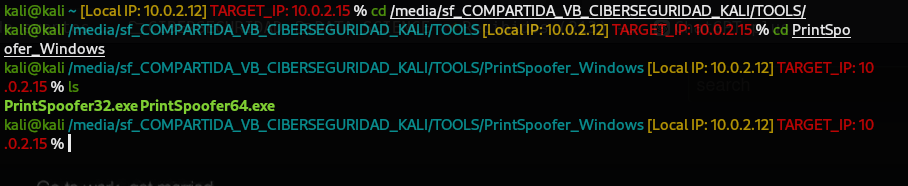
EJERCICIO 1.- EXPLOTACIÓN MÁQUINA WINDOWS CON EL MÉTODO “*PRINTSPOOFER”.*

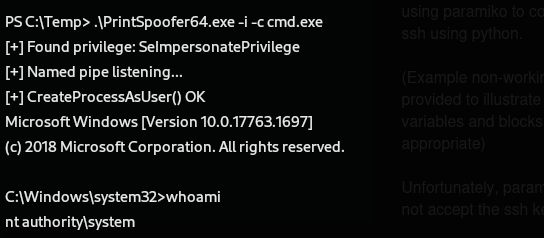
* Una vez instalada y conectada en el mismo rango de red que mi maquina Kali, procedemos a realizar un netdiscover para conocer la dirección IP del objetivo siendo esta 10.0.2.15.
* Ahora, dado que tenemos usuario y contraseña del usuario *“vagrant”,* procedemos a conectarnos a la maquina Windows a través 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”*