Aquí están todas las funciones de las opciones de Impacket que proporcionaste:

Lista

1. \*\*impacket-addcomputer\*\*: Agrega un equipo al dominio de Active Directory.

2. \*\*impacket-atexec\*\*: Ejecuta comandos en sistemas remotos a través del Programador de tareas de Windows.

3. \*\*impacket-changepasswd\*\*: Cambia la contraseña de un usuario en un controlador de dominio de Active Directory.

4. \*\*impacket-dcomexec\*\*: Ejecuta comandos de forma remota a través de DCOM (Distributed Component Object Model).

5. \*\*impacket-DumpNTLMInfo\*\*: Extrae información relacionada con NTLM (NT LAN Manager) de un tráfico de red capturado.

6. \*\*impacket-esentutl\*\*: Permite trabajar con bases de datos ESENT (Extensible Storage Engine) en sistemas Windows.

7. \*\*impacket-exchanger\*\*: Interactúa con el servicio Exchange de Microsoft para enumerar información y realizar acciones.

8. \*\*impacket-findDelegation\*\*: Busca delegaciones de credenciales en un entorno de Active Directory.

9. \*\*impacket-GetADUsers\*\*: Obtiene información sobre usuarios de Active Directory.

10. \*\*impacket-Get-GPPPassword\*\*: Recupera contraseñas almacenadas en Preferencias de Directiva de Grupo (GPP) de Active Directory.

11. \*\*impacket-GetNPUsers\*\*: Realiza una solicitud de Servicio de No Preautenticación (AS-REP) para enumerar usuarios de Active Directory.

12. \*\*impacket-getPac\*\*: Extrae el Ticket de Autenticación Preautenticado (PAC) de un ticket Kerberos.

13. \*\*impacket-getST\*\*: Obtiene un Service Ticket (ST) de un controlador de dominio de Active Directory.

14. \*\*impacket-getTGT\*\*: Obtiene un Ticket Granting Ticket (TGT) de un controlador de dominio de Active Directory.

15. \*\*impacket-getArch\*\*: Obtiene la arquitectura del sistema operativo de un host remoto.

16. \*\*impacket-GetUserSPNs\*\*: Enumera Service Principal Names (SPNs) asociados a cuentas de usuario en Active Directory.

17. \*\*impacket-goldenPac\*\*: Genera un PAC dorado para obtener acceso a recursos de Active Directory.

18. \*\*impacket-keylistattack\*\*: Lanza un ataque de lista de claves en un controlador de dominio de Active Directory.

19. \*\*impacket-karmaSMB\*\*: Implementa un ataque de Karma para interceptar solicitudes SMB (Server Message Block).

20. \*\*impacket-kintercept\*\*: Implementa un servidor proxy Kerberos para interceptar solicitudes TGS (Ticket-Granting Service).

21. \*\*impacket-lookupsid\*\*: Realiza la traducción de SID (Security Identifier) a nombres de usuario y viceversa.

22. \*\*impacket-machine\_role\*\*: Enumera el rol de un equipo en un dominio de Active Directory.

23. \*\*impacket-mimikatz\*\*: Ejecuta el proyecto Mimikatz para interactuar con credenciales y tokens en sistemas Windows.

24. \*\*impacket-mssqlclient\*\*: Interactúa con servidores Microsoft SQL Server para ejecutar consultas SQL y realizar diversas acciones de administración.

25. \*\*impacket-mssqlinstance\*\*: Enumera instancias de Microsoft SQL Server en una red.

26. \*\*impacket-net\*\*: Enumera información sobre equipos y usuarios en un dominio de Active Directory.

27. \*\*impacket-netview\*\*: Enumera recursos compartidos y usuarios conectados a un servidor de red.

28. \*\*impacket-nmapAnswerMachine\*\*: Responde a solicitudes Nmap (Network Mapper) para obtener información sobre un sistema.

29. \*\*impacket-ntfs-read\*\*: Lee archivos y directorios en sistemas de archivos NTFS (New Technology File System) de Windows.

30. \*\*impacket-ntlmrelayx\*\*: Implementa un ataque de relé NTLM para obtener acceso a sistemas de destino.

31. \*\*impacket-ping\*\*: Realiza un ping a un host remoto utilizando el protocolo ICMP (Internet Control Message Protocol).

32. \*\*impacket-ping6\*\*: Realiza un ping a un host remoto utilizando el protocolo ICMP versión 6.

33. \*\*impacket-psexec\*\*: Ejecuta comandos de forma remota en sistemas Windows utilizando el servicio PsExec.

34. \*\*impacket-raisedChild\*\*: Crea un proceso secundario en un sistema remoto.

35. \*\*impacket-rbcd\*\*: Ejecuta comandos de forma remota utilizando el servicio Windows RunAs.

36. \*\*impacket-rdp\_check\*\*: Verifica si un servidor RDP (Remote Desktop Protocol) está disponible en un host remoto.

37. \*\*impacket-reg\*\*: Realiza operaciones de registro del sistema en sistemas Windows.

38. \*\*impacket-registry-read\*\*: Lee claves y valores del registro del sistema en sistemas Windows.

39. \*\*impacket-rpcdump\*\*: Enumera interfaces RPC (Remote Procedure Call) disponibles en un sistema Windows.

40. \*\*impacket-rpcmap\*\*: Muestra un mapeo de servicios RPC disponibles en un sistema Windows.

41. \*\*impacket-sambaPipe\*\*: Interactúa con tuberías SMB (Server Message Block) en sistemas Windows.

42. \*\*impacket-samrdump\*\*: Extrae información de la base de datos SAM (Security Account Manager) de un sistema Windows.

43. \*\*impacket-secretsdump\*\*: Recupera contraseñas almacenadas en un sistema Windows utilizando varias técnicas.

44. \*\*impacket-services\*\*: Enumera servicios registrados en un sistema Windows.

45. \*\*impacket-smbclient\*\*: Permite interactuar con servidores SMB (Server Message Block) para realizar diversas acciones.

46. \*\*impacket-smbexec\*\*: Ejecuta comandos de forma remota en sistemas Windows utilizando el protocolo SMB.

47. \*\*impacket-smbpasswd\*\*: Cambia la contraseña de un usuario en un servidor Samba.

48. \*\*impacket-smbrelayx\*\*: Implementa un ataque de relé SMB para obtener acceso a sistemas de destino.

49. \*\*impacket-smbserver\*\*: Implementa un servidor SMB para compartir recursos en una red.

50. \*\*impacket-sniff\*\*: Captura y analiza paquetes de red en una red.

51. \*\*impacket-sniffer\*\*: Captura y analiza paquetes de red en una red.

52. \*\*impacket-split\*\*: Divide archivos grandes en segmentos más pequeños.

53. \*\*impacket-ticketConverter\*\*: Convierte tickets Kerberos de un formato a otro.

54. \*\*impacket-ticketer\*\*: Genera tickets Kerberos para solicitudes de servicio.

55. \*\*impacket-tstool\*\*: Realiza diversas tareas relacionadas con tickets Kerberos.

56. \*\*impacket

-wmiexec\*\*: Ejecuta comandos de forma remota en sistemas Windows utilizando el protocolo WMI (Windows Management Instrumentation).

57. \*\*impacket-wmipersist\*\*: Implantación persistente en sistemas Windows utilizando el protocolo WMI.