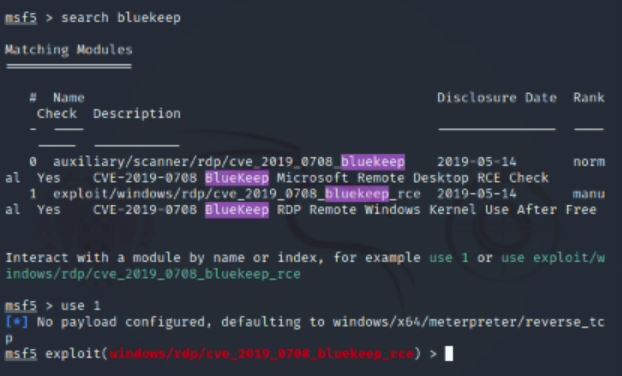
|  |  |
| --- | --- |
| **Informe sobre la vulnerabilidad encontrada** | |
| Nombre | Exploit con Bluekeep |
| Módulo | windows/rdp/cve\_2019\_0708\_bluekeep\_rce |
| *Payload* | Por defecto. Windows/x64/meterpreter/reverse\_tcp |
| Plataformas afectadas | Windows 7 / Windows 2008 |
| Medio de infección | A través de la red, cuando un atacante no autenticado se conecta con una máquina mediante RDP y envía peticiones. |
| Tipo de vulnerabilidad recogida en el CVE | (CVE-2019-0708) Vulnerability in Remote Desktop Service Remote code execution. |
| Posibles objetivos | Cualquier usuario con Windows 7 o Windows 2008. |
| Descripción | Realiza una denegación de servicios a la máquina vulnerable, realizando un ataque de pantallazo azul. |
| Contra-medidas | Actualizar el sistema operativo y no abrir los puertos de máquinas remotas a personas sin autenticación. |

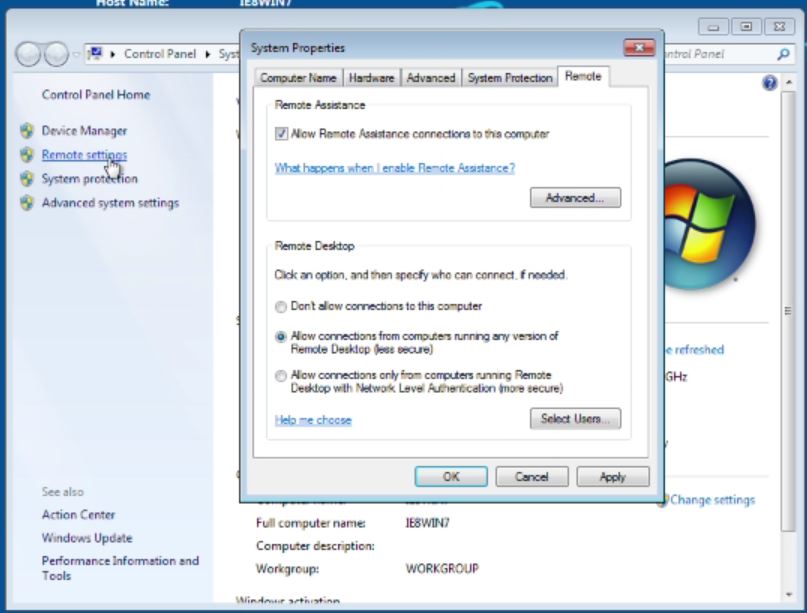
Pasos seguidos:

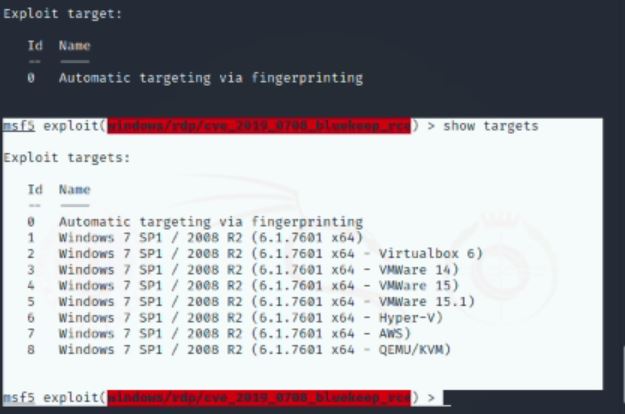
Primero, realizamos la configuración para conectar ambas máquinas como en el guión de la práctica. Tras realizar estos paso, y comprobar que ambas máquinas se han conectado correctamente, procedemos a entrar en msfconsole.

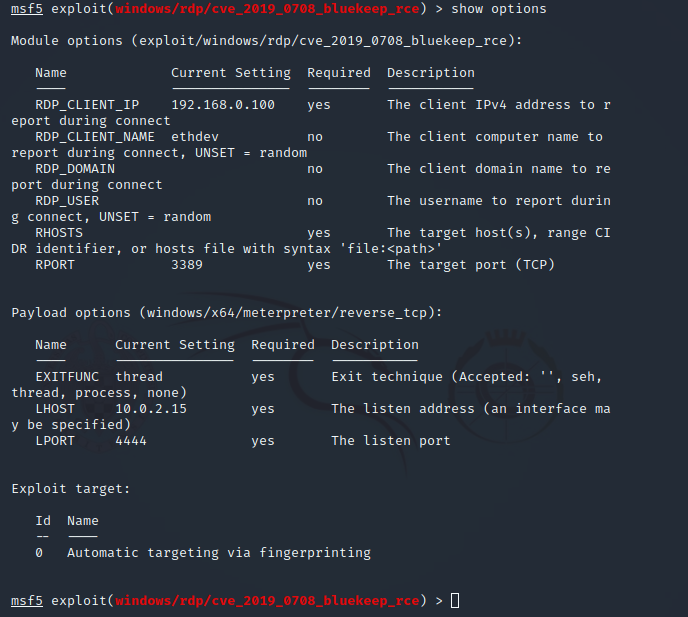
Dentro de la consola buscamos el exploit que queremos utilizar, en este caso, ‘bluekeep’ y seleccionamos la opción que queremos, que es, “exploit/Windows/rdp/cve\_2019\_0708\_bluekeep\_rce”.



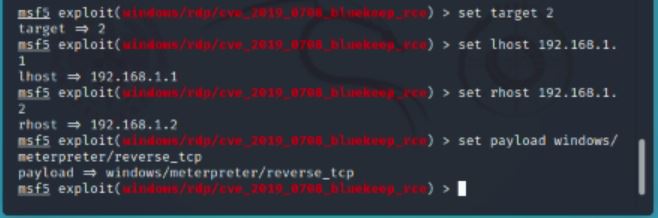
En el siguiente paso, la máquina vulnerable tendremos que configurarla para que permita acceso a máquinas remotas sin autenticación, abriendo el puerto 3389. Para esto tendremos que ir a Panel de control -> Propiedades -> Remote settings y dentro de esta, permitir las conexiones remotas en este ordenador.

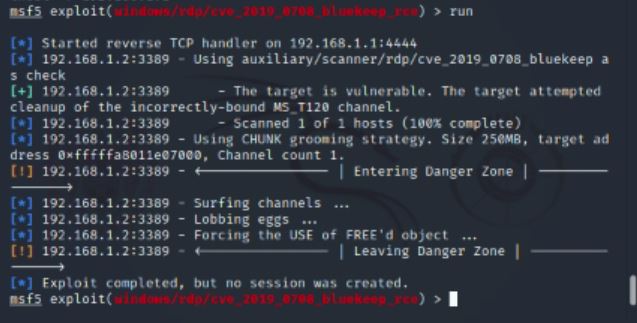


Una vez realizado este paso miraremos las opciones que tenemos que configurar en la máquina atacante, los puertos a configurar en este caso serán LHOST, RHOST y el PAYLOAD. Excepcionalmente para este exploit también habrá que seleccionar el TARGET, a que máquina y desde cual se va a realizar el ataque.



Configuramos los puertos que se nos piden que hemos comprobado en Show options. Seleccionaremos el target 2, ya que el ataque lo realizaremos en Windows 7 desde Virtualbox 6.1.



Una vez configurado, ya podemos proceder a hacer el exploit, usando los comandos ‘exploit’ o ‘run’.

En nuestro caso, el exploit ha funcionado pero no crea una sesión, por lo que no conseguimos realizar el ataque con éxito (el pantallazo azul en la máquina vulnerable). Esto se debe a que el puntero del script que realiza este exploit hay veces que no se encuentra en donde debería estar y por eso no se realiza correctamente. Para corregir esto habría que realizar un volcado de memoria, para obtener el valor en el que debería estar el puntero y reemplazarlo en el script correspondiente.

Sin embargo, hemos intentado realizar estos pasos pero nos ha resultado imposible. Por lo que no hemos conseguido explotar la vulnerabilidad correctamente.