|  |  |  |
| --- | --- | --- |
| Número | Caso de Uso | Descripción |
| 1 | Enviar Archivo | El bot o máquina remota debe de poder enviar un fichero al servidor cuando éste lo solicite. |
| 2 | Recibir Archivo | El bot o máquina remota debe de poder recibir un fichero al servidor cuando éste lo solicite. |
| 3 | Recibir Orden | El bot o máquina remota debe de poder recibir una orden del servidor. |
| 4 | Enviar Output | El bot debe de poder ejecutar la orden del servidor y enviarle el output. |
| 5 | Abrir Reverse Shell | El bot o máquina remota debe de poder abrir una Shell reversa al servidor cuando éste lo solicite. |
| 6 | Generar Payload | El módulo payload generator debe de proporcionar un payload de infección con todo lo necesario para establecerse en la máquina objetivo y además ser dinámico y multiplataforma. |
| 7 | Recibir Outputs | El atacante debe de poder recibir las salidas de las ordenes que ejecutan los bots. |
| 8 | Lanzar Campaña | El atacante debe de contar con la capacidad de lanzar una campaña a todos los bots que estén conectados. |
| 9 | Enviar Orden | El atacante debe de poder enviar una orden a uno o a varios bots. |
| 10 | Subir Archivo | El atacante podrá elegir un archivo local y subirlo a la máquina remota que desee. |
| 12 | Descargar Archivo Remoto | El atacante podrá elegir un archivo de la máquina remota que desee y bajárselo de manera local. |
| 13 | Monitorizar Servidor C&C | El atacante podrá monitorizar en todo momento los recursos del servidor. |
| 14 | Establecer Reverse Shell | El atacante podrá elegir un bot remoto que se encuentre conectado y abrir una Shell reversa brindándole control absoluto. |